GREAT CHAIN OF NUMBERS

a guide to smart contracts, smart property, and trustless asset management

TIM SWANSON

Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management

By Tim Swanson

Cover art credit: Matt Thomas and Invisible Order

Contents

Foreword

> *"It is a rare mind indeed that can render the hitherto non-existent blindingly obvious. The cry 'I could have thought of that' is a very popular and misleading one, for the fact is that they didn't, and a very significant and revealing fact it is too."*
>
> - Douglas Adams, Dirk Gently's Holistic Detective Agency

The physical world has an intractable problem; things exist.

Whether a bar of gold or a bus pass, left to their own devices these valuable objects will not move or act of their own accord. Furthermore, if you want to sell such an item, you have the unenviable task of finding someone who would like that item from you, is willing to pay you in the thing you desire and is local enough to make such a deal logical.

Money used to have this problem; we used antiquated systems that move promises for dollars around the world at 1960 speed. Bitcoin changed the equation, introducing the distributed ledger technology that allows value to change owner with no regard for where the transacting users are geographically located.

Bitcoin is to money what Smart Property is to ownership. A fundamental reinvention of how things should work, and a better way. The problems are not new, and the solutions enacted to this point were designed with that liability of physical existence in mind.

We are no longer constrained by this liability.

This all occurs against a backdrop of open source innovation and cooperative competition among the projects vying to "win" the battle for Bitcoin 2.0. Where six months ago there were two projects, now there are eight, with new protocols announced at least monthly.

When Satoshi Nakamoto mined the Genesis Block, he had months before there was much competition for the tokens he was mining and years before the first competitor for his protocol emerged. In this next generation there is no luxury of obscurity. The race is on and the only sure winner is technological progress.

In the information age, technological optimization is often confused with technological progress. Both are measures of growth, improvement in the lives of users of these technologies, but they are very much not the same thing.

Optimization is a purely additive process. Moore's law and the competitive nature of the free market demand that these items be made smaller and denser. Faster and cheaper. This is steady and predictable, and it can be mapped and planned for.

Sometimes optimization constitutes progress; but most real progress, paradigm shifting in implication, comes from doing something unexpected. Intentionally or not.

You cannot plan for this.

You are not prepared for this.

But then, neither is anybody else.

So rejoice, because you got here first. Consider the manuscript that follows your guide to the exciting world of smart property, and let me be the first to welcome you to the Future of Money.

Adam B. Levine
Editor-in-Chief, *Let's Talk Bitcoin!* March 3rd, 2014

Preface

With the help of many members of the community, I have written this short book for beginners, entrepreneurs and risk-takers who – having heard of a bitcoin or cryptocurrency, but knowing little about it – want to understand how algorithms can constrain governance and transfer value in a consensus-driven, voluntary manner.

Trustless asset management tools built on top of a cryptoledger such as Bitcoin or Ripple (which are tamper-proof) could not only reduce fees and redundancies in the developed world but also empower those in the developing world who are more easily marginalized as they lack political capital (*guanxi*).[1] Cryptoledgers could also help governments and non-governmental institutions keep track of internal assets and reduce the barriers to financial services, leveling the playing field and allowing individuals from all walks of life to actually codify and manage scarce goods and value that they currently own in a more secure manner.

From securely automating parts of the financial industry (e.g., back-offices) to lowering transaction costs of international trade, this new type of mathematical tool – cryptoledgers – can be applied to many new segments and markets, some more obvious than others. For instance, in January 2014 I was interviewed by Donald McIntyre who asked me why I was interested in cryptocurrencies and smart contracts.[2] I explained that there are additional use-cases for using cryptoledgers to track property titles and contractual agreements that could be utilized not only in the developed world but also in developing countries like China.

While there are a number of analogies comparing the significance of these tools with historical equivalents – from railroad infrastructure, to operating system platforms – at their core decentralized applications like Bitcoin and its progeny have the potential to impact virtually any industry that is integrated with the internet. And the insights from experts, entrepreneurs, investors and developers below illustrate many of the other uses that cryptoprotocols can provide and gives readers a foundation to build from and to explore.

There will likely be challenges and hurdles along the way, from embarking on educational outreach beyond early-adopters to carefully studying and complying with all the legal and jurisdictional issues of a particular instrument.

Yet there are also likely financial rewards for reducing the fees involved in remittances or providing more secure and robust mobile payments. For instance, according to Gartner, "mobile payments will top $720 billion a year by 2017, up from $235 billion last year [2013]."[3] Finding a way to build an application that provides value in this niche is just one area of disruptive potential that a decentralized or distributed cryptoledger can attempt to do without exposure to counterparty risks.

Finally, this manuscript is not an exegesis on the economic foundation or utility of cryptocurrencies. While economists were consulted, this guide is an attempt to show the potential of changing how interactions and value can be transferred and managed in a manner that could not be technologically or mathematically done until this past decade.

This is an exciting journey and one that I believe will outlive and outlast the hype and hyperbole of both its largest ideological proponents and opponents. In time some of the visions and claims may ultimately be vaporware, yet several have the potential to impact commerce the same way that the internet did 20

years ago and the PC did 35 years ago. Let me help provide you with the knowledge that was distilled and shared with me over the course of my own educational process.

Tim Swanson

San Francisco, March 2013

Acknowledgements

I would like to thank the following entrepreneurs, businesspeople, experts, investors and thought-leaders for their time, views and feedback for this guide: Derek Au, Steve Bennet, Nikos Bentenitis, Isaac Bergman, Vijay Boyapati, Vitalik Buterin, Preston Byrne, Zachary Caceres, Wences Casares, Raffael Danielli, Ben Davenport, Tuur Demeester, Mark DeWeaver, Joel Dietz, Charles Evans, Scott Freeman, Michael Goldstein, Ron Gross, Mike Hearn, Jon Holmquist, David Johnston, Petri Kajander, Zennon Kapron, Jeremy Kandah, Stephan Kinsella, Daniel Krawisz, Daniel Larimer, Adam Levine, Taariq Lewis, Jeremy Liew, Rui Ma, Hakim Mamoni, Robert McMillan, Amos Meiri, Jared Mimms, Alex Mizrahi, Kevin Moore, Tom Mornini, Chris Odom, Ryan Orr, Stephen Pair, Salvatore Delle Palme, Sean Percival, Jesse Powell, Chris Piaca, Celso Pitta, Mike Reid, Scott Robinson, Dan Roseman, Meni Rosenfeld, Alan Safahi, Robert Sams, Sebastian Serrano, Justin Simcock, Koen Swinkels, Nick Szabo, Alex Tabarrok, Stefan Thomas, Kyle Torpey, Eddy Travia, Stephan Tual, David Veksler, Jack Wang, Andrew White, Matthew Wilson, Yanli Xiao, Mike Youssefmir and Sean Zoltek. The usage of handles: “cityglut,” “Graviton,” “PhantomPhreak” and “Uniqueorn,” is to protect the privacy of the individual.

Throughout the book I refer to their insights. This is not an explicit endorsement of their opinions or services but rather serves as an on-the-ground reference point. Nor by providing me with quotes do they endorse this book or my opinions. Furthermore, in the interest of financial disclosure, I do not currently have any equity positions in the firms or companies discussed throughout, nor was I provided any financial compensation for the inclusion of companies or projects.

Glossary

Because of the dynamic nature of this new ecosystem, the data and statistics cited here will quickly become outdated. This is not making excuses for the manuscript but rather illustrates to you the rapid pace of change relating to innovations and opportunities in this new space.

Before embarking on reading this book, below are commonly used definitions for several important terms used throughout the guide:

Smart contracts[4] are computer protocols that facilitate, verify, execute and enforce the terms of a commercial agreement.[5] Current proto-examples include some digital financial instruments used on electronic securities exchanges.

Smart property is property whose ownership is controlled via smart contracts that may or may not reside on a cryptoledger.

Cryptocurrency[6] is a virtual token (e.g., a bitcoin, a litecoin) having at least one *moneyness* attribute, such as serving as a medium of exchange.[7] It is transported and tracked on an encrypted, decentralized ledger called a **cryptoledger**.[8]

Trustless asset management refers to the ability to manage an asset such as a virtual token in a trustless manner – relying on mathematics, rather than a trusted 3rd party like a payment processor or a bank through the use of a cryptoledger.

Decentralized autonomous organization (DAO), also known as a decentralized autonomous consensus platform (DACP), is a virtual entity that interfaces with a cryptoledger and performs a specific, preprogrammed task. In its simplest form it is merely an agent programmed to do a specific task like acting as a multisignature wallet that sits on the ledger waiting for outside instructions. In order to modify or fulfill its task, it must receive a certain threshold of digital signatures from keyholders (e.g., voters, shareholders) and perhaps with a 67% majority, have the right to release the entity's funds and modify its code.[9] It can fulfill the functions of an organization, corporation, or agent by conducting operations such as payroll management, issuance of dividends, stock, or debt, or otherwise executing repetitive, mechanical, quantifiable actions from a cryptoledger.[10]

When spelled with an uppercase "B" **Bitcoin** (or uppercase "L" Litecoin) refers to a peer-to-peer network, open-source software, decentralized accounting ledger, software development platform, computing infrastructure, transaction platform and financial services marketplace.[11] When spelled with a lowercase "b" **bitcoin** (or "l" for litecoin) is a digital cryptocurrency and unit of account. As of this writing one bitcoin is equivalent to $600 USD and one litecoin is worth approximately $15 USD. In addition, the acronym "**BTC**" is often used to represent a bitcoin (and "LTC" for a litecoin).

Chapter 1: Introduction

This guide is a brief primer and resource for those looking to understand:

what a cryptoledger is,

what smart contracts are,

how smart property works and

the disruptive impact of trustless asset management.

While I typically use examples from the United States and China, there are numerous business and personal applications for each in any country, irrespective of size.

This is not a guide on how to invest, and you, the reader, should make sure to conduct thorough due diligence of the specific area you are looking to create value in. While there may be seemingly unlimited opportunities in this burgeoning field, there are also many risks – known and unknown. You should begin your search by familiarizing yourself with the groundbreaking works, which are freely available online, of Nick Szabo, who pioneered the field of smart contracts and smart property.[12] It is also highly recommended that in addition to consulting with someone familiar with business development related to cryptocurrency applications, you also speak with legal counsel and/or a risk assessment specialist who can help quantify and qualify the potential legal risks.

As this guide will illustrate in a general sense, even if you create an ostensibly ironclad smart contract that is used on a cryptoledger to track or transfer an asset, there may be brick-and-mortar legal institutions that do not recognize the manner in which the transaction takes place (e.g., exchanges must continue to use passive, paper-based interfaces). To some in the cryptocurrency community the traditional mechanisms seem anachronistic. The stark reality is that the traditional mechanisms (postal mail, fax machines) are still required for business and show no signs of disappearing anytime soon.

Keeping an Open Mind

The economics of Bitcoin can and will continue to fill countless volumes.[13] As to whether cryptocurrencies or tokens that act as virtual representations and abstractions of value actually are valuable, is in the eye of the beholder (or more appropriately, keyholder). It is also a self-correcting quandary: if you do not see value in holding any type of cryptocoin, metacoin or “colored” coin, then you simply will not accept them.

One of the primary benefits of Bitcoin and cryptocurrencies like it, the argument goes, is that it will reduce costs and friction in international commerce. Below is an image used with permission from Pierre Rochard that may help readers qualify many of the transaction costs between precious metals (gold, silver), fiat currencies (US dollars, euros) and cryptocurrencies:[14]

Transaction Cost	Precious Metals	Fiat Currencies	Bitcoin
Storage	0.15% to 1% per year	Subsidized by FRB*	*Free and 100% reserve*
Transportation	Expensive	Inconvenient	*Free & Easy*
Security	Physical	Institutional	*Cryptographic*
Fiduciary media	Inevitable	Inherent	*Impossible*
Recordkeeping	Manual	Manual	*Automatic*
Counterfeiting	Impossible	Inevitable	*Impossible*
Issuance	Mining	Politics	*Algorithm*
Payment clearing	Expensive	Centralized	*Cheap & Distributed*
Scarcity	High	Arbitrary	*Fixed - 21 million btc*
Authentication	Expensive assay	Trust counterparty	*Built-in*

** fractional reserve banking*

Economists and legal experts have suggested that Bitcoin is not a real "thing" with some pointing out that, in some jurisdictions, cryptocurrency is currently beyond proprietary classification.[15] I note below, they would be correct: it is nothing more than a virtual ledger entry. Yet, despite this level of abstraction, there are those who find utility in subjectively valuing its scarcity relative to other assets, namely, fiat currencies. Whether your neighbor or your favorite blogger values it the same way as you is not fundamentally important in the long run.[16] Ultimately what matters is, what additional units of utility both the token and the protocol could provide for you or others. Furthermore, if physical manifestations of value were all that mattered, then all of the abstractions humans use on a daily basis – from signing documents that represent contractual obligations and financial instruments, to swiping a credit card that sends electrons to a payment processor – would simply be a futile exercise in mental gymnastics.[17]

Altcoins

If you are new to the cryptocurrency world, you may have arrived through a variety of paths, including the altcoin world. An altcoin means "alternate coin" – which commonly means any cryptocoin or cryptoledger that is not Bitcoin. Sometimes an altcoin is an exact replica of the Bitcoin codebase: in other instances, it is drastically modified.

Namecoin is widely considered to have been the first altcoin. Namecoin is designed to act as a decentralized DNS system that makes domain name censorship difficult, if not impossible.[18] It was created in 2010 as a modified version of Bitcoin, and in 2011 the mining of namecoins (after block 19,200) was effectively merged with Bitcoin through a software update (e.g., pools had to use a new software release).[19][20]

While Namecoin provides DNS functionality, it can also be utilized as a messaging system, torrent tracker, and even a notary (which other cryptocurrencies can do as well). While it is uncertain that any or all of the altcoins or the ongoing "2.0" (next-generation) projects described below will ever be successful in accomplishing their goals, these potentially new innovations, like Namecoin before them, show that cryptoledgers can be integrated to provide rich functionality beyond the current token system.

This is not to say that the cryptocurrency community has uniformly embraced disruptive change: far from it. Like all inclusive groups, there are varying amounts of elitism, rigidity, and openness throughout.

People learn about cryptocurrencies through various ways. Many late-adopters, have learned about mining or even coding through other altcoins such as Litecoin and Dogecoin – which serve as gateways for new entrants to the larger crypto ecosystem.[21] These coins have done so, at least in part, because of the psychological value of being rewarded with a significantly larger amount of tokens for either fiat or mining (e.g., ten dollars for one billion dogecoins) – avoiding what is referred to as 'mental transaction costs' of doing decimal calculations in bitcoin.[22] Yet depending on the venue, these projects are often frowned upon by many early Bitcoin adopters.[23] Thus if you, the reader, choose to enter the community, you should know there are various political turf wars that I recommend you stay away from as they are a distraction to the value-added potential and business opportunities that trustless asset management promises.

This book focuses on the opportunities of the ecosystem, not a particular protocol: it is impossible to know what market conditions will be like in three or five years, what regulatory issues will arise, what developmental tools will or will not be made or what market participants will find utility in. Alice may, for some reason, find utility in a project or cryptocurrency that Bob find's distracting and pointless. For this reason it is important to distinguish your own subjective valuation from others'. While the analogy is imperfect, consider this sardonic perspective to dismissing Bitcoin alternatives *a priori*:

> 'It is too bad about English. All of that wasted effort on other languages. English is perfectly good but there are so many competing efforts that distract from a simple, powerful chain-of-letters – an alphabet. If only we had an L'Académie française to manage, prune and develop the language in a directed rational manner. Just look at all of these ridiculous languages used by just a fraction of the world's population. They are wasting scarce resources in maintaining all of those goofy spinoffs that do not really further the linguistic ecosystem as it is pointless redundancy. They merely just reinvent the wheel time and again with projects on syntax, grammar and style. It is too bad that English is not the only protocol used. And since it does not have 100% market share it is likely that the entire linguistic endeavor will fail. And fail hard.'

Skepticism is warranted for claims that in order for cryptoprotocols to be successful there needs to only be one cryptoledger in the world. This is akin to saying that for the internet to be successful there needs to only be one website (e.g., Reddit), and all of us need to support it and only it. People like choices; and consequently they have created alts. And there is probably room for more.

As Carl Sagan purportedly said, "It pays to keep an open mind, but not so open your brains fall out." Therefore, keep a lookout for new opportunities but be wary of lemons and scams – these exist in every economic sector including this brave new world of cryptocurrency. Conduct your due diligence and caveat emptor.

Chapter 2: Smart Contracts

"Setting something in stone" is a common phrase used to describe permanence of a promise or obligation. While there are numerous historical and sacred texts that deal with justice, tort, and commerce, one example illustrating the confluence of permanence and clearly defined obligations etched in stone comes from Mesopotamia. The Babylonian Code of Hammurabi dates back to roughly 1772 BCE and consists of 282 laws. While the famous "eye for an eye" (*lex talionis*) is inscribed on surviving clay tablets, roughly half of the code deals with contracts involving payment of wages, rent and liability for damaged property. Other clay tablets from Mesopotamia record interest-bearing loans and debts. While the interpretation and enforcement of these obligations is a matter of speculation and historical restoration, the human endeavor to codify duties and responsibilities is a never-ending story.

A more recent example, contrary to common belief, Samuel Goldwyn actually said, "his verbal contract is worth more than the paper it's written on."[24] Yet either way it is stated, Goldwyn's oft misquoted catch phrase illustrates one of the core issues that continually impacts property law and rivalrous resources: how to create clearly defined terminology, guidelines and terms of service in a reliable way.

In 2006 Nick Szabo, the progenitor of the idea of cryptographic contracts, compared humankind's current analog spectrum of decision making to a digital system to describe the differences between "wet code," which is interpreted by human brains and "dry code" which is interpreted by computers.[25] In contrast to the seemingly binary logic of machine language, even though contracts, rules and regulations may be written by ostensibly objective parties, they must still be interpreted and enforced by yet another party or parties of humans. And as a consequence stipulations do not always go as they were originally delineated. This may change however as Szabo also described how computer programs have been and will continue to slowly edge towards mastering different niche domains that reach farther into "wet code" – into the human realm of nebulous obfuscation, fickleness, inconsistency, and abuse. This is the subject of disagreement in this manuscript and will likely continue to be in the near future.

What is safe to say is that smart contracts and cryptoledgers are not a silver-bullet panacea solving ambiguity in human interactions beyond the reach of the algorithms. According to its latest biannual arbitration scorecard, The American Lawyer's 2013 survey highlighted 165 treaty arbitrations and 109 contract arbitrations involving $121 billion in disputes, a record.[26] Similarly, Fulbright & Jaworski publish an annual Litigation Trends and Survey Report in which they survey senior corporate counsel regarding various aspects of litigation and related matters. In the latest survey they found that contract disputes in the US (44%) and UK (57%), remained the largest type of litigation pending against their company, followed by labor and employment disputes.[27] Aside from the famous fabricated contract from Paul Ceglia, few contractual disputes involve tampering of the actual contract in the developed world – more often than not the agreements are certain and the facts, or its meaning, are in dispute.[28] But as discussed below, smart contracts encompass the wider spectrum of formalized agreements, such as financial instruments (synthetic assets) or codified representations of value (e.g., tokens).

Automation in commerce is increasing daily. With the advent of NASDAQ in 1971, electronic securities exchanges have traded shares of stocks, bonds, and other instruments on a daily basis and in some cases continuously for twenty-four hours a day. This digital creation was made despite the fact that then-contemporary paper-based exchanges capable of trading similar instruments have been in use at least since the founding of the Dutch East India Company in 1602.[29] While there are numerous reasons for why the NASD built it, the primary motivating force for electronic exchange in general is that it provides

users with faster logistical and organizational efficiencies, much like electronic mail does compared with its analog counterpart; while simultaneously removing numerous intermediaries, middle men and 3rd parties though often they interpose new ones. While there are still hardcopies of securities (e.g., a share register) that in some cases must be maintained and on-file with governmental and corporate entities, in reality the instruments on all modern exchanges are just electronic bits that are representations – abstractions of various contractual obligations, conditions, and terms of service in the real world.

A smart contract is a proposed tool to automate human interactions: it is a computer protocol – an algorithm – that can self-execute, self-enforce, self-verify, and self-constrain the performance of a contract.[30][31][32] Whereas Bitcoin and its direct progeny are referred to as the "1.0" generation, as shown below, contracts, on "2.0" platforms – the next generation of cryptocurrency, are able to enforce themselves.[33] They do not have a physical enforcement arm the way legal contracts do.[34] Rather, because they embody complex contractual relationships in computational material, they move certain defined asset(s) automatically under certain conditions.

Twenty years ago, Nick Szabo used a specific name for some of these instruments: synthetic assets. Synthetic assets, in his words, "are formed by combining securities (such as bonds) and derivatives (options and futures) in a wide variety of ways. Very complex term structures for payments (i.e., what payments get made when, the rate of interest, etc.) can now be built into standardized contracts and traded with low transaction costs, due to computerized analysis of these complex term structures."[35] Today, both lawyers and software programmers have the ability to create these types of instruments.

Although some may have attempted to build *a priori*-based arguments against using such digital representations, post 1971, *a fortiori*, it has become clear that scarcity (a rivalrous asset in the economic sense) and value need not be solely represented by physical phenomena.[36] And while each individual has his or her own subjective valuation, some currently see that there is potential utility or even speculative value in holding, using, and trading these electronic financial instruments.

In Cryptoledgers We Trust

Decentralized cryptoledgers are another refinement and evolution of Szabo's 'wet-to-dry' system.[37] Paper-based ledgers and electronic ledgers are typically held and maintained by 3rd parties such as banks or clearing systems; these entities create a "trusted" environment that, the argument goes, could be abused and manipulated by human elements (e.g., changing content, destroying records, double-spending) and imposes considerable cost. When you trust a 3rd party, you are exposing yourself to the malfeasance of that 3rd party.

In November 2008, Satoshi Nakamoto – a pseudonym for one or several individuals – released a white paper that, for the first time, detailed a method for using a decentralized, encrypted software-based ledger that solves these 3rd party abuse and vulnerability issues. That white paper gave rise to Bitcoin.[38]

In contrast to the existing methods, argued Nakamoto, a decentralized cryptoledger called the Bitcoin protocol can serve as the sole middleman. As an algorithm the protocol is unbiased and capable of auditing, authenticating, validating, approving, and transferring integer values along a ledger that is distributed to tens of thousands of computers (called mining machines) that are located around the world. These computers run an open-source program that provides all of these aforementioned functions and they are rewarded for their work (seigniorage), by the provision of an integer value, a virtual-only token called a bitcoin (sometimes referred to as a "cryptocoin").[39] The Bitcoin ledger also

has other potential uses that have not been fully utilized such as the ability to manage smart contracts or any instrument, asset or token that can be arithmetically encoded into software. In fact, the upcoming version 0.9 release of Bitcoin will provide room in the ledger for each transaction (also called a *tx*) to include an additional 80-byte hash, just large enough to provide for a "distributed contract" – a feature that has drawn even greater outside interest over the past year due to its ability to represent any asset class or property, not just one value (fiat).[40]

In practical terms, the Bitcoin cryptoledger is its own 3rd party repository as it creates a consensus-based, trustless environment that negates the role of 3rd party intermediaries that existed in a paper-based analog world. It also acts as a decentralized timestamp database. Whereas historically timestamps were issued by a Time Stamping Authority (TSA) – or digital notary – that is vulnerable to abuse and tampering, a user can now store a timestamp on the ledger without concerns over data corruption as it stored on thousands of decentralized machines.[41] More to the point, it provides the abilities of many other functionaries (e.g., accounting, auditing) and institutions (e.g., data warehouse) thus making a multitude of middlemen entirely redundant and allowing for bilateral transactions to take place. Whereas Alice's Accounting Co., may take a quarter of a year to audit and reconcile accounts for Bob's Boutique Bookstore, a bitcoin transaction, as well as the entire global Bitcoin ledger, called a blockchain, is authenticated, verified, copied, and audited approximately every ten minutes (Litecoin is even faster, verifying every two and a half minutes).

While the underlying mathematics and cryptographic concepts took decades to develop and mature, the technical parts and mechanisms of the ledger (or blockchain) are greater than the sum of the ledger's parts. Simply put: bitcoins do not actually exist.[42] Rather, there are only records of bitcoin transactions through a ledger, called a blockchain. And a bitcoin transaction (*tx*) consists of three parts:

an input with a record of the previous address that sent the bitcoins;

an amount; and

an output address of the intended recipient.

These transactions are then placed into a block and each completed block is placed into a perpetually growing chain of transactions —hence the term, block chain. In order to move or transfer these bitcoins to a different address, a user needs to have access to a private encryption key that corresponds directly to a public encryption key.[43] This technique is called public-key encryption and this particular method, Elliptic Curve Digital Signature Algorithm (ECDSA), has been used by a number of institutions including financial enterprises for over a decade.[44][45] Thus in practice, in order to move a token from one address to another, a user is required to input a private-key that corresponds with the public-key.

To verify these transactions and movements along the ledger, a network infrastructure is necessary to provide payment processing. This network is composed of decentralized computer systems called "miners." As noted above, a mining machine processes all bitcoin transactions (ledger movements) by building a blockchain tree (called a "parent") and it is consequently rewarded for performing this action through seigniorage. Blockchain trees are simultaneously built and elongated by each machine based on previously known validated trees, an ever growing blockchain. During this building process, a mining machine performs a "proof-of-work" or rather, a series of increasingly difficult, yet benign, math problems tied to cryptographic hashes of a Merkle tree, which is meant to prevent network abuse.[46]

That is to say, just as e-commerce sites use CAPTCHA to prevent automated spamming, in order to participate in the Bitcoin network, a mining machine must continually prove that it is not just working, but working on (hashing) and validating the consensus-based blockchain.[47][48] At the time of this writing the computational power of the network is 200 petaflops, roughly 800 times the collective power of the top 500 supercomputers on the globe.[49]

To prevent forging or double-spending by a rogue mining system, these systems are continually communicating with each other over the internet and whichever machine has the longest tree is considered the valid one through pre-defined "consensus." That is to say, all mining machines have or will obtain (through peer-to-peer communication) a copy of the longest chain and any other shorter chain is ignored as invalid and thus discarded (such a block is called an "orphan").[50] If a majority of computing power is controlled by an honest system, the honest chain will grow faster and outpace any competing chains. To modify a past block, an attacker (rogue miner) would have to redo the previous proof-of-work of that block as well as all the blocks after it and then surpass the work of the honest nodes (this is called a 51% problem).[51] Each 10 minutes (on average) these machines process all global transactions – the integer movements along the ledger – and are rewarded for their work with a token called a bitcoin.[52] The first transaction in each block is called the "coinbase" transaction and it is in this transaction that the awarded tokens are algorithmically distributed to miners.[53]

When Bitcoin was first released as software in 2009, miners were collectively rewarded 50 tokens every ten minutes; each of these tokens can further be subdivided and split into 10^8 sub-tokens.[54] Every 210,000 blocks (roughly every four years) this amount is split in half; thus today miners are collectively rewarded 25 tokens and in 2017 the amount will be 12.5 tokens. This token was supposed to incentivize individuals and companies as a way to participate directly in the ecosystem. And after several years as a hobbyist experiment, the exchange value of bitcoin rose organically against an asset class: fiat currency.

While colloquially someone may say he or she has ten bitcoins, there is no physical or even digital object that is an actual bitcoin.[55] We are talking simply about the ability, by virtue of having exclusive knowledge of a given unlocking private password (a key) of a given schema, to cause a change in a ledger entry in that distributed schema. And because all the mining systems operate with clearly defined "dry" rules, through consensus they respect the ledger entry change. In other words, transferring a bitcoin is merely moving a specified integer value from one address to another address; all such moves are recorded on a public ledger. As a consequence, users can actually access, transfer, and "store" these tokens through numerous mediums including a digital wallet (accessible from a laptop, tablet, smartphone), through an online browser and even through air gapped, cold-storage techniques such as a "paper wallet" or USB drive.[56] Yet the actual ledger remains distributed amongst the mining equipment.

Another way to look at the Bitcoin system is through a thought experiment: try to stop using the word "property" to refer to the thing owned, the thing in which there is a property right.[57] Instead, talk about an owner of some owned thing – or resource. The owner has a property right *in* some owned thing – in some resource. So then ask: what is the ownership or property right in a bitcoin? What exactly is a bitcoin? You then have to carefully define what you mean. And of course it is not ownership of "a bitcoin" – since there can be fractional bitcoins (the smallest unit is called a satoshi). Economics does not have a category of "property," as it is the study of human actors and scarce resources. Property is a legally recognized right, a relation between actors, with respect to control rights over given contestable, rivalrous resources. And with public-private key encryption, individuals can control a specific integer value on a specific address within the blockchain. This "dry" code effectively removes middlemen and

valueless transaction costs all while preserving the integrity of the ledger. In less metaphysical terms, if the protocol is a cryptocurrency's "law," and possession is "ownership," possession of a private key corresponding to set of transaction (*tx*) outputs is what constitutes possession.[58] All crypto assets are essentially bearer assets. To own it is to possess the key. The shift from bearer, to registered, to dematerialized, and back to bearer assets is like civilization going full circle, as the institution of property evolved from possession to the registered form that predominates in developed countries today.

In terms of the logistics and mechanics of exchanging bitcoins to and from fiat, there are several methods. For large volume, over the past several years there have been several companies (BitStamp, Kraken, BTC-e) that have created web-based exchanges by which a user deposits a token and the exchange in turn is partnered with a physical bank in specific jurisdictions.[59] Once a user "sells" the token on the exchange, this bank then provides fiat liquidity to the exchange. Since the genesis block in 2009, approximately 12.4 million bitcoins have been mined, some of which are permanently lost (e.g., where a user has lost or forgotten the information comprising his or her private key).[60] As of this writing, the current market cap of all mined bitcoins is seven billion dollars; for comparison, MasterCard's current market cap is $125.24 billion.

Not a One-Trick Pony or One-Hit Wonder

With its decentralized, peer-to-peer abilities that allow for near-instant transfers and trustless authentication of value while simultaneously serving as a registry of all property ownership (titles) with an algorithmically controlled stable money supply, the Bitcoin protocol has several limitations.[61]

Since the initial release of Bitcoin, up until now, the protocol has not been natively capable of managing and tracking more than one asset class. For instance, three years ago, when ten thousand bitcoins were traded for a pizza, the token could have just as easily become pizzacoin.[62][63] That is to say, while value was exchanged, those using the blockchain could have attempted to track the value of pizza. Or more precisely, those using bitcoin as a medium of exchange (MOE) could have used pizzas as the unit of account (UOA) (e.g., when setting the bitcoin price of those alpaca socks, consult the bitcoin-to-pizza ratio).[64] Instead, the users of bitcoin consulted the bitcoin-to-fiat so fiat remained the unit-of-account as prices in fiat are generally used to measure the value of goods in the physical economy. Another way to look at this is, those using bitcoin could have treated it in a "colored coin" manner (see below); and conventionally each coin would have equaled 1/10000th of a pizza. As a consequence, it became clear that in order to begin tracking, trading, and managing smart contracts in a decentralized manner (and thereby exchanging smart contracts and even smart property), you were limited to just a few workarounds described below.[65]

How do we trade assets on the blockchain? Purely proof-of-work, blockchains present logistical problems. One choice is to build and maintain tens of thousands of altcoin blockchains that serve as ledgers for each asset. This in turn would require a hash generating network to verify and protect against double-spending attempts (i.e., the 51% problem). While there is no specific engineering reason that prevents this solution from being carried out (and perhaps it could take place through endeavors like Humint),[66] motivating the human element to build and maintain a mining network in a profitable manner could be very cumbersome. At the time of this writing there are several hundred different altcoins, most of which are mere line-for-line copies of Bitcoin or Litecoin – there are even automated tools that allow users to create their own clones, such as Coingen and Razorcoin.[67] Yet, despite the existence of these altcoins, their creators have thus far been unable to re-create the "network effect," which continues to back Bitcoin.

Another approach could be to build another layer, or platform, on top of a blockchain which specifically relates to an underlying reference asset. Of all the existing decentralized cryptochains in existence, the one with the most institutional momentum, merchant exchanges, and community involvement (both in terms of software development and user base) is Bitcoin. In economic terms this is called the "network effect." That is to say, the more people who use the network, the more valuable the network is. Other examples are social media sites like Facebook: the more your friends use it, the more potential value it has for you. Or with credit cards, the more merchants that accept Visa, the more useful and convenient it is for you.[68] While other altcoins (and altblockchains) may be invented, convincing a critical mass of user, merchant, and developmental adoption is a constant uphill battle. It should also be noted that first-movers are not necessarily the players that the market chooses in the long run. For example Diners Club was the first credit card; yet it was displaced by other participants and is relegated to a small niche today. Similarly, both Friendster and MySpace were the first funded companies in the social networking space, yet it was Facebook that became the industry leader. Kodak, Blockbuster, and Tower Records are also recent examples of incumbents that were unable to adapt to a different market landscape. In fact, the technology industry is filled with instances of disruptive innovations and creative destruction, including most notably RIM, which spearheaded the smart phone with its Blackberry concept but after mismanagement woes is now on the verge of bankruptcy.[69][70]

For the near future at least, Bitcoin is the protocol *du jour*.

While some efforts have focused on the above approach, projects like Mastercoin and Colored Coin have chosen to build on top of Bitcoin's blockchain, to use it as a verification and transportation protocol – allowing them to focus on building asset management tools instead of building an entirely new hashing infrastructure. Both of these projects have a different method of managing assets. Mastercoin issues its own token called a mastercoin (a type of metacoin) that can be bought or sold like a bitcoin on an exchange. On January 3, 2009, the genesis block for Bitcoin's blockchain was publicly released, laying the foundation for all other future blocks to build on top of.[71] Similarly, on July 31, 2013, the Exodus Address was setup for Mastercoin which the resulting framework is situated atop.[72] Only a limited number of mastercoins were created during the subsequent month of August and they are only visible to users that use a specially designed wallet that can distinguish them from the rest of the blockchain.[73] Despite some initial developmental hiccups, the community responded by providing 4,700 BTC ($5 million at the time) in crowdfunding.[74] These mastercoins in turn insert tiny messages into the blockchain that can be used to represent user-defined assets like a derivative or gambling bet. Special digital wallets and online tools are used to track, trade and sell these mastercoins to anyone around the world.

The Colored Coin project is a little different from Mastercoin in that a certain amount of Bitcoin (e.g., 0.001 BTC) are "colored" to represent a particular asset (e.g., green for a car, blue for a house, yellow for gold, pink for shares of stock). Users can then exchange these "colored" assets with one another using the Bitcoin blockchain as the ledger. For example, if you own a home, you could use 0.001 BTC (or any other arbitrary amount) to represent transfer and assign it a secondary attribute, the "color" blue or any other "color" to represent the character of the asset (e.g., a house).[75] You can then send and exchange this new blue token using a special digital wallet called the Chromawallet to a buyer who uses a similar wallet. Using an online exchange (or even decentralized exchange) the buyer can purchase your "colored" token with bitcoin or some other combination of "colored" coins. All of this is managed through the same ledger. The only intermediary in this process is the blockchain, which manages the tokens just as it would any other bitcoin.

While there are several other projects with similar abilities on paper (NXT, Invictus Innovations, Counterparty), they all share a main goal: to allow a decentralized cryptographic ledger (a blockchain) to serve the roles and functions that had previously been managed by numerous 3rd parties. While it is unclear which of these, if any, will be successful, the full implications and applications of trustless asset management are spreading more widely into the larger software development community.

For perspective I contacted Mike Hearn. Hearn is a core Bitcoin developer who recently left Google to work on the protocol full-time.[76] He also has spearheaded the effort to enable smart contract functionality with the protocol, designing several codebases and use-cases for future development. In an email exchange I asked him if he thought that smart contracts would initially be limited to financial instruments. In his view, "well, 'contracts' in the sense Satoshi used them are about Bitcoin and Bitcoin is inherently about finance so yes, I think they will be restricted to finance."

And what kind of application does he think could bring cryptocurrency to a wider audience? "That's the million bitcoin question isn't it. I don't know. There might not be one killer app in particular, but a variety of apps that are merely useful enough that everyone has a bit of Bitcoin lying around for the occasions when they need them. I explored micropayments last summer as part of trying to answer this question."

Due to fees set by traditional payment processors, microtransactions have been an area that was financially difficult to do until Bitcoin, which permits divisibility to the one-hundred millionth decimal place (and virtually farther if patched in later versions). Many off-chain wallet and exchange solutions such as those at Coinbase and Circle enable users to exchange bitcoins at this granular level. An off-chain transaction is one in which the movement of value (e.g., an asset) takes place outside the public blockchain. That is to say, initially users sent bitcoins to one another directly through the blockchain, this is called an on-chain solution. However, now Bob can send bitcoins from any of his wallet to his friend Alice who may be using a hosted wallet at an off-chain provider such as Coinbase (a trusted 3rd party). Or in other words, Bob's tokens first go to a Coinbase on-chain wallet which is synched to the public ledger, but then using an internal database, the representations of these tokens are divvied out to a specific user within Coinbase's internal off-chain wallet system. There are trade-offs to using each approach. While on-chain solutions such as Blockchain.info are reliable and cannot be exploited by a 3rd party, trading and exchanges are conducted in the 10 minute time frames (due to blockchain speeds). Yet readers should be aware that while there are advantages of using a trusted 3rd party situation (namely speed and microtransactions below the dust limit), it could also result in the total loss of tokens as illustrated by the Mt. Gox fiasco in which thousands of customers potentially lost all of their holdings.[77]

Similarly, Hearn and others have discussed how in the near future, a mobile device (smartphone, laptop, tablet) could pay for wireless access with random WiFi hotspots via Bitcoin-based micropayments. That is to say, one of the problems with the current wireless infrastructure is that there is no automated, secure manner for strangers to use wireless hotspots without having to trust one of the parties, which could lead to abuse (e.g., credit card fraud). If instead, if Alice's WiFi router was enabled with Bitcoin functionality (i.e., had a built in wallet) then Bob could pay for usage via bitcoin – even as little as a fraction of a cent's worth – and both parties could be satisfied.

Assurance Contracts

But are there practical, present-day uses for the technology which are not contingent on some hypothetical future blockchain gaining widespread acceptance? Alexander Tabarrok, an economist at George Mason University and creator of the "dominant assurance contract" model and I exchanged emails in part of my initial exploration into the real-world applications of smart contracts.[78] An assurance contract is a contract in which contributions to a group goal are held in escrow until the amount reaches a certain threshold, after which point the contributions are then released (e.g., crowdfunding via Kickstarter). This has been discussed as an alternative model for funding public infrastructure (e.g., a lighthouse, water treatment plant, roads, or bridges) and consequently its objective, binary funding model has frequently put it in the spotlight as a relatively easy example for smart contract developers to encode. The "dominant" version is a twist in that if contributions fall short of the threshold, those who contributed not only receive their original funds, but also a bonus – creating an incentive for many people to donate. Tabarrok writes:

> I see smart contracts and the internet of things as ending the problem of asymmetric information. In economics, asymmetric information problems occur when one party to an exchange has better information than the other party and out of fear of being exploited the lesser informed party backs out of the trade. Both parties lose since no trade occurs even when trade would be mutually profitable. Smart contracts and the internet of things can overcome many of these problems by making information revelation more credible and even by making trade conditional on information that neither party may even know!
>
> Capitalism like science and technology is a dynamic system and no one can predict where it's going to go. I expect only to be surprised by the uses people will find for dominant assurance contracts. Kickstarter and other groups have made assurance contracts more familiar (you only pay if enough people join). Dominant assurance contracts make a Kickstarter-like proposition even more compelling (you only pay if enough people join and if not enough join *you* get paid). I hope to see experimentation and eventually I hope that familiarity in the private realm will encourage people to experiment with DACs to fund public goods and government services which was my original motivation.
>
> The big, immediate gain of using cryptocurrencies and cryptoprotocols is quite pedestrian, lower transaction fees. Our payments technology is expensive and cumbersome. This is true for credit card payments, dominated by a handful of firms, and even more so for the government run checking system which is basically a 19th century system. Transaction costs are not sexy but there are a lot of transactions in the world and there are many billions to be made by improving the system. The company that first cracks the transaction cost nut, and I think that will mostly require reputation and scale rather than new technology per se, will be for payments what Google is for advertising. Big advances in the technology of asset management and banking, the sexy stuff, will come after and on the back of the billions made by reducing transaction fees.

A DAC is a decentralized autonomous corporation, an AI entity that performs the functions of companies (e.g., payroll, issuing dividends) and is discussed at length in chapter 5. There are several civic crowdfunding platforms that have been launched over the past couple years including Citizinvestor, neighbor.ly and ZenFunder.[79]

Legalese Challenges

Implementation of DACs, however, is not without its problems. In view of this I spoke with Stephan Kinsella, a patent attorney, author and Bitcoin investor "while there seems to be potential with cryptocurrencies, cryptoprotocols and smart contracts in general, in my experience the legal industry changes at a glacial pace. Many if not all of the segments are highly regulated and filled with well-established incumbents especially those integrated with banks. As a result, most clients and partners typically like to continue utilizing traditional services and solutions and thus are very resistant to innovation. Similarly, letters of credit and dispute resolution boards have existed for decades so this is not necessarily a selling point. While there are theoretical advantages to using independent arbitrators or escrows, many contracts for property ownership or car ownership already set up a system of clauses where parties choose an arbitrator or how to use an escrow. For instance, in terms of percentages, even when disputes arise the amounts of parties that ultimately use an escrow are quite small. Though, perhaps with enough buy-in this could change later in time." [80]

The problem, in his view, is that cryptocurrency is competing with an existing legal and commercial transaction infrastructure. "Again, while smart contracts present a very efficient and optimized marketplace, educating a userbase will be a constant uphill battle because in some ways you may have to reinvent the wheel; or recode the wheel as it were. For instance, to hedge against a breach of contract Bob may have to issue a $1 million bond to cover insurance. And in the event that this happens, you would likely need to work with a 3rd party who will have to look over the evidence of the case which in turn adds cost to the transaction. Sometimes if a deal continues to sour, Bob will sue or simply write-off the loss. Yet these types of interactions can and will likely happen despite using cryptoledgers. Furthermore, while cryptoprotocols offers many methods to constrain governance, such as title management I do not see why banks would rewrite their system for this service any time over the next several years.[81] They are typically risk averse and conservative. In fact, I still see legal contracts with provisions that were written decades ago – even over a century – because they withstood legal scrutiny. While smart contracts in theory could provide similar provisions, proponents and developers of next-generation crypto platforms should be aware that it will take many years of continuous education to convince businesses to adopt this different framework."

According to Kinsella and others I spoke to on this matter, the smart contracts which would give rise to the fewest problems would likely be narrow contracts covering easily quantifiable, fungible commodities (e.g., oil, metals, ore, agriculture) or simple services, such as those provided by auto-repair shops and beauty salons – that is to say, something that is objectively measurable, mechanical and consistent, and low on consumer protection or complex representations and warranties. While Bob and Alice would need to be aware of the various jurisdictions that provide different guidance and policies regarding the licensure of services (e.g., cosmetics, accounting), cryptoledgers and trustless asset management could enable a frictionless environment for bartering. Decentralized exchanges that can manage cryptotokens could allow local service providers to buy, sell, and trade in-kind without going into fiat. [82] While the tax and regulatory implications will unquestionably be different depending on the jurisdiction, this type of "cryptobarter" system may become useful and socially empowering in countries with faltering monetary institutions – like Argentina or Greece.

Argentina

In February 2014 I spoke with Wences Casares, an Argentine native and creator of a Bitcoin wallet used by institutions. He recalls, in his youth growing up "in Patagonia I remember when we had so much inflation twelve years ago that my mother would carry her salary around in plastic bags and spend it as soon as she got it. She would go to a market and there were workers whose sole job was to replace the

sticker prices many times throughout the day because the price levels soared." In addition, Casares noted that at the national level, "the government did not want to raise taxes or lower spending so they printed more, causing inflation. And when I talk to others about Bitcoin throughout the day I use different analogies depending on the person's background. Yet when I describe how Bitcoin works to Argentines, they figure it out very quickly. They realize it cannot be confiscated and can be used as a store of value."

Between 1998 and 2002, the Argentinian economy shrank by 28% as measured by GDP.[83] At the end of 2001, the national government defaulted on $132 billion in debt and inflation reached a monthly high of 10.4% in April of 2002.[84] Simultaneously the unemployment rate reached 20% by December 2001 and remained near 25% the following year all the way into 2003.[85] While subsequent administrations reversed several of these policies, including restructuring external debt, in 2008 the Argentinian government nationalized private pension funds, amounting to $30 billion in private savings.[86]

Based on his experiences, Casares says that "when I have helped process face-to-face Bitcoin exchanges in Argentina, when you look at the other side of the transaction these users are not hackers or geeks, they are common people who see it as a good store of value. Many in fact do not have much in savings but see how Bitcoin cannot be inflated. People with significant amounts of money can easily move into hard assets yet those at the bottom, the common person cannot. Bitcoin helps them and I imagine will continue to do so in the future. There are a lot of benefits of Bitcoin, different people latch onto different benefits yet if another similar inflationary event happens, because of the proliferation of mobile phones it could catch on like fire."

Sebastian Serrano, another Argentine native and founder of BitPagos, a virtual currency merchant payment service provider, expresses similar sentiment based on his first-hand experiences, "In Argentina there was a big wave of bartering that began in early 2002 whereby people traded food, services, almost anything at *ad hoc* fairs.[87] During late 2001 through 2002 the peso was in free fall and there was a large increase in unemployment, which motivated people to trade things for things. In fact, a few months into this crisis, many fairs and bartering clubs were already issuing their own 'credits' and creating their own bills as a form of scrip.[88] Eventually a federation was created that issued a general note, yet counterfeit of this credit became a big problem. As the economy recovered, the need for these clubs diminished and people stopped going to them – and while a few may persist, most completely shut down. Yet I think cryptocurrencies and a decentralized asset management system would have helped with this barter system out substantially. Not so much for price discovery but rather to prevent fraud because many of these fairs suffered from counterfeit notes and lack of transparency on how the notes were issued or distributed.[89] And I think we are a few iterations behind something like a smart contract-based system that could be used in a scenario like that. And perhaps these new platforms being developed will help in the long-run, because contracts make sense when time is a factor. Thus, it is going to be very interesting to see how this develops again if we have another financial crisis."

In 2013 the Argentinian peso lost 25% of its value relative to a US dollar and to stem capital outflows, Argentine policymakers enacted strict capital controls.[90] As a consequence, ordinary people lacking in political clout have had difficulties in protecting their peso-based savings because access to foreign currencies is restricted. While there is a fledgling Bitcoin community in Argentina, there are few formal outlets to exchange pesos to bitcoins or other cryptoassets that can provide a store of value resistant to inflation.[91] Trustless asset management could enable ordinary people to, instead of relying on the local currency (e.g., peso) to exchange goods and services, exchange their services via different cryptotokens.

Such a system, if implemented, would be a more accurate rendering of the Big Mac index.[92] The Big Mac index is an annually published currency-comparison tool created by the *Economist* that measures the purchasing-power parity (PPP) of each country. That is to say, a Big Mac is a relatively consistent, quantifiable good that irrespective of jurisdiction should cost the same relative to the local currency. However, since 1986, due to internal monetary policies a Big Mac is visibly overvalued or undervalued relative to chained US dollars. While merchants and entrepreneurs do not necessarily need to know every available global price point for haircuts, oil changes, or even in-flight training these indices could help provide price discovery, enabling Argentinians to trade their goods and services at roughly market-rate prices without using local currencies. In fact, just as globalization acts as to arbitrage wage rates of low-skilled employment between regions (i.e., *ceteris paribus*, the process of making textiles should cost roughly the same irrespective of locality), ultimately a decentralized system could enable entrepreneurs to coordinate economic investment to or from certain regions.

In one speculative example, Bob the mechanic in Buenos Aires could create a variety of "colored" tokens to represent tune-ups, repairs, and oil-changes and place them on decentralized exchanges that track those specific services. Alice from the suburb of Avellaneda is an airline pilot and could similarly create tokens to represent certain amounts of flying time (e.g., two hour in-flight training) and also place the tokens onto a decentralized exchange. Each exchange could list both the local rate for service (i.e., what the supplier is charging in fiat) as well as various cryptocurrency rates. While inflation may erode purchasing power of fiat currencies such as the peso, decentralized platforms could enable both goods and service providers the ability to retain and exchange value in a decentralized manner that negates the need to use a repeatedly devalued intermediary. Alice and Bob could use price-matching services to transfer service tokens directly redeemable for the said service to one another, or even exchange for other intermediary cryptocurrencies. To exchange between specific cryptoledgers, a consensus-based DAC may require "smart contracts" to provide for escrow and arbitration mechanisms before contracts are allowed on a ledger or exchange. Or users may be willing to accept contracts without such clauses (i.e., caveat emptor), helped along in their commercial decision by independent decentralized autonomous agents which could provide a feedback, reputational mechanism (e.g., credit score) to allow market participants to see whether either Alice or Bob is a risky merchant.

But what a cryptoledger makes up in quantitative sophistication, it lacks in the qualitative – bartering in times of economic stress might work, but a real consumer economy might not. According to Stephan Kinsella, "tens of thousands of formal and informal contracts are used every day between individuals, small companies and large institutions – and each of these may contain different nuances and subtleties relevant to the local setting. Even hiring someone to be a temporary assistant may require qualitative language – some formalized legalese – and it will be difficult to automate those things. In fact, most contracts outside the financial industry may not have clauses that are entirely mechanical; thus while smart contracts and cryptoledgers create a full-proof method of tracking ownership of assets, more than likely in some instances you will still need judgment calls involving humans – and there is already a subsidized public system in place for that which many market participants may be reticent to give up.[93] Thus not only do you have to provide educational outreach but also consumer buy-in."

Another question that both Stephan Kinsella and Sean Zoltek (chapter 6) brought up: how do we inform market participants that the benefits and advantages of switching to a new system outweigh the costs of using the existing infrastructure? For instance, homeowners in many developed countries can already sell property without a realtor by using websites. Similarly, homebuyers can purchase a deed and register it themselves. And if you want to sell it quickly you can simply use a real estate agent. Furthermore, while apartments, condos and townhomes are typically homogeneous units, not all houses are fungible, as they usually have some unique attributes that need to be quantified. While this

may be a small technical challenge that can be overcome, proponents should be aware that some consumers (or homeowners) may be uninterested in quantifying their assets via programmatic contracts.

Outside perspective

While much of the current literature, both academic and software development, is typically written for a US-based audience, I spoke with Preston Byrne, a fellow at the Adam Smith Institute and a London-based securities lawyer. In his words, "the smart contract as envisioned by Nick Szabo does not yet exist. When it does, it will need to incorporate substantially all of the legal elements of a traditional contract and express them in the functions it performs automatically, at least to the extent that it is written to do so. It may be possible for a degree of modularity to be built into the code so, e.g., specific terms recognised at law could be reflected in code (provisions relating to termination, for example, on the occurrence of specific events) and standardized for use across different transactions."

In Byrne's view, while not impossible, drafting commercially viable smart contracts will not be easy – and code alone will not be sufficient. "If a contract is a negotiated agreement which (in the event of a dispute) a court can enforce, a smart contract is a contract which enforces itself. Contracts are governed for the most part by (1) agreed rules and (2) a set of very complex legal fictions which govern how those rules should apply in the circumstances. For example, in English law it is required for any contract that is formed to incorporate an agreement of some kind, an actual transfer of value moving from both parties and the intention to create legal relations between them. In the event of a breach of the agreement or its being rendered voidable or void, they have a number of remedies – rescission, for example, where the contract is rendered void ab initio, specific performance, where a court orders one party to do something it had covenanted to do, and (more usually) damages compensating the injured party for loss. While sometimes parties to a commercial contract will be able to recognise when a breach or other misfeasance has occurred and sort out the appropriate remedies between themselves, ultimately the final arbiter of (1) what the contract means and (2) what the consequences of particular breaches will be lies in the hands of a court or arbitrator which has the ability to bind the parties and coerce them to its will. Contracts mediated entirely by distributed, pseudonymous blockchains by fully autonomous DAOs are not well suited to this role." This is an issue that several individuals discussed in the evolution of this manuscript. If the theory is there, where are the smart contracts? Ignoring the hype and handwaving, the main obstacle is the technical codebase and complementary support services that need to be implemented – the infrastructure needs to exist to allow for smart contracts to fulfill the functions described by Szabo and Byrne.

Some sources have explained it is nearly impossible to remove all human interaction in commerce - therefore why bother with using a cryptoledger system? Byrne argues that there will nonetheless be advantages beyond reducing transaction costs that lenders will be interested in – and only when cryptoledgers become more widespread in large organizations will smart contract technology become of practical use. According to Byrne, this should not take long: "corporates and financial institutions have high overheads for personnel and equipment. They automate their operations when they can. The idea of replacing complex server architecture with a distributed blockchain – if indeed such a thing can be done – seems to me to be a rather simpler and more elegant solution for a bank to manage its balance sheet than legions of employees. A blockchain is basically the world's most transparent and accurate accounting product. It's only a matter of time before proprietary blockchains crop up internally at financial institutions, governments and businesses where it will start serving that function. Consequently, the resources saved - currently used to pay salaries of financial services professionals - will be redeployed into lending operations and the economy at large."

"In a similar fashion," Byrne argues, "governments could do the same thing with their own finances and practically everyone would benefit. In the UK the public sector pay bill is £167.5 billion a year - 25% of state expenditures, 12% of GDP, and £3000 per year for every man, woman and child in the country. [94] The UK could create a state-backed cryptocurrency - cryptosterling - tomorrow. Just write it, ensure only the Bank of England can mine it, issue everyone in the country with a private key, trade it for cash and deposits on a 1:1 basis over six months and replace national insurance numbers with a metal card containing the corresponding public key. Paying salaries and taxes, and claiming benefits, would be as simple as scanning a QR code and a bit of online monitoring; we could abolish the welfare bureaucracy overnight and save vast quantities of expenditure."

"Such a currency would be superior to any other form of legal tender," Byrne says: "imagine being able to see every transaction conducted globally in sterling in real time, all while possessing the benefits of any other crypto, including security, transparency, speed, irreversibility, and low cost. It would also have the benefit of being able to be tinkered with as the state would control the majority, if not all, of the hashpower on the network and have knowledge of at least some of the private keys. This is useful, for example, to reverse proven fraud, rescind a contract or engage in quantitative easing - arguably things any state needs to be able to do in order to maintain civilisation."

He adds, "I am aware there are those who will howl that this is not what Satoshi intended, and that this will result in a state which has absolute control over the money supply and the ability to interfere with personal finances mediated by the official blockchain. I agree. However, advanced states have this capability already – we are just paying hundreds of thousands of bureaucrats to exercise it. Plus, nothing about a state-backed cryptocurrency prevents us from trading out and using some other cryptocurrency of our choice (e.g., dogecoin). If cryptocurrency is to take off we need to start thinking in these terms."

Byrne's proposal of replacing sterling (GBP) with a sterling cryptocurrency which provides unforgeable transparency is already being experimented with in Iceland with the new Auroracoin initiative.[95] The team behind the project 'pre-mined' (created) 10 million Auroracoins (AUC) and no more will ever be made. The creators of Auroracoin plan to give every citizen of Iceland 31.8 AUC on March 25 as a transparent mechanism to mitigate against a future banking crisis. Similarly, the Mazacoin project is working with the Lakota Nation, a Native American tribe, to create an alternative cryptocurrency that can "give native American communities some fiscal autonomy."[96] While it is unclear what changes to the regulatory framework will occur in each jurisdiction or if market participants will adopt and utilize these tokens, this space will likely grow with other such experiments over the coming years.

Byrne also sees other developmental issues arising from breach of contract and thinks that one particular problem stands in the way of integrating cryptoledgers with repayment prioritization: what he calls 'trusted 3rd party dogmatism.' In his words, "There is currently very little dialogue between cryptocurrency advocates, mainstream financial institutions, and governments on cryptocurrency's role in the economy – developers and libertarians are working furiously on one side of the rift and government, institutions and corporations cautiously observe from the other, and both size each other up – as if getting ready for a fight."

"Given that cryptocurrency technology was ostensibly designed to wrest control of commerce from banks and the state," Byrne adds, "this state of affairs should not be a surprise. The result of this dichotomy, however, is that there is a disconnect between the banks who mediate transactions in the real economy and the cryptocurrency which seeks to supplant them. This is counterproductive; the technology is open-source and can benefit everyone, including the banks. But the gulf, until bridged,

will act as a serious hindrance to development. Take the idea of an asset-backed (secured) peer-to-peer loan as an example, where the borrower borrows in cryptocurrency and also collateralises the loan with cryptocurrency. Talk to a cryptocurrency advocate, and he sees an opportunity to write a smart contract protocol that disintermediates a bank, avoids taxes and allows him to earn a little cash on the side beyond the reach of the revenue authorities. Talk to a bank at the moment, and they talk about money laundering, terrorist financing and regulation. It doesn't have to be like this."

In his view, the solution is to reintroduce the trusted 3rd party (TTP) in a highly reduced but nonetheless essential custodial role. "Let's return to that asset-backed peer-to-peer loan for a minute. For a bank to write that loan, it would normally negotiate an agreement on certain terms, take security over the assets concerned, and submit to a set of complex legal rules. As Szabo noted:

> 'Over many centuries of cultural evolution has emerged both the concept of contract and principles related to it, encoded into common law. Such evolved structures are often prohibitively costly to rederive. If we started from scratch, using reason and experience, it could take many centuries to redevelop sophisticated ideas like contract law and property rights that make the modern market work. But the digital revolution challenges us to develop new institutions in a much shorter period of time.'[97]

Continuing, Byrne notes that, "Szabo correctly points to the fact that the common law is a very complex body of rules. He is also correct in that any smart contract we draft will benefit greatly by following its example. Cryptocurrency will benefit more, however, from interaction with the law than attempting to replicate a parallel legal system of its own. The primary, and one might say defining, characteristic of the English common law is that it was not, at least historically, made primarily through legislative fiat. Its evolution has been organic, with existing rules changing to new circumstances in the face of new and ongoing testing (litigation) – it is a form of transductive algorithm. For example, the law relating to guarantees is notoriously complex because guarantors almost always have an economic interest in challenging the legitimacy of the instrument when the contract is called in, meaning that the rules are very specific and great caution must be exercised when drafting them."

A transductive algorithm is inference from specific experiences and is a technique used in machine learning.[98] Or in other words, being taught (or learning) about specific cases by which the knowledge can then be used for future cases in a similar domain. And as Byrne suggests, it may take some time for the legal framework to organically form around cryptocurrencies, through a similar process.

Continuing, "Even in simple agreements, however, a hard rules-based approach – as an outsider to bank lending and law practice might perceive it – is far from the norm. Law is 'wet code' not by mistake but by design. Returning again to an asset-backed loan, let us suppose that this loan enters into default. In the real world it is possible for one party to forbear from exercising its rights, or to seek a situation-specific solution which fits the facts on the ground. Even if a loan is in default, it may not be in anyone's interest to formally call it and enforce. In my experience enforcement is an extreme solution; it is, however, the final remedy on which all faith in commercial contracts is based. Coding smart contracts that make a role for TTPs who can be reasonably relied upon to act fairly, and have adequate resources or insurance so that if they breach their obligations they're still worth suing, is a necessary step if cryptocurrency is to be adopted by the mainstream. To do that, however, the cryptocurrency community needs to get over its ideological aversion to governments and banks and start selling to them."

While his proposal will likely receive a mixed reaction, he sees this evolution in terms of the existing role of a 3rd party. In his view, "taking the asset-backed loan as an example again, let us suppose there are multiple lenders. Usually those lenders will enter into a contractual arrangement with an agent or trusted 3rd party, another bank or a professional trustee company, to hold and exercise their rights, at their direction and on their collective behalf. This arrangement works because (1) the common law allows the lenders to contract with that TTP on certain terms and (2) the parties know where to find the TTP if it screws up."

In Byrne's view, once a trusted 3rd party is removed from simple transaction of the kind in the style proposed by Nick Szabo, such an agreement differs from a contract concluded in the normal way in that:

> 1) "the TTP and its associated costs are disintermediated and users become independent of existing institutions; however,
>
> 2) "the price of decentralisation is full cash collateralisation, making even the most basic lending contract unviable for ordinary commerce;
>
> 3) "the element of discretion to hold our rights in abeyance and adapt to changed circumstances is limited by the algorithm; and
>
> 4) "in all likelihood, the possibility of enforcement for losses which arise beyond the provisions made in the smart contract itself will be compromised, because
>
> > (a) by design, the technology doesn't permit this course of action (as a party who would be liable for, e.g., consequential loss would almost certainly not hand over his private key in circumstances where his liability would increase); and
> >
> > (b) even if one could present the contract to a court and trace all of the relevant assets, reintroducing a contract to the legal system when it was intentionally structured to exist outside of it does not tend to work out well for the party seeking to rely on its provisions."

This is an issue that numerous reviewers of this manuscript asked: for digital contracts, how is the problem of real life enforcement solved? After all, even if things are enforceable on the blockchain, a human still has to input the conditions for which contracts will be executed, and if anything happens in real life, it still has to be enforced by lawyers and the state. However, there is no clear cut answer to this and each jurisdiction will likely react in different ways: from acceptance to outright banning.

Yet Byrne sees only one solution: invite 3rd parties back into the equation.

As Szabo said, "by extracting from our current laws, procedures, and theories those principles which remain applicable in cyberspace, we can retain much of this deep tradition, and greatly shorten the time needed to develop useful digital institutions."99 To Byrne, this means that while "a technical understanding of jurisdiction specific legal principles is absolutely essential to smart contract design, trying to encode the sophistication of common law into an algorithm is impossible – see, for example, the Eurosail-UK 2007-3BL case, where ambiguity relating to the statutory consequences of a purely mechanical provision, which in all likelihood nobody expected would ever be invoked at the time the

contract was entered into, had significant consequences for an entire industry. Reifying agreements in code and pushing for full decentralisation will create more commercial problems than it solves."

Byrne thinks that the tradition can be easily retained and employed if it is applied, "the way in which this will be done is by ensuring smart contracts keep a foot in the real world. We would still see a paper contract specifying what is reserved for the blockchain and what is not - automata are well suited to matters like collections, cash sweeps, swap payments and collateralisation, managing and blocking 'accounts' (query, if a blockchain is used, whether the need for accounts could be dispensed with as well), payment prioritisation, and even servicing issues such as title transfer on enforcement, as Nick Szabo has suggested (e.g., in the case of securities backed by a pool of automobile loans)."

"The role of an individual contract's sole TTP," he continues, "could be limited mainly to holding the private keys on trust and in confidence for the parties pursuant to the terms of their contractual agreement, leaving the rest to the machine, only intervening to exercise the critical discretion when things go horribly wrong – granting flexibility for complex situations involving insolvency, recovery of uncontemplated losses, and changes in the law such as reference currency re-denominations. This human element which is held in reserve is also what would permit judicial control of the transaction." However, Byrne added, "to move things forward on this front, computer programmers need to start talking to lawyers and bankers. This is not to say that this would prevent anyone from using the technology outside of the legal system. It is only to say that in order to mature, the technology will need to maintain some connection to the legal system and submit to its jurisdiction."

While it is too early to tell how this intersection will play out in the United States, it will likely fill volumes of books over the coming decades. In the meantime there are several cases currently being litigated that involve cryptocurrencies, including one concerning a Johns Hopkins doctor who sold prescription pain pills (oxydocone) through Silk Road – an anonymous marketplace that is largely known for its illicit drug trade.[100] Similarly, Alydian was an ASIC mining company that went bankrupt and during the bankruptcy proceedings, the judge raised some questions that nearly all other jurisdictions will have to become familiar with: What is a token? What is a cryptoledger? Does it exist, and if so, where? Can it be controlled or rescinded? And so forth.[101]

And in Byrne's view, there will likely emerge a balance that companies and institutions each come up with in terms of how integrated their operations will become with math, algorithms and cryptoprotocols – "a 'balance of trustlessness,' if you will. I think for most contracts of a large, capital-intensive nature (securitisations, corporate lending, corporate acquisitions, asset and property purchases) smart contracts will ensure they fall within legal jurisdiction in order (1) to better assess and mitigate commercial and counterparty risk and (2) to create a nexus with real-world assets which can be enforced against – the market will demand it. The courts will develop an interpretive framework to compel people to turn over these assets. If a trusted 3rd party knows the private keys, a central agent can control them and give effect to court orders. The same is true for a government body using the technology, which in its hands should remain subject to both judicial and constitutional control."

Chapter 3: Next Generation Platforms

As innovative and groundbreaking as Bitcoin has been, it has several known technical limitations.[102] Simultaneously, the current development team is hard at work on priorities revolving around improving the security of the protocol from vulnerabilities and exploits.[103] This is not a criticism of their activities and actions, especially in light of the transaction malleability issue that caused frenetic activity within the ecosystem during the middle of February.[104] Other developers in the community have tried to assume the mantle of responsibility for improving the functionality and capabilities of this space. Some projects involve fusing exoskeleton systems built around the Bitcoin protocol; others create their own independent ledgers; still others have even created bridges between Bitcoin and other ledgers.

Below, I introduce eight projects that are currently developing a mechanism to design and transport smart contracts or smart contract functionality.[105] For each, I attempted to interview the main developers.

Colored Coins

As noted above, one way to utilize a crypto blockchain to verify wares is through a process being developed called Colored Coins.[106] In a nutshell, this endeavor allows users to "color" a token to represent a specific asset such as a car, home, boat, commodity, a share, a bond – virtually any type of asset (e.g., 0.5 BTC colored green to represent your home). These tokens can then be exchanged, just like bitcoin tokens, by anyone anywhere. This enables a decentralized, trustless form of asset management that uses a blockchain as both a ledger and transportation mechanism.

Alex Mizrahi, who is leading the development of the Chroma Wallet used by the Colored Coins project says that "it is going to be very easy for the asset management industry as a whole to use Colored Coins.[107] For example, some of the first places we are going to have adoption will likely be real-estate and portfolio management. In fact, for any type of asset management it's going to be simple to issue his own color that represents his goods. A portfolio manager can issue one color that represents a portfolio of stocks backed by the real holding and sell it globally. If he is savvy and his products are good, his colors are going to have demand. So transferring ownership is very easy, quick and safe — just like bitcoins. In the real estate industry someone can issue their apartments using colored coins and have them float on the blockchain, or manage time-sharing based on color."[108]

Meni Rosefeld, another member of the development team, described several of the advantages of using a secondary attribute (color) within the asset management industry. "The greatest advantage is the removal of barriers of entry. Currently, new businesses wishing to raise capital use cumbersome and inefficient private deals; and those aspiring to be listed in order to allow for the market to valuate them with an efficient mechanism, can only do so with a great expenditure. With colored coins, anyone can easily raise funds in exchange for equity, removing barriers of entry, encouraging innovation and allowing society as a whole to better allocate its resources between ventures."

One area of confusion within the Bitcoin community is the misplaced understanding – that centralized servers are needed to issue and track a secondary attribute (the "color"). According to Rosefeld, this is incorrect. "No centralized servers are needed for tracking – this is done in the decentralized network of the host currency (such as Bitcoin). There does need to be an entity issuing each particular colored coin – however, an entity raising funds for a generic purpose is not usually in the business of running an exchange. Without colored coins, they would have to resort to a large 3rd party exchange with all the

usual problems of barrier of entry (for both issuers and exchanges) and vendor lock-in. With colored coins, they can outsource the tracking and exchange to the efficient decentralized network. The issuer is only involved when issuing or recalling the coins; investors can then trade the coins between themselves without involving any 3rd party, which has implications for privacy, efficiency, and the kind of advanced transactions one can do."

I also spoke with Amos Meiri, head of dealing at eToro, another member of the development team for the Colored Coins project.[109] I asked: would it be easier to simply conduct all trade privately at the centralized exchange where it will be more scalable and private. In his view, "Centralized exchanges definitely have their advantages, but colored coins can be useful for following reasons. First, users do not need to trust their bitcoins to a centralized exchange. Companies cannot manipulate ownership records (to commit fraud, for example). So basically, if somebody gives you an IOU, it isn't a good idea to leave it with the person who issued it or to affiliated parties. Another reason is that companies cannot control how its shares are being traded, thus it cannot block trade. And lastly, there is no need to maintain servers or manage security due to its integration with the blockchain."

While this is obviously easier said than done, as noted above, this idea of using cryptoledgers to manage smart property has inspired and motivated numerous other groups to put forth similar efforts. For example, Counterparty.co was launched in January.[110] Its mysterious, relatively anonymous development team has released similar open-source applications, documents, binaries and tools that allow users and entrepreneurs to build smart property functionality such as derivatives and dividends in a decentralized manner. Also in January, reporter Jon Southurst discussed several other groups including Reality Keys that can utilize a crypto protocol to build a predictions market or a way to hedge against currency fluctuations.[111]

Mastercoin

At the beginning of January 2014 I spoke with Taariq Lewis, the founder and CEO of BitcoinBusiness, a Bitcoin advisory firm and he is also the Smart Property and Business Development Lead of the Mastercoin Project.[112] Mastercoin is a crowdfunded, non-profit endeavor to create an open-source decentralized exchange protocol for Bitcoin. As noted above, the Mastercoin project has received 4,700 bitcoins ($5 million at the time) in crowdfunding which has been used to pay for bounties, building tools and write documentation all of which is ultimately released on an open-source basis.[113][114]

According to Lewis, "we are on the tip of the iceberg of the democratization of upper level finance and investment management. One apt analogy is that the current system involves a highly siloed, highly centralized organization reminiscent to the music industry prior to P2P innovations. We are now approaching the first wave of people being able to distribute financial products to each other on a peer-to-peer basis. While this obviously has regulatory repercussions such as the SEC and CFTC oversight in the US, there is no "Wolf of Wall Street" in crypto. In fact, projects like Colored Coin, Counterparty and Mastercoin will create applications that will decentralize stock and bond exchanges allowing individuals and entrepreneurs to build dividend products and distribute the assets without middlemen."

I also spoke with Ron Gross, co-founder of Bitblu and executive director at the Mastercoin Foundation, who also pushes the open-source nature of the project. "With Mastercoin, we are all developing open source software and tools that eventually will enable anyone to build their own applications on the platform. We are still hiring people for the core development team yet ultimately we want to move into a decentralized structure where we as team do not actually own anything or manually hire and fire but

rather a Decentralized Autonomous Application (DAA) does. In addition we have put together a series of external bounties, where we give away $100,000 each month to developers outside the organization either working on specific milestones or just doing general innovation around the ecosystem. Thus new programmers to this space could immediately be financially rewarded for looking through a list of bounties and submitting solutions to them, or for being creative and building around the infrastructure."

Gross sees this ecosystem eventually mapping the real world in a digital space: as self-reinforcing entrepreneurial activity – continuously builds the ecosystem a new financial system will emerge that serves as a bridge between cryptoledgers and the existing world. As part of this vision, a natural outgrowth encompasses decentralized applications, bonds, asset backed coins, commodities, real estate, betting and prediction markets that correspond to a smart property token will emerge. One on-going project he highlighted in particular was an open-source omniwallet, which will eventually be capable of handling and tracking the cornucopia of altcoins, metacoins, and even colored coins.

Yet getting there will obviously involve hurdles. According to Gross, "just getting the protocol developed and robust will be a rewarding challenge. The infrastructure is not quite ready for large more complicated projects and is undergoing massive development yet Mastercoin and all the other protocols in the same space are still accessible due to the open-source nature. Any developer, anyone can come – look at the spec, go into the debates, send in your pull requests, look at the code – and contribute immediately. There is no need for a central brick-and-mortar building because if you contribute anything that is positive, you will get rewarded for it. BitAngels is launching a fund soon that is going to invest in protocols, development of DAOs and other "2.0" initiatives through hackathons where the top winners will receive a $500,000 investment.[115] And through these efforts we will build a better financial system, one that is decentralized and creates complete financial freedom. The impact of creating such tools is obviously a matter of speculation but even a fraction of the pie is going to be really large."

I also spoke with David Johnston, managing director of BitAngels, the first angel investment network focused on digitial-currency startups, and a board member at the Mastercoin Foundation.[116] In his view, "cryptocurrencies are more than a payment network, it is more than a new type currency or store of wealth. It is a whole new platform and is a way for people to now make programmable money and that gives rise to smart contracts. Now that this money is programmable I can put it into applications, I can create other digital tokens. That's what really gets me excited where anyone can build anything. In the long-run we also plan to turn the entire project into a DApp, to maximize resources and improve efficiencies."

A DApp is short for decentralized application. The Mastercoin platform, like arguably every other one, is still a work in progress and has gone through several iterations based on community feedback. It also faces market competition from several others in this space such as Open-Transactions, Invictus (formerly BitShares). As a consequence, it looks like a promising area for Christensen-style innovation.

NXT

Launched in late November 2013, NXT is a new cryptoplatform written entirely from scratch in Java.[117] The platform has the ability to natively track "colored coins" – tokens that represent a specific asset based on their "color" (e.g., using a fraction of NXT to represent a car or house). It also includes a decentralized asset exchange, which means you can buy and sell assets without going through a 3rd party. For instance, one of the problems that impacts centralized exchanges and online stores today is that both your fiat and tokens are vulnerable to theft, hacking and other abuse. In one notable instance,

in December 2013, an online commerce site called Sheep Marketplace was hacked and 96,000 bitcoins were removed from its web-based wallet making it the largest known cryptoheist.[118] This type of abuse is nearly impossible in a decentralized peer-to-peer exchange because there is no single centralized point of attack.[119]

In February 2014, I exchanged messages with "Uniqueorn," contributor to the NXT development team.[120] In his view, "the best way to compare NXT to the other cryptocurrencies is basically to not do it. NXT is not an altcoin at all. While most of the cryptocoins being circulated are typically clones of the Bitcoin codebase with a few slight variations, very few of them bring anything new or substantial to cryptocurrency functionality. On top of this is a built-in encrypted messaging system (like BitMessage) and anonymous payments (similar to Zerocoin) which adds an additional layer of privacy to protect confidential information and trade secrets. Yet a lot of work still needs to be done both with our platform and the rest of the industry. You cannot expect that your mother and father are going to sit down and understand this. For them it is supposed to be a tool to make their lives easier, not harder."

Another key difference is that unlike Bitcoin and Litecoin which utilize proof-of-work mechanisms that scale in difficulty with network hashrate (i.e., additional hashrate added to a cryptoledger proportionally increases the block difficulty level); NXT instead utilizes something called 'Forging,' which is basically recirculation of NXT (Proof-of-Stake).[121] "Uniqueorn" noted that, "proof-of-stake allows 'miners' to generate NXT without requiring the use of relatively large sums of electricity that other cryptocoin proof-of-work systems currently do." In other words, the barriers to entry are significantly lower as user does not need to utilize a top-of-the line ASIC machine which is discussed later in Chapter 7. Therefore, a user can "forge" tokens on a smart phone, a solar powered Raspberry Pi, or a laptop computer. In practice, an algorithm randomly picks one node to process all of the transactions and all other machines know this system is the sole transaction 'forger' – thus all other erroneous transactions can be discarded. All machines participating in this 'forging' effort are rewarded according to the proportional amount of NXT they have; thus if you have 1% of the tokens you have a 1% chance of being selected to forge the next block. Because the transactions nodes are known, this provides increased security, an estimated 90% of the NXT tokens must be controlled by one agent in order to compromise the network via a double-spend (e.g., 51% attack).[122]

I also corresponded with 'Graviton' who is the Nextcoin.org community founder.[123] According to him, one of the motivations for why the core team decided to move beyond Bitcoin was, "there certainly seemed to be demand for a technically advanced cryptocurrency with a completely new codebase that puts away the requirement for energy expensive Proof-of-Work once and for all. The environmentally green and attack resistant Proof-of-Stake algorithm, plus the important fact that NXT is not only a payment instrument but a new generation platform natively supporting a suite of services such as decentralized trading and encrypted messaging, seems to have filled gaps that were shining open wide with the existing old school cryptocurrencies."

He is also looking forward to the deployment of a decentralized asset exchange as well as colored coin functionality on the NXT platform and believes that these will "become a popular standard for quite a bit of trading applications, for both - cryptocurrencies and assets denominated in them. The rest of the industry will integrate seamlessly to that, so the distinctions between various crypto brands will start to dissipate." And like several other developers interviewed, "the killer app would be to have available the simplest possible means to pay for merchandise & services in fiat nomination but from one's cryptocurrency wallet, to be able enjoy the fiat price appreciation with the same wallet, and to flip your wallet contents to another crypto with a push of a button. Preferably on mobile."

Ethereum

Another “2.0” project that is gaining traction is Ethereum, announced in January 2014 which brings together both a cryptoledger and a Turing-complete programming language. In short, a Turing-complete programming language means that the language can be used to simulate any other computer language (not just its own). The original Bitcoin protocol and software implementation released in 2009 included a language called Script that had many limitations (it was intentionally not Turing-complete) and as a consequence has largely been underutilized. As a consequence, developers have had to try and use these duct-taped exoskeleton wrappers to build on top of the protocol to enable new functionality. Many developers, including those with the Ethereum project, recognized this limitation and, rather than building and providing a specific feature set, will instead use a Turing-complete C-like language (CLL) that software developers can then use to build a cornucopia of tools, including any type of smart contract, asset management instrument or even a decentralized autonomous organization (DAO) that can then be automatically executed, controlled, and audited by the Ethereum ledger.[124] While its approach is one of the most holistic thus far, its long-term success still requires a critical mass, mind-share and the network effect.

To find out more about Ethereum, I corresponded with Vitalik Buterin, head writer at Bitcoin Magazine and a lead developer on the Ethereum project.[125] Because of the all-encompassing abilities “2.0” projects are slated to have, it could be confusing for developers to determine on which platform to initially build their apps, but that may not be the only hurdle. In his view, “I would say the main challenge in the 2.0 space is going to be (1) building contracts, and (2) building interfaces. These have always been problems, of course, but up until now they have been eclipsed by other, larger, problems, like maintaining server infrastructure and scalability, ensuring security of funds, regulatory compliance and having banking relationships. With decentralized apps, most of those problems are gone, so the only two issues that still remain - contract design and interface design - are now at the forefront. The two problems can easily be handled separately; someone should be able to write a derivatives trading GUI and have that port over automatically to various systems inside of Ethereum, BitsharesX and whatever else people want to trade on.”[126]

Several other developers and investors I spoke with had similar sentiments: creating easy-to-use, intuitive interfaces for end-users would quickly set your product apart from the pack. While there have been many advances, especially for merchant plugins, backing up and securing wallets can be quite cumbersome and even a chore to handle at times, stunting wider-spread adoption.[127]

Buterin had previously worked on both the Colored Coins and Mastercoin project. While portable, both of these currently utilize the Bitcoin protocol, which has a couple of limitations. In Buterin’s view, “one of the key features of Bitcoin is that it has a concept of "simplified payment verification” (SPV), where a Bitcoin node can verify the validity of a transaction in the blockchain by only downloading the very small subset of data in the blockchain that is relevant to that particular transaction. Given that a "full" Bitcoin node now takes 14 GB of space to run, beyond the reach of many users, this mechanism has become an essential part of Bitcoin security. The problem with on-blockchain meta-protocols, however, is that they do not benefit from this protocol. The underlying Bitcoin layer has no way of knowing whether or not a given transaction is valid in the context of the meta-protocol, so the Bitcoin blockchain will include transactions that are both valid and invalid, and so the validity of a given meta-protocol transaction can only be calculated by recalculating the entire state of the protocol up until that point - requiring the full blockchain. Ethereum solves these issues by not being a meta-protocol, instead relying on an independent blockchain.”

SPV is a type of thin client that provides Bitcoin users a lightweight method for sending and confirming transactions without having to carry around the entire database.[128] It does this by downloading only the headers for all the blocks (i.e., the Merkle tree) and not the entire blockchain itself. As a consequence, this flexibility enables Bitcoin clients to be used by point-of-sale registers that may not have enough space or bandwidth to continuously download the entire blockchain. And at this time, as Buterin notes, the only way to completely confirm that a transaction based on Colored Coins or meta-coins like Mastercoin is valid is to re-check the entire blockchain. This presents a significant obstacle to scalability.

When describing and defining what a "smart contract" and "DAO" are, it can be confusing at times because a robust smart contract is sometimes used synonymously with a DAO. According to Buterin, "I would say there is no clear-line distinction between the two, but there are some general differences in connotation. To me, a smart contract is something that is single-purpose and ephemeral, so they are created for a specific task and can disappear at the end. A financial contract is a good example there. An autonomous agent is something that is more long-term focused, and includes an internal AI to make decisions. And finally, a decentralized autonomous organization is a long-term contract between many people, perhaps even with the ability for people to join in as signatories or trade their positions away, whose main role is to hold on to assets and use some kind of voting system to manage their distribution. There can be many different types of DAOs; the more basic ones live entirely on the blockchain, but more advanced ones might have some of their data stored on other decentralized networks or across a number of servers."[129]

Throughout this manuscript, several of Mike Hearn's presentations are referenced, including the Turing 2013 conference.[130] While both Hearn and Vitalik Buterin use the same name, DAO, the definitions for what the term implies, varies. In an email exchange, according to Hearn, "what Vitalik calls DAO's are not quite the same as what I discussed in the Turing talk. I used to think they were the same, but on closer inspection he called Bitcoin itself a DAO so it's obviously different. Assuming you mean agents, there are so many challenges I doubt it will happen any time soon. Really you need trusted computing for it to work well and that won't work well at least until Intel release CPU's supporting their SGX extensions, which they didn't even announce a date for."

Trusted computing is a term for computers that can be controlled a certain way via encryption. Many governmental agencies such as the US Department of Defense require that computers acquired by vendors have such functionality. In September 2013, Intel released its programming reference manual for Software Guard Extensions (SGX) which could potentially create similar functionality in consumer-based systems.[131]

Throughout this guide I describe simple "smart contracts" with the assumption they do not have any sophisticated internal AI components. Similarly I refer to relatively simple DAOs that wholly reside on the blockchain. As programmers become more acquainted with decentralized software and the technology evolves and begins to be used in practical applications, it is likely the specific meaning of each term will be subject to change.

BitShares

This last point is viewed as a critical issue to other 2.0 project managers as well. I had an email exchange with Daniel Larimer, the creator of BitShares, and the first person to describe Bitcoin as a Decentralized Autonomous Company (DAC).[132] BitShares is a new way to view cryptocurrencies where you view your

wallet balance as shares rather than coins. According to Larimer, Bitcoin can be viewed as a DAC where each bitcoin represents one share in the Bitcoin ecosystem. The transaction fees that Bitcoin charges can be viewed as revenue to Bitcoin and the mining rewards can be viewed as expenses paid by Bitcoin to secure the network.

Larimer decided to change the analogy from coins to shares so that the underlying economics could be considered when designing next generation crypto systems. Based on this analogy, he sees several ways to improve Bitcoin when viewed as a company. In his view, the driving principle is that all companies should generate profits by minimizing expenses while maximizing revenue from product sales.

In the case Bitcoin, the primary expense is security which is provided by an expensive proof-of-work (PoW) process described in chapter 2. In BitShares systems all security is provided by proof-of-stake (PoS). In his view, a PoS (which is also used in NXT) can be thought of as having the shareholders vote on the valid transaction ledger. In this way those who own the system secure the system without having to spend increasingly larger sums of capital to do more work than any attacker can. This last point was recently described by Nicolas Houy, a researcher at CNRS, stating, "Bitcoin miners have engaged in an arm race to computational power and in the end, much hardware, engineering and energy are used to solve mathematical problems that are artificially made extremely complex."[133] A PoS system is supposed to remove this artificially complexity and lower the capital costs for entry.

The other thing BitShares systems do, according to Larimer, is focus on increasing the value of the transactions that can be performed and thereby generating additional transaction fees. Because there are no miners to pay, transaction fees can be viewed as profits for the system and these profits are used to buy back and retire shares. This has the effect of increasing the value of the shares still in circulation. It is economically similar to earning a dividend. The value from the fees is transferred to the shareholders proportional to their stake.

The first BitShares system being developed by his team is called BitShares X which continues with the company analogy to implement the business model of a bank and exchange simply be defining a new set of transactions supported by the blockchain. According to Larimer, one unique attribute about BitShares X is that there are no counter-parties, employees, vaults, or contracts and yet according to him, BitShares X facilitates the creation of BitUSD purportedly the same way that the Federal Reserve creates FedUSD: it lends it into existence backed by collateral.

BitShares X uses shares in the system as collateral to back BitUSD. BitUSD can be thought of as an asset that you can sell for a dollar's worth of shares in BitShares X. Depending upon when you buy or sell your BitUSD you will get a different number of shares, but based on their initial model the purchasing power should be approximately a dollar. And according to him, like Bitcoin where there are no issuers backing the value of a bitcoin, there are no issuers of BitShares X shares or BitUSD. The entire system operates on nothing but a chain of numbers following a predefined set of rules enforced by the consensus of the network.

Larimer also believes that BitShares X is just one of many potential business models that could be defined entirely in software. And while one of the challenges is finding developers with an understanding of both economics and consensus, yet other business models his team sees opportunities in include insurance, domain names, gaming, auctions, and voting. Voting is another issue that other

entrepreneurs in this space touched on, which is described in greater detail in the NGO segment in chapter 8.

I also spoke with Charles Evans, economic advisor with the Invictus-run BitShares project. The way he looks at BitShares is that

> "a share can be issued for agricultural commodities, like coffee, tea, cardamom, etc. If someone who grows a commodity that has a corresponding BitShare sees that the BitShare can be sold for more than it would cost to deliver the commodity, then the grower can offer, e.g., 100 kg of cardamom in exchange for 100 kg of BitCardamom, sell the BitCardamom on the open market, and ship the cardamom to the buyer. Note that the BitCardamom is not "backed" by cardamom. It trades on a prediction market, in which players worldwide try to discover a single, global price for a fungible commodity. When someone with specialized local knowledge sees an arbitrage opportunity—here, simultaneously buying BitCardamom with a promise to deliver cardamom and selling the BitCardamom on the open market—that party can exploit the opportunity. Instead of negotiating with local wholesalers, who might have information advantages over local growers, and relying on one's own ability to haggle well, the grower can use a global information market as a guide. Likewise, if the price of BitCardamom rose over time, prospective growers worldwide would be able to see the price and respond to the price signal."

Counterparty

For perspective I had an email exchange with Ryan Orr, who is a professor at Stanford University (teaching Global Project Finance and Infrastructure Investment) and chairman at Zanbato.[134] Orr has also been closely following Counterparty, which is the first functioning protocol layer fully integrated with the Bitcoin blockchain that supports peer-to-peer transfers of a coin called XCP.[135] At the beginning of January the Counterparty development team announced that they had successfully released a working protocol including asset-backed issuance, betting, dividends, callable assets and the world's first decentralized exchange.[136]

As the next few months will involve a race between Colored Coins, Mastercoin, and Counterparty as well as other non-blockchain equivalents such as Ripple and Open-Transactions, with each system bringing its new innovations, many outside commentators have expressed interest over Counterparty's integration with the Bitcoin blockchain and execution to date. "The fact that we have six serious competitors is a huge development for the entire segment," says Orr, "The early days of this race will be about tech execution whereas the later days will involve regulatory finesse. The 'value web' (as opposed to the 'information web') is finally here. The significance of these developments for the future of the field finance are gargantuan – what we are witnessing could be the equivalent of the invention of http on top of TCP/IP, and these are the protocols that are likely underpin the evolution of the value-web over the coming decades."

In February 2014 I exchanged messages with one of the lead developers, who used the pseudonym "PhantomPhreak."[137] According to him, "Counterparty is a protocol, and a piece of software, that takes the technology underlying Bitcoin and extends it beyond simple payments, implementing a wide range of financial instruments. It may be used to trade cryptocurrencies, create assets, make bets, and more, with all other Counterparty users, safely and anonymously, with no middleman at all. It is built on top of the Bitcoin blockchain, so it can be very simple and reliable. It is being developed very quickly, and it has a large feature set already. Counterparty inherits all of Bitcoin's security and reliability. It is open-source,

and its launch was entirely decentralised, as is the protocol itself. And as its name suggests, implements a completely distributed, automatic and deterministic clearing house, so there is no counterparty risk to speak of in most transactions. Of course, if someone were to issue an IOU using Counterparty that he did not make good on, then the anonymous nature of the protocol would leave the slighted party with little legal recourse."

This last sentence is of particular interest as it still shows a problem that is currently not solved in a decentralized manner, as Preston Byrne identifies in Chapter 2. As this space matures, developers will need to learn how to structure smart contracts so they are legally and commercially useful. How to enforce these clauses without an escrow-based DAO, without an independent mediator or without a reputation system (e.g., credit score) can and will be tricky but could be a business opportunity for experienced professionals in those segments who are looking to get exposure to the cryptocurrency sector. One competing developer explained to me that, "Counterparty is way ahead of the game because their distributed financial system is deployed today. In many ways, the team is reminiscent of Satoshi: they are people in our community who saw a problem with prior attempts and are fixing it. All others are still spinning their wheels and really need to deliver functionality on which we can all explore further. What's more, proof-of-burn is a big commitment and raises the stakes for everyone. That's why there's so much development activity going on with Counterparty. The investors have to pull to make the coin work and they're pulling hard. They released alpha software and folks are losing money, but they're shipping code updates daily which means the software is getting better and the markets more active. This is an exciting space and this level of competition motivates all of us to take it up a notch."

Proof-of-burn (POB) is a unique turn on allocating "scarce resources" (tokens). Whereas cryptocurrencies such as Bitcoin, Litecoin and Dogecoin use proof-of-work to allocate resources (e.g., a token), proof-of-burn requires that the miners (or any user actually) send their tokens such as a bitcoin to a provably unspendable address (a terminator address) where they are untouchable forever by any party.[138] The first and only "burn" took place beginning on January 2, 2014 and lasted for thirty days – now all of the XCP that will ever exist have been created. During that time, 2,130 BTC were effectively destroyed amounting to roughly $2 million in market prices (the actual repercussion was that all other holders of bitcoin saw a net gain in value by roughly 0.01%).[139] Counterparty then automatically converted the "burned" token into its own unit, called an XCP resulting in no premine or foundershares. It currently takes five XCP to create your own asset, the five are destroyed in the process as a spam control function. While it is a controversial method, proof-of-burn does remove the human element from the equation. That is to say, while other '"2.0" projects are typically funded by IPOs whose assets are then (usually) managed by a non-profit organization, because there is still a trusted 3rd party involved, abuse can occur. That is not to suggest that any abuse is happening, but rather that Counterparty is re-solving the Byzantine General's problem in a different yet mathematically similar, manner than what Satoshi did in 2008.[140]

"PhantomPhreak" also sees potential in other decentralized platforms, "I think that there's a very good chance that so-called second-generation cryptocurrencies will "take off" in the next year or so. Bitcoin was a revolution, in a number of ways, and now it's time for an evolution of the core concepts and paradigms that it introduced. Computer science has to catch up with it, so to speak. A secure, distributed blockchain can be used for so much more than simple payments: advanced financial instruments (a la Counterparty), messaging protocols (c.f. Bitmessage, Twister), etc. Certainly the future of finance is more decentralised than the present, and the economy as a whole will have to change accordingly."[141]

Bitmessage is a peer-to-peer protocol that allows users to send encrypted messages to anyone in a decentralized trustless manner (i.e., Bitcoin for messaging).[142] Twister is an encrypted decentralized peer-to-peer microblogging application that uses both the Bitcoin and BitTorrent protocols to enable users to tweet and communicate anonymously.[143] Other projects in this space are Bitcloud (decentralized cloud services), Maidsafe (decentralized dropbox and API platform) and SyncNet (decentralized web browser).[144]

In addition, he believes there are many applications that financial instrument designers could contribute to this space and in particular Counterparty, stating: "the most obvious possible contributions are simply new features. Right now, for instance, Counterparty only has two different types of 'bets', namely simple 'Equal/NotEqual' bets and contracts for difference. Counterparty, however, has the potential to implement very nearly the entire range of tools commonly available to professionals in the financial industry. Of course, pretty much any developer could contribute a lot to the Counterparty project, which still has a relatively small codebase and an underdeveloped software ecosystem, simply by writing user-friendly interfaces, or algorithmic trading engines, for example, on top of the reference client."

I also exchanged messages with "cityglut" who is another member of the development team. In terms of business opportunities, it is his view that, "what cryptocurrencies in general and Counterparty in particular allow for that is arguably most significant is further decentralization. I believe that businesses which capitalize on this aspect of Counterparty will have opportunities they have not had until now." As noted above, this project does have code that is shipped and is currently being used by the community at large.

He also sees that there are a number of areas of low-hanging fruit. According to him, "in my mind the most obvious financial instrument that Counterparty is currently lacking is a real options function. Counterparty allows for binary (Equal/NotEqual) bets and the creation and (distributed) sale of assets, and I believe that a combination of these functions could create a full-blown options function, but it may well be that in Counterparty's current implementation this is infeasible. Even if an options function can't be built from Counterparty's extant functions, it seems to me both possible and desirable to implement options in Counterparty in some way."

Yet there are challenges too, "It is precisely Counterparty's brand new functionality that entails greater necessary due diligence on the part of users. Since anyone can make an asset, and anyone can publish a broadcast upon which to bet, users must do what they can to make sure the asset they are purchasing is legitimate, and that the broadcast upon which they are betting has not been "tampered" with. In an effort to facilitate the former, we have recently implemented a *description space* for every asset: issuers of assets can include up to 42 bytes (in UTF-8) with each issuance, describing the asset being issued. Regarding broadcasts, aside from the financial incentive feed-operators have to stay honest (namely, collecting betting fees), we imagine that an - albeit informal - reputation system will naturally evolve, helping users to decided which addresses' broadcasts to bet on and which to avoid."

This secondary attribute, a type of descriptive space is a feature that many of the other platforms are trying to enable in order to organize and manage different types of assets. The issue involving reputation is also a theme repeated by many other investors, developers and experts and one that a DAO escrow could potentially resolve.

Open-Transactions

Chris Odom is a cofounder and CTO of Monetas and the lead developer of Open-Transactions (OT).[145] Open-Transactions is an open-sourced digital software suite that utilizes current technology to enable trustless financial cryptographic interactions through privacy features such as blind signatures. It is also portable and ledger agnostic allowing developers to bridge its applications to other cryptoledgers.

Many outside investors and businesses frequently ask Odom a theme on the same question, what business solutions can be developed for this segment? Yet according to Odom, "asking what profitable business opportunities there are for crypto currency is the same as asking that question for the Internet in general. It is extremely broad in scope. I think we are talking about a transformative invention, comparable to electricity, computers or the Internet. It's going to create all new spaces, and it's also going to transform all existing sectors. While Open-Transactions currently is integrated with Bitcoin, it is ledger agnostic because it is a financial crypto library, similar to how OpenSSL is a communications crypto library. In terms of immediate opportunities, we have some bounties posted on CIYAM.org/open. However, people should definitely be aware of risks. Cryptocurrency can be used in legal and illegal ways, so it's not the currency itself, so much as how you use it. You just have to watch out for regulatory compliance issues, and if those get too onerous, you have to look at moving your company to another country. Some countries are less free than others. For an investor I might also point out some of the unique propositions of OT, one being its ability to operate in a low-trust way, that it is federated. And that it's also able to fill the gap and do the things that all the other servers do in the Bitcoin world like the MtGox server, or the BitStamp server, or any of these Bitcoin services that use a server. Any of them could be replaced in a lower-trust fashion, using OT at least, using OT as the financial engine, not necessarily the web GUI pieces."

One advantage that Open-Transactions has over conventional blockchains which have algorithmic delays, is that because it uses known servers, Bob can trade near instantaneously. Whereas confirmation of bitcoins, bitshares and other blockchain based instruments are measured in minutes, users can only execute trades in those intervals as well. And if you can put OT on a distributed database, in theory that means you can have cryptocurrencies that confirm instantly without centralized control as well.

Ripple

Ripple, commercialized by Ripple Labs, is a payments protocol that acts as a payment platform, decentralized currency exchange, and smart contract network that can be used with any digital currency, including Bitcoin. Ripple provides a solution for implementing an asset cloud via "trusted" gateways.[146][147] At scale, Ripple or Ripple like systems provide instant liquidity and exchange between counter parties, where there can be a trustless exchange between 3rd parties, and those 3rd parties can decide where their exchanged assets will settle within the network, such as any gateway who provides redemption for the represented asset. In addition, unlike other payment platforms that use variants of proof-of-work, it uses a consensus ledger which is distributed to a global network of servers.[148] These servers continually receive transactions and proposals from other servers on the network and these are compiled into a "Unique Node List" (UNL). Proposals from servers not in the network are discarded while those remaining are vetted and algorithmically "voted" on by the servers. Once a consensus (defined at 80% agreement on what transactions are legitimate) is reached, the server validates the proposals and closes the ledger, creating a "last closed ledger" (similar to a block). The process then repeats itself. This process takes roughly five to fifteen seconds allowing quicker transactions than nearly any proof-of-work system today. Altogether its network processes roughly $20 million each month from approximately 68,000 user accounts.[149]

Beginning last year, Ripple Labs created an initial money supply of 100 billion XRP which was predetermined to be enough to last for hundreds of years.[150] The designers of Ripple realized they had a problem if someone wanted to flood the network with useless transactions, which is the currency equivalent to spam. To this the network charges a transaction fee which permanently deletes 3 "drops" of XRP. Each drop is equivalent to the smallest possible amount of XRP, thus .000003 per network transaction cost. A drop is equivalent to the Bitcoin "satoshi" the smallest possible unit of BTC which is .00000001. As of this writing more than 3,500 XRP have been permanently removed from the network.

According to Jon Holmquist, an early Bitcoin adopter and Community Liaison at Ripple Labs, "beginning 15 years ago a merchant could create a webshop in 10 minutes and attract visitors from around the globe. Yet, they could not easily pay for the merchandise until 5 years ago. With the development of cryptocurrencies such as Bitcoin, consumers can now use money without borders. However one of the biggest issues today is obtaining bitcoins especially when you reside in an economically depressed region. Ripple lets you exchange and obtain whatever currencies you want to use. As Ripple continues to build partnerships, the network creates a self-reinforcing positive feedback loop that takes care of itself. As a consequence, because Bitcoin has gotten a lot of push behind it, it is possible to have a fiat exchange in every country which then allows customers to finally purchase from any country, with their own currency."

A math-based currency is a term often used by members of the Ripple Labs team to describe the concept of "programmable money" – that is to say, virtual tokens that are mathematically constrained by algorithms and difficult if not impossible to forge.[151][152] The Ripple payment system works alongside Bitcoin by enabling users to use XRP, a token, to represent certain financial instruments (like currencies) which can then be instantly transferred globally and exchanged for Bitcoin and then a fiat currency.

Both XRP and the Ripple protocol can be leveraged in other ways as well. Steve Bennet, a finance professor at San Jose State University and an angel investor with CrossCoin Ventures which is a new business incubator partnered with Ripple Labs, points out that the project has "built a new incubator which will later become an accelerator focused on building out the Ripple ecosystem.[153] Currently we are focused on attracting Bitcoin-related companies which can leverage the Ripple platform to provide new value to customers globally." Bennet's team (including Ryan Orr mentioned above) plans to work with both new startups and existing companies, provide them access to Ripple's management and even exchange Ripple for a percent of equity much like several other "2.0" projects have done (e.g., Mastercoin, NXT). His vision is to leverage the incubators' resources (e.g. networking, mentoring, legal) and help the incubated teams focus their energy on providing value-added services to a broad array of consumers who are unfamiliar with cryptocurrencies.

I also spoke with Stefan Thomas, co-founder of WeUseCoins, creator of bitcoinJS and CTO of Ripple Labs. In his mind, "the easiest way to describe Ripple right now is that it is a FOREX platform that removes most intermediaries and does so in a matter of seconds.[154] And because you reduce the total amount of fees that are charged from the remittance process, this provides thinner spreads for users who traditionally have had to worry about currency fluctuations. That is to say, in the past, it could take hours or days for funds to move across borders whereupon the value of the currency could decrease." Yet as noted above, Ripple's platform is nearly instantaneous and powered by a distributed network of ledger "processors" (slightly akin to "miners" but requiring very little infrastructure) and gateways.

And according to Thomas, “while processor nodes do vote and verify the ledger integrity to prevent forgery and double-spending like a blockchain, these processors are unlike the “miners” used in blockchains because of the way the light-weight method consensus is determined which requires substantially less infrastructure (e.g., no need for ASICs or GPUs). Consensus of the ledger is done through a peering method; similar to how peering with trusted nodes works with internet providers. The ledger itself is a bundle of digitally signed data transactions which is sent through the network and voted upon by client peers (nodes). These nodes poll one another to see which transactions came first, the ones that are determined to be false or illegitimate are discarded and all others are included in a verified ledger state that is then considered closed. This entire process takes between every 5 to 15 seconds and nodes that become unreliable with spam are then ignored by peers. The reason the timing is not a fixed rate because transaction bundles not only vary by size (e.g., consumption by consumers does not happen at a unison, flat rate) – and it also illustrates how data itself is processed globally through current public infrastructure. In contrast, the reason that Visa is slightly faster is that they use private centralized nodes which requires significantly more overhead and capital expenditures.”

“Gateways are the actual organizations that move assets in and out of the Ripple network. They can range from single-individuals to large banks. Users establish trust lines with gateways which can be located in any part of the world, providing liquidity into nearly any local currency. A unique feature about gateways is, that while they may be a single-point-of-failure in the traditional sense, users can still route around censored nodes. Furthermore, gateways cannot appropriate the assets of one specific user: either they default for everyone or none at all. So for example, Bob can create a debt line with Alice who is trusted party, a gateway. Gateways live by reputation, so they have an incentive to fulfill their obligations. Bob can then exchange a local currency with Alice for IOUs (XRP) with which Bob can then send to any other gateway and convert XRP into the local currency. This can be done in a matter of seconds, which is significantly faster than any blockchain-based system, yet is actually more secure (51% versus 80%).”

Ripple Labs refer to their technology as a 'value web', an 'Internet for money', and 'http for money.’ Existing financial institutions could serve as gateways today by establishing 'trust lines'. The gateway system enables financial institutions to exchange value in the form of digitized assets (e.g., commodities, fiat currency). For instance, Bob’s Bank of Buffalo could set up a gateway and trustline with Alice’s Agriculture Bank in China. Bob could provide USD liquidity to Alice and Alice could provide RMB liquidity to him in a cheaper and quicker manner (between 5-15 seconds) than existing wire services which could take days and charge relatively high fees. Ripple acts as trusted ledger for all participants, yet cash balances must be settled outside of the Ripple protocol. XRP is the only currency native to the network.

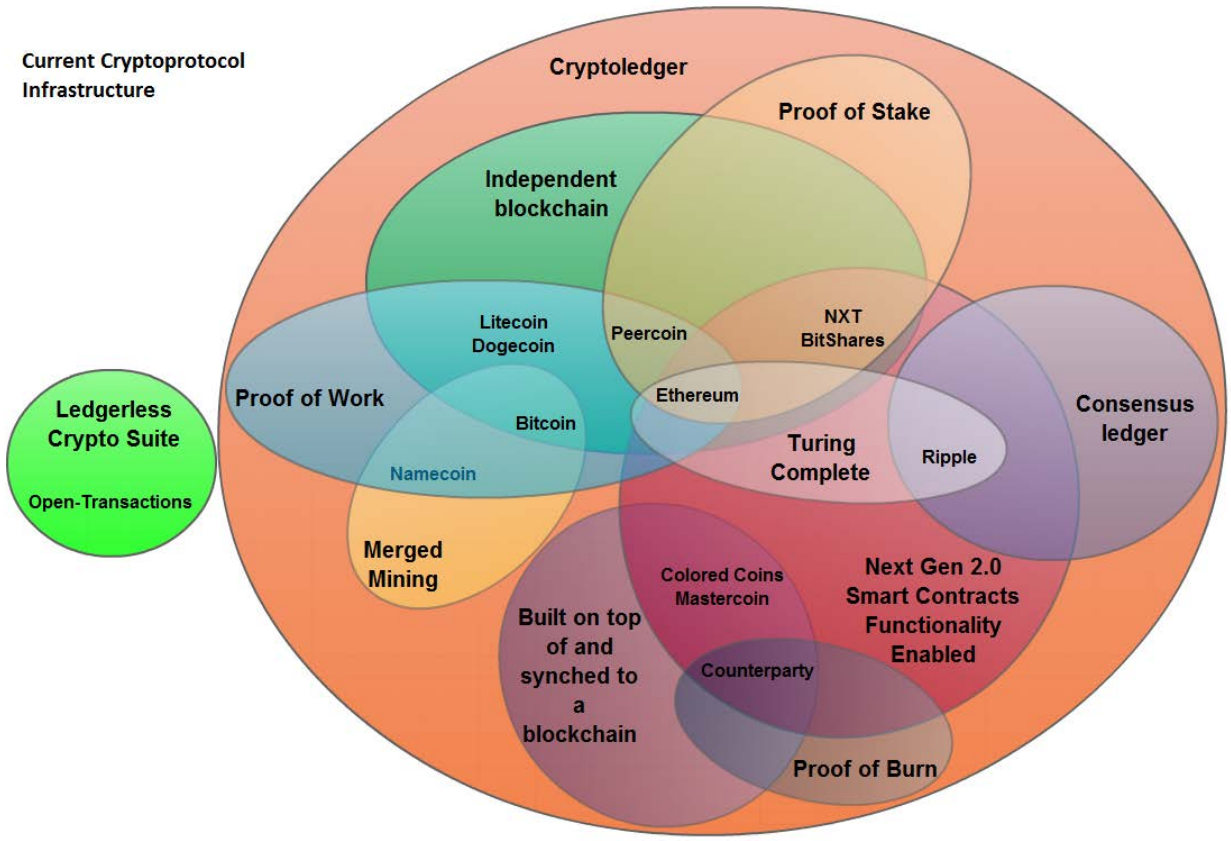
Thomas continued with, “another competitive advantage that the Ripple protocol has over others in this space is that our code uses the smallest amount of trusted code base, basic OP codes which provide the most secure assembly code to which to build from (e.g., interacts directly with the iron, with the metal of the semiconductors). Thus the native software client is less vulnerable to exploits that occur from building above with other higher-language layers. And over the past two years we have open-sourced a significant amount of codebase including the protocol to the public. This in turn has led to further refinements and security fixes. In addition, we are continually looking at ways to expand the protocol’s use, making the ledger essentially a database that will allow for the transaction of smart contracts.[155] And because this network is slightly more efficient than most other platforms, this allows for new innovations to take place down the road.” This contract-based system will be Turing complete and include two-stages, the first of which is non-deterministic which enables contracts to interact with real-

world protocols such as DNS and HTTP and also allows users to include language interpreters and reference libraries.

"This space is rapidly evolving; for instance, the original Bitcoin client was much more cumbersome than it is today. For beginners it used to take 24 hours to download the blockchain and confirm transactions. Now there are numerous projects each of which trying to provide value-added services and this competition is pushing us to look at new ways to innovate, such as peer-assisted key derivation function (PAKDF) – a mathematical way of utilizing blind signatures.[156] One of the user-adoption problems in this space is that it is hard to memorize long secure passwords and frustrating for new users to learn how to securely save passwords on disk drives. In contrast, PAKDF will allow Alice to use relatively weak passwords that can be sent to Bob who will sign something (e.g., a contract) without knowing and therefore unable to break Alice's password. This is called a blind signature which adopts a form of homomorphic encryption and we are integrating into Ripple."[157]

Whereas a user would need to memorize a long passphrase, this specific application of securely signing a password could lead to ease-of-use for end-users. In a nutshell, a blind signature scheme "allows a person to get a message by another party without revealing any information about the message to the other party."[158] The analogy typically used to describe how this worked is, Alice places a message inside a carbon lined envelope. This envelope is sent to Bob, who cannot read or see any of the information, but can sign on the outside of the envelope, which imprints the signature on the carbon inside the envelope.

Current Cryptoprotocol Infrastructure



This Euler diagram shows two main systems, those currently part of a cryptoledger and those that are not, which in this case is solely Open-Transactions (OT).[159] As noted earlier in the chapter, OT works by connecting its OTX protocol to other services (much like SSL does with other databases) such as Bitcoin and is therefore ledger agnostic.

Within the cryptoledger diagram are essentially two other distinctions, those that use a blockchain and those that use a consensus ledger. At the time of this writing only the Ripple protocol uses a consensus ledger. When it was first created, Namecoin was also originally its own independent blockchain but the mining process has since merged with the Bitcoin ledger. The other independent blockchains above are Litecoin, Dogecoin, NXT, BitShares and Ethereum. At the time of this writing, the Ethereum team has not settled on which system it will use – it may use a hybrid approach similar to what Peercoin has done (proof-of-work and proof-of stake).

Proof-of-work (PoW) involves a network of mining machines as originally employed by Bitcoin in 2009. Computers are given a series of increasingly difficult benign math problems which they complete as a way to stave off rogue attackers. In this example above, Litecoin, Dogecoin, Namecoin, Bitcoin and potentially Ethereum use a proof-of-work method.

Proof-of-stake (PoS) is different in that the transaction node for a block is randomly assigned and all network participants communicate directly with it. One advantage to this approach as it reduces the amount of hashing power needed to secure the network. At the time of this writing, only NXT in the above diagram uses a pure PoS method; Peercoin uses a hybrid and Ethereum may also use a hybrid as well.

Proof-of-burn (PoB) is a unique method that has only been used thus far with Counterparty; a user sends a token (a bitcoin) to a provably unspendable address (a terminator address). The largest benefit of using this approach is that it removes the need to have a trusted party or a custodian to look after "IPO" assets.

The inner red diagram illustrates the smart contract features described in this chapter. While the Bitcoin protocol could conceivably utilize such contracts, the functionality has not been 'turned-on' by the development team (version 0.9 will allow for 80-byte hashes that could include a hash of a distributed contract). While there are multiple different platforms that will offer such functionality, a stop-gap solution based on bitcoinJS (a Java-implementation) is being developed by Bitpay called bitcore and is described in chapter 7. Other platforms that can or will shortly allow smart functionality include Colored Coins, Mastercoin, Counterparty, NXT, BitShares, Ethereum and Ripple.

Projects that are being built on top of a blockchain include Colored Coins, Mastercoin and Counterparty. Both Colored Coins and Mastercoin work exclusively with Bitcoin's blockchain, and while Counterparty does as well, other projects such as Peercover (discussed in chapter 5) have enabled Counterparty's currency to bridge with Ripple's network.

While Ethereum and Ripple are categorized as being the only Turing-complete platforms above, it should be noted that Ethereum has not yet shipped but is expected to in the next six months. In addition, developers with NXT and BitShares expect to include similar robustness if not full Turing complete functionality at some point in the future.[160]

One large category that is not distinguished in the above diagram is that of "altcoins."[161] Strictly speaking, anything that is not Bitcoin is considered by early adopters as an altcoin. Thus everything but Open-Transactions in the diagram is considered by some, as a type of altcoin. However, this devolves into individual preferences and politics, so it is best ignored.

Chapter 4: Smart Property

Since the release of the original genesis block in 2009, hobbyists and professional traders alike have been practicing trustless asset management – except there has been only one asset: bitcoin, and it has been traded on what until recently was essentially an unregulated securities exchange. The next evolutionary step is to begin using cryptographic ledgers to track, manage and exchange smart contracts and even smart property.

According to Nick Szabo, the lowest-hanging fruit in this segment is contracts that are 99.9% "dry" code – which is to say, those already formalized which can then be executed automatically via software code with extremely few manual exceptions.[162] This would immediately encapsulate nearly all of the securities and financial instruments currently traded on electronic exchanges such as NASDAQ and Euronext (of which the NYSE is a component).[163] This has a number of Christensen-disruptive qualities affecting middle management and potentially entire departments of individuals at financial institutions who neither write the code nor provide additional interpretive value to such contracts, and whose jobs (e.g., auditing, accounts reconciliation) could conceivably be made redundant by a decentralized cryptoledger.

Virtual, digitized assets and financial instruments may be easier to visualize since many people reading this already have experience receiving salaries via direct deposit, using 3rd party payment processors (e.g., PayPal, Alipay) and even online brokerages (e.g., E-Trade, Scottrade); but how could smart contracts interact and control physical property?

Through a modification appropriately called smart property.

Szabo was one of the first to describe a solution to this interaction conundrum, with what he called a "proplet."[164] He stated in the paper, "the goal of proplet design is to control physical objects with digital protocols." In his view, the functionality of a proplet could be fulfilled with a microelectromechanical system (MEMS), a device that has microsensors with several capabilities including the ability to track ownership, determine precise location and provide robust security. Most modern-day smartphones and tablets, as well as some automobiles, include some type of MEMS (such as an accelerometer).

While ten or fifteen years ago it may have been a tall order to convince manufacturers to add "proplets" to their wares, the unintentional spread of MEMS-like devices has taken place through an organic push called the "Internet of Things" (IoT) (e.g., home automation). This is a term coined by Kevin Ashton in 2009 to refer to the ability to uniquely identify and tag any kind of object through an Internet-like structure.[165] This can be done with existing technology such as RFID, NFC, barcodes, QR codes, and digital watermarking. As a consequence, many modern appliances such as refrigerators, thermostats, smoke detectors, doors, vacuums and even light-bulbs could be manufactured with IoT features built-in.[166] According to *BI Intelligence*, by 2018 there will be 9 billion IoT-enabled devices; more than all smartphones, smart TVs, tablets, PCs and wearable computers combined.[167] Yet keep in mind, just because something is automated such as WiFi enabled light bulbs or even doors, that this is not smart property. It may be automated or even autonomous but it is not "smart" in the sense that ownership and control can be reverted automatically to a different party via a smart contract.

If an object has not only IoT functionality, but also proplet-functionality, it can be managed by digital protocols which in turn can be managed by smart contracts.[168] In fact, Szabo used a similar insight in an exchange: "Equipment and appliances that are not already titled, but have enough resale value to use as

collateral, are good candidates to use the new peer-to-peer title registries and for building in proplets or something similar."[169]

The question of logistics – how to control a physical object remotely through a contract – is a common one that Szabo and others have considered. In one of his first publications on this topic, Szabo uses an example of a car lease and a smart lien protocol.[170] A smart contract for a car lease may include a clause, such as a lien that revolves around a "time lock" (nTimeLock is the technical term used in Bitcoin). In such a contract, if a lessee fails to make a payment, the smart lien protocol is invoked, preventing the use of the vehicle and enabling a creditor (and repo firm) to retake control of the vehicle. Obviously there could be grace periods coded into such clauses and even operational exceptions, such as not revoking operation while a car is driving down a freeway.

Another example recently explained by Vitalik Buterin could be a museum pass.[171] Using your phone's NFC capability plus a feature like a "colored" coin or even bitcoin itself, assuming you own that token unit, you can sign a message attached to it with a private key. You can purchase a museum pass and then you can digitally sign the pass that allows admission into a museum. If you want to sell the museum pass you can transfer the virtual coin to someone else, they can sign the pass with their key (which is on their phone), and ownership is passed to them. Or, if Bob managed a rent-to-own store, he could include some kind of "proplet" to electronic merchandise that would facilitate the creditor-borrower ownership (e.g., failure to pay for a television, refrigerator, or even arcade machine results in service termination).

Despite this marginal progression through automation of pharmaceutical dispensaries, automation of factory work, self-driving vehicles, and voice recognition, there is a gulf between what can be done and whether or not it will be legally allowed.

However, according to Szabo,

> "There isn't any big technological barrier to this. It's largely a matter of learning about the technology and being persuaded enough of its utility to make the relatively large capital investment for such hardware (as opposed to cryptocurrencies and the title registry itself which is just software). The biggest barrier will probably be synchronizing with or replacing existing titling systems. There's no terribly difficult new technology required, but when it comes to property that is already registered (for example in the U.S. states register car titles), there has to be synchronization between the two registries, or else the states (in the case of cars) has to switch to using a block chain as the registry of record for their title systems. Alas there will probably be a lot of slow-moving bureaucracy and politics involved. Since title registries are already pretty good in the developed world there is probably an earlier market for these kinds of systems in less developed countries when it comes to existing kinds of property. In the developed world block chain titles will at first primarily be used for financial instruments or contracts (and of course, the first use of all has been to store and transfer titles to money itself). Also, equipment and appliances that aren't already titled, but have enough resale value to use as collateral, are good candidates to use the new peer-to-peer title registries and for building in proplets or something similar."[172]

Let us explore the car example. What this would mean is that a state department of motor vehicles (DMV) would need to be convinced to use a computer system that is connected with the same cryptoledger or database that is being used to transfer automobile ownership. This could conceivably

be done with existing technology. However, if the past five years of regulatory uncertainty and risks with cryptocurrency is any indication (e.g., anti-money laundering laws, Know Your Customer, Money Transmitter License, Money Service Business), it would seem unlikely that all departments like the DMV will quickly adopt this method and allow assets such as vehicles (or houses or securities) to simply trade hands without some kind of tax or oversight.[173][174]

What happens to smart contracts if a cryptoledger one is using is abandoned by miners?[175] For example, maintaining a single-use proof-of-work cryptoledger is not necessarily an optimal use of resources (discussed later in chapter 8). As noted above, you could potentially use the consensus-mining power of the Bitcoin network (or alts) to actually track and manage nearly every type of asset. The fact that it only tracks one is non-optimal in terms of assets per hash. But hypothetically, if Bob created a new cryptoledger for the DMV that is then solely used to allocate and track vehicles from a DMV registry, what happens if the underlying ledger loses all of its miners in a year or two?[176] The ledger then no longer is usable for its purpose.[177] And the vehicle titles are potentially forgeable and untrackable if miners abandon the network. The solution to this is that in all likelihood, the codebase for the smart contracts and DAO that utilize a cryptoledger will be portable due to its open-source nature. Thus you could create and encode additional copies of the smart contracts and place them on multiple ledgers for redundancy. That is to say, the developmental costs of duplicating and triplicating the smart contracts onto other ledgers are minimal. Either that or the ledger would be mined by the state, and electricity costs would be passed on to the general public as taxes.[178]

There may be other opportunities for entrepreneurs to build tamper-proof and tamper-resistant containers with embedded smart property elements (NFC, MEMS), allowing users to track packages in near-real time.[179] Or perhaps industrial design consultants can find new opportunities to assist companies wanting to affix proplets to their wares – a process which incidentally fulfills what Richard Brown jokingly stated last fall: on the blockchain, nobody knows you are a fridge.[180]

Paper Meets Electricity

Smart contracts are coming of age in a period of paper-based controls designed to prevent error, fraud and abuse by delegating tasks to different, imperfect agents. For example, an auditor may split up functions in a warehouse in which delivery, sales, receipt of payment and accounting are assigned to different parties. According to Szabo, this segregation-style method is done as to require conspiracy by each party in order to accomplish fraud and abuse. Yet in a paper-less, digital era many of these functions are now redundant as they are provided by a decentralized cryptoledger that is immune to abuse (without a corresponding digital key); thus there is a need for *smarter* controls, not more stringent ones. Such controls would explicitly outline, by way of smart contract, the exact relationships, duties and responsibilities of each party to a transaction. This will transform traditional hierarchy and organizational structure within companies (both small and large), allowing the possibility for more horizontal, flatter firms. And typically, the flatter the organization, the fewer the transactional layers and delays between decision makers and information (e.g., removal of some information asymmetries).[181]

With the advent of CRM, ERP and other advanced accounting, auditing and HR software that condense administrative overhead, these hierarchical and organizational changes have been taking place with increasing rapidity over the past 20 years. Yet they create new challenges in terms of trust. For example, mergers between accounting, investment, and consulting firms can create blurred lines of fiduciary responsibility and accountability. Szabo suggests that trust "will erode still further as

accounting firms start taking advantage of the vast amount inside and marketing information."182 Like clockwork, throughout each year there are numerous investigative reports detailing these types of insider cases, of people being allowed access to privileged information or to execute trade orders without authorization.

General Turdgison's memorable quote regarding "Plan R" which (un)intentionally was used to bypass authorization protocols and the chain-of-command to unilaterally drop nuclear bombs against the Soviets sums up this conundrum: "the human element appears to have failed here, but we'd hate to condemn an entire program based on a single slip up."[183] Jokes aside, even if there is no intentional abuse by insiders, outside parties can still gain access to sensitive documents and information through social engineering as outfits like Lulz Security have demonstrated in a very public fashion.[184] Perhaps in an era of Bitcoin or Ripple-based cryptoledger turnkey solutions, large enterprises could not only manage access to key documents (away from the prying eyes of Alice and Bob) but easily manage physical plants, campuses and even fleets of cars through the use of proplets. There will likely even be various profitable business opportunities for (attempted) key recovery consulting.

Slowly Evolving

More than twenty years ago, automobile manufactures created the precursors to the modern electronic data interchange (EDI) standard.[185] EDI is a document standard that essentially turns paper-based business forms into electronic forms and thus acts as a common interface between two or more computer applications that enables them to understand what the documents mean. By using standardized markup, syntax and terminology (e.g., XML), organizations can quickly and cheaply send structured information to other compliant systems which allows closer integration. For example, a manufacturer can seamlessly send documents to vendors in its supply chain. Automobile and aerospace companies were some of the first firms to implement this technology as it allowed computer systems to automate what had otherwise been a manually intensive, error-prone, and sometimes – abused network of systems.

Over the years EDI has grown to digitally absorb dozens of forms such as: product and price catalogs, purchasing orders, inventory status updates, shipping orders, customs declarations and receipts. Consulting, accounting and law firms have followed suit, automating administration, billing and cost recovery systems into one standardized documentation and file format used by ECRS and LEDES software packages that have become industry standard in any enterprise of meaningful size. The supply chain industry and shipping industry are further fusing with technology through the power of cloud-based services. For example, in October 2013, Ingram Micro acquired Shipwire, a cloud logistics and supply chain management provider.[186] That same month, Pacejet Logistics raised $4.5 million in an effort to connect logistics services with carriers like UPS via the cloud.[187]

As a testament to Nick Szabo's groundbreaking work, rather than rephrasing what he has written, I recommend that all readers interested in smart contracts read his seminal piece, Formalizing and Securing Relationships on Public Networks, which deals with many of these matters in considerable detail.[188]

Though Szabo presents a holistic view of a trustless system, we should keep in mind that his view is a proposal – a visionary one, but one which will be tested by many hypothetical and real-world scenarios that will challenge the idea of trustless asset management in the coming years (and which will likely fill many volumes of writing). The influence of hackers – not of the blockchain itself, but of more

vulnerable systems authorized to interact with it – is particularly illustrative. When Alice's digital key on her smartphone or laptop is hacked by Bob and her smart contract-enabled car is sold and then fraudulently resold to numerous individuals, what recourse could she have? In an ideal scenario, the security of the car and her key would remain out of the reach of hackers, but as has been illustrated over the past five years, digital keys can be lost, stolen and extorted (e.g., the CryptoLocker virus, or unencrypted wallets being stolen from cloud storage).

In all likelihood, as Preston Byrne and another legal professional consulted on this manuscript think, market demand for consumer protection might discourage and even reverse decentralization, rather than promote it. As Byrne speculates, "there would likely be several centralised repositories tasked with verifying legal title and reversing fraud - whether those be corporate or government entities. Alice might, in this case, specify in advance which agency or court would have authority to make that decision (by possession and cold storage of the relevant private key) when title first lawfully passed to her; she might also have to pay a small one-off fee (assuming a competitive market for custodial services). Likewise, purchasers would want to be able to verify that any digital title they possessed was validly transferred and not subject to equities in favour of any third person. The blockchain would therefore need to be paired with other methods of title verification - which would likely be less expensive than the current title transfer systems in place in many jurisdictions (e.g. a state DMV). In the event Alice does not want to pay a small fee for a 3rd party, however, she could use an unregulated blockchain, but that ancient rule would apply - caveat emptor."

Chapter 5: How smart contracts could work

Theory is grey

While they do sound neat in theory, as Dr. Faustus discovered, "theory is grey, life is green."[189] One problem with institutions is not that they do not follow rules but rather that there is no conceivable set of rules that could unambiguously cover all of their activities. Thus, to minimize nebulous outcomes, it is imperative for a programmer or businessman to conduct the necessary research and gather all of the requirements needed within the design phase of a smart contract. This will be challenging one of the reasons that few known decentralized autonomous organizations exist today is that they could likely face various vulnerabilities and exploits that prevent them from carrying out their duties. In fact, in his presentation to the 2013 Turing Conference, Mike Hearn (a core Bitcoin developer) noted this point: implementing the theory is much more difficult than creating it.[190] Thus while science fiction novels and movies tease our imaginations with seemingly intelligent AI agents, creating even simple forms of non-creative bots will be a tall order.

Time Clock and Log-in

Over the past century there have been multiple mechanisms used by employees to verify that they worked a particular shift at a particular location. Depending on trust levels, an employee may only need to say hello to their boss, others may need to sign their name on a particular line in a notebook. Others might need to use a "card" that is punched with a timestamp throughout the day (e.g., when an employee first walks into the office, at lunch, after lunch and to clock out at the end of the day). And there are even other employers in the past decade that have installed tracking software on computers. While it is easy to verify that an employee is logged into the network or that an employee is indeed sitting at their desk and superficially looking at the monitor, some employers want to know exactly what is happening on each machine.[191] Thus after an employee logs into the system, the software can siphon all of the input metrics (e.g., website visits, keystrokes, files) that they create during the day or other programs that randomly takes snapshots of the screen to verify that an employee is not watching videos when they are supposed to be filling out TPS reports.[192] There are ways that each of the older "analog" systems can be abused. In the case of time sheet or even time card, a friend or colleague could be asked to stamp your card even if you do not go to work. Yet with the advent of software or even network-based tracking, it is much more difficult, if not impossible to abuse an on-site computer without making the company aware that the software has been removed or the network has been hacked.

Again, the goal of smart contracts and smart property is not to intentionally build some kind of totalitarian panopticon, but rather to enable all parties to clearly codify their responsibilities, obligations and compensation. As I described earlier in the chapter, marginalized individuals such as migrant workers in China have little recourse during contract disputes due to the household registration system (*hukou*). And they have a lot to gain if their contracts are not only tamperproof but that they can also prove in some manner if they fulfilled the contractual obligations such as on-site time.

While some requirements will be more difficult to codify into a smart contract, one area of low-hanging fruit could be the time-honored clock "punch." There are several ways to do this with existing systems: by using an RFID badge or NFC chip inside a phone, the "clock" would just have to be connected to whatever mechanism and network is ultimately responsible for sending the affirmation signal to the smart contract or DAO that automatically pays them. Another example would be to use biometric fingerprints or eye scanners to verify the employee is "clocking in" (or out) and then connect that

system to the same mechanism mentioned in the previous example. There are limitations however: for instance, if an employee or contractor gets a piece rate or must frequently switch sites throughout the day to different neighborhoods, campuses, or even cities. Creating a tamper resistant mobile check-in device that replaces the immobile clock to keep track of the number of pieces could be a business opportunity in the future.[193] In fact, through the microtransaction abilities of Bitcoin, users can send micropayments, signed with their digital key, to prove that they were in a particular hotspot for a particular amount of time.

Decentralized Autonomous Organization

As I described in the introduction, a DAO is a virtual AI agent capable of performing, fulfilling, and executing the tasks, actions, and functions normally conducted by managers and executives, such as paying bills, issuing dividends and even crowdfunding an IPO. [194][195][196] This would be done in a trustless or quasi-trustless environment, the "balance of trustlessness" determined by the intention of the parties and the capabilities of the code. By using a Turing-complete language integrated with a cryptoledger, a DAO is essentially a tamper-resistant or tamperproof entity, immune to many of the abuses and vulnerabilities that have been happening to brick-and-mortar organizations are today (e.g., burglaries, arson, unintentional exposure to proprietary documents). Currently no real decentralized autonomous organization (also known as a decentralized autonomous corporation or autonomous agent) is known to actually exist on a cryptoledger, although there are payroll bots and various software-based HR tools out on the market that integrate at the edges (BitPay).[197]

Some analysts claim that Bitcoin itself is a DAO because all of the users technically must submit a digital key which counts as some kind of voting mechanism, shareholders (miners) receive direct compensation for their work (seigniorage) – and there is no administrative overhead per se.[198][199] Yet, since development and direction of the Bitcoin protocol itself is not handled by direct "votes" it is thus more akin to a proto-DAO.[200]

But voting and separate personality does not a company make. Just like the cargo cult on Vanuatu dressed up like soldiers with the belief that air cargo planes would return with wartime goods, implementing voting into a cryptoprotocol and assuming this will create a company is a fairly superficial understanding of a corporation.[201] Because of how development has come under the purview of the Bitcoin Foundation, the current Bitcoin ecosystem is a blend between "shareholder" and "stakeholder" system.[202] This has potentially destabilizing issues in the long-term: fiduciary responsibility boundaries are fuzzy due in part to how it is funded (sponsorships) and how the organization wants to be perceived from the outside. Furthermore, like any initiative there is the possibility that the network could be abandoned by users; a company cannot function without shareholder input. This is not to say that there should not be a foundation (or many foundations) or even that a foundation could not receive money from outside sources or that users will abandon the project and network – rather, that because there is no direct voting process by bitcoin holders (like in a real corporation), the decision making process of the actual direction of the protocol itself is not an example of a DAO.

Last fall privacy advocates objected to a new "Coin Validation" project (whitelisting of bitcoins) and subsequently started the Dark Wallet and Zerocoin projects in an effort to move development one direction.[203] While core developers have differing views, there have been no direct votes with digital signatures by bitcoin holders in this process. [204] In fact, in the face of the new Coin Validation route that foundation members discussed, Roger Ver's Blockchain.info promoted Shared Coin (developed by Gregory Maxwell, a Bitcoin developer) as a way to work around potential white and blacklisting.[205][206][207]

This is not an endorsement of any proposal, but rather serves as an example of how a DAO could be used to mollify a set of actions.

Putting the DAC into DACP

Vertical institutions traditionally have created hierarchies in which intelligence and decision making is conducted at the top and automation functions based on guidance from human inputs. An illustration of this phenomenon is legacy companies that arbitrarily trim divisions to meet certain metrics and consequently often cut at the edges of the network. The lower echelons of departments in this case are sometimes viewed as replaceable or some simply lack the political capital (*guanxi*) that other departments may have had. However, this dynamic all changed when Bitcoin introduced the idea of autonomous distributed consensus, automation at the center of the network and intelligence on the edges.

Unlike in a legacy company where decision-making authority is concentrated at the executive level, in a Decentralized Autonomous Consensus Platform (DACP), the decision-making authority is part automated, in that it has specific rules that are followed without possibility of deviation from expected form, and conversely human interaction and bias is limited to the edges.[208] In such a model, power and authority, rather than being collected at the top, is spread to the edges of the network by allowing key holders (or VoiceHolders) to influence the decision-making and priorities of the DACP proportionally with their preapproved voting rights (e.g., when setting up a firm, a voting structure is put in place usually based on the amount of equity or shares an individual has).[209]

The legal liability and responsibility of a DACP or DAC still trace back to the key holders who sign their digital keys with a DACP which then calculates results based upon the prearranged voting proportionality. For example, Bob's Boutique requires that the allocation of special funds used by the DACP to hire contractors must be approved by a threshold of digital signatures. If the threshold is unmet then the DACP does not release the funds to hire the contractors.

Software-based solutions used to calculate, authenticate and verify shareholder votes for many corporations and organizations already exist yet most still rely on a trusted 3rd parties and are susceptible to social engineering and man-in-the-middle attacks. Thus, one opportunity for e-voting enterprises is to build consoles and virtual applications that utilize a cryptoledger, allowing members of organizations and institutions of all sizes to securely sign policy decisions. To prevent internal takeovers and allow for quick dissolution (e.g., to manually reallocate assets), a self-termination clause could be programmatically designed within a DACP that could be triggered if enough shareholders submit signatures (or Voice) to a specific internal address within a specific timeframe (nLockTime).

In another real-world example: a DACP can be created as articulation of an assurance contract based upon a predesigned outcome, those who agree with the sentiment send funds to the DACP (the fundraising) and after a value-threshold is met, the DACP acts to bring about the desired result. Funds that are raised during this process are not releasable until a threshold (e.g., 51%) of those who put the value there in the first place, or those who purchased extra shares (e.g., giving larger voting pools) agree to both the need for the expenditure, and the final product being submitted for reimbursement.

Again, as mentioned in chapter 4, although this may sound futuristic, these autonomous platforms have no "artificial intelligence" at the top of the pyramid. Where the capstone used to be the ultimate centralization of power, in the words of Adam Levine, "now it is only the nexus point for consensus from

those participating further down the structure." It has the ability to spend funds, but only at the direction and authorization of the majority of shareholders. Just like Bitcoin, DACs and DACPs are consensus driven, rules-based systems. To be part of the system, according to Levine "is to follow the rules, so there can be no pre-mining, no individuals with privileged status at all. Privilege is the antithesis of efficiency, and these structures seek efficiency above all things."

Below is a rubric designed by Levine in his forthcoming paper to describe a hypothetical DACP assurance contract:

1. DACP specification is proposed with Kickstarter Address collecting Ethereum/Bitcoin
2. Received funds comprise development funds and initial DACP monetary base
3. Kickstarter Address hits funding threshold and DACP Proposal Hub bounty is issued and rewarded by DACP consensus
4. Proposals to develop DACP are created, and one or multiple are accepted
5. Completed bounties are reviewed, and bounties are released by prearranged consensus. DACs cannot integrate submitted bounty solutions until the winner has been paid.
6. Once the platform is created and operational, DACP token holders can sell their tokens for Ethereum/Bitcoin at current market rate, hold it to speculate on the platform becoming more popular relative to the fixed number of DACP tokens, or exchange their DACP token with the DACP itself for DAC token as described above.

Experimental Cases

What a DAO could do is actually execute the contract based on pre-agreed to conditions. If a digital signature counts as a vote, the only way to modify what a DAO would do is to get X amount of votes to approve some kind of execution process. The specific amounts are hardcoded into the program beforehand and perhaps some are weighted differently. To a limited extent, multisignature transactions, also known as m-of-n transactions (e.g., "joint bank account" "multisignature lotteries"), already work with Bitcoin itself, although again, you are limited to around 10,000 bytes, which would not be enough to fit hundreds of "votes."[210]

Multisignature authorization of transactions is not a new concept as it has existed for hundreds of years in every corner of the globe. This is done, as Szabo pointed out in chapter 3, to force conspiracy to take place in order for abuse to be undertaken. That is to say, no single individual has the unilateral ability to abuse the treasury of an organization (or launch a ballistic missile).[211] For example, using the Bitcoin protocol today as established by the built-in rules of Script (the name of the internal language), three parties could sign a contract which is programmed to release funds so as long as it receives the digital key of at least two of the parties. As a consequence, this makes the Bitcoin protocol the legal system as it is impossible to use the tokens without the signatures. Or in other words, if Bob operates a small company he may need to have 2-out-of-3 executives sign a document in order to release funds to pay for warehouse expansions. With cryptocurrencies, the same idea applies wherein to move a ledger value (a bitcoin) to a different address, a smart contract or DAO that holds and controls "locked" tokens needs a predetermined amount (threshold) of digital signatures to release them.[212] While it is not a DAO, Bits of Proof has developed software that provides this type of 2-out-of-3 reconciliation with a company, Bullion Bitcoin.[213]

In the future, a small auto-body company could create a DAO on the Ethereum ledger (or Litecoin, Bitcoin, etc.). The company has five executives, each with a digital key needed to utilize and modify the

cryptoledger. Based on the company charter (and as specified in the smart contract or DAO), at least three of the five are required to use their keys in order for the tokens within a DAO to be used. After a company meeting, an agreement is made to use the funds and three executives – Alice, Bob, and Carol – are asked to use their digital signatures (keys) to tell the DAO to release a certain amount of tokens. Utilizing their smartphones (or any network connected device with an app tied into the ledger), they then submit their key and the funds are released.

This can scale up in the case of shareholders of a company. Unfortunately as noted above, the current Bitcoin protocol has technical limitations that prohibit hundreds of digital signatures being sent to a specific address. Yet other projects like Ethereum could potentially enable hundreds or thousands of signatures to be sent to a DAO. This then could enable shareholders to vote on specific policies. For example, if the board of a shoe manufacturer wants to expand production of a new running shoe that requires the use of tokens managed by a DAO, based upon pre-approved programmatic rules, they would need to bring this up for a shareholder vote. A DAO could be preprogrammed to fulfill specific functions based on voter thresholds, like a majority or supermajority of votes (51%, 67%, etc.). In this example, if there are 1,000 shareholders altogether, the DAO which was programmed with a 50.1% threshold, would only release the tokens if it received 501 digital signatures from all shareholders.

Peercover

In January I spoke with Jared Mimms who is working on Peercover, a startup that allows anyone to become their own decentralized insurance company.[214] After months of work, they created one the first known smart contracts using a cryptoledger, interfacing with Ripple.[215] According to him, "Peercover's goal is to allow for a sandbox where people can chain smart contracts together and produce profit bearing assets (companies) without having to code. This mean the companies provide valuable services and are simple for people to use and join once companies are founded. Peercover has developed a series of what they call "company types." Each of these is really just an "algorithmic framework" for a company, including an "offer system" that allows founders to invest in companies by chaining 3rd party services to them to make them more attractive to join. Finally, a built-in trading system and soon to launch Simple Stock market allows founders to sell portions of their assets and investors to easily trade equity and reap automated or manual dividends." Mimms claims that Peercover is "the first true contract client in the space" which likely will increase competitive attitudes from other projects.[216]

With respect to smart contracts more broadly, Mimms says, "these types of instruments could provide a real opportunity for decentralized innovation. Specifically, I saw how cryptocurrencies can allow for the automation of superfluous corporate functions. And to accomplish this I began working with Peercover, where we can provide customers and entrepreneurs the ability to trade through gateways (via Ripple) without having to build and manage an entire backend. Ripple has an open API that we use because currently it is the most efficient and robust at enabling truly decentralized merchanting with low confirmation times compared with competing APIs that can take an hour per confirmation."

Ripple Labs open-sourced the Ripple protocol last fall; the Ripple network has confirmation times between 5-15 seconds versus several minutes for blockchain-based ledgers.[217]

"For our first "smart contracts" we initially focused on peer-to-peer insurance companies – contracts – because of the new Obamacare mandates. That is to say, there is a noticeable absence of insurance startups in healthcare and our platform makes it easy for companies to build their own custom solutions. While we call them "companies" they are essentially a simple decentralized autonomous corporation

(DAC). Furthermore, one of our current plans is to integrate social networking functionality within Peercover to allow people (developers, customers, merchants) to talk to one another. As a consequence, part of this process will require taking necessary steps to prevent fraud, thus we will verify people's identities. This may sound easy but as we have learned with working on various altcoin projects, if there is money involved some people will go to great lengths to commit fraud by forging and doctoring "official" photographs."

The DAC claim is quite bold as no other team besides Invictus has announced any such development in a production environment. And while legal compliance issues such as Know Your Customer (KYC) compliance have briefly been mentioned in passing; authentication has been a hurdle for other parts of the ecosystem, especially involving exchanges.[218] According to several investors I spoke, maintaining KYC databases will likely become outsourced to firms that solely focus on this area of law.

Altcoins such as Dogecoin and altprotocols such as NXT surprised Mimms and his team this past year and he credits these two specifically for introducing a new marketing mechanism and potentially new platforms. It is through these experiences that "we have learned to become adaptive and open to new cryptocoins and cryptoprotocols. Because of our trial-by-fire experience, we can integrate with a new altcoin or altprotocol within a few nights whereupon we then provide users with a very flexible sandbox and drag-and-drop functionality to all users. For example, if you own a bicycle repair shop you can create a customized contract that enables funding options, stock issuance, dividends and even discount management (e.g., 20% coupons to all users). We are also the first company to actually create contracts that allow for accredited investors to create crowdfunding in compliance with SEC laws. That is to say, instead of paying an investment bank like Goldman Sachs or J.P. Morgan to IPO your stock, you can do it yourself through a $200 kickstarter on our platform. You can issue dividends and allow other people to hold shares."

This crowdequity meme is also discussed in chapter 7 with examples from BankToTheFuture, JoinMyIPO and LTBcoin. How the legal issues will be resolved in countries such as the United States is also an aspect to look into if your company is interested in this competitive space (e.g., allowing non-accredited investors to invest).[219]

Looking toward the future, Mimms says that Peercover has "also begun development towards using Watson-like functionality to provide fully autonomous customer service. As a part of this effort, we have begun implementing tools such as a "tax" tab that will automate the amount of taxes to be withheld (e.g., a percent based on regional sales taxes that can be sent to specific cryptocurrency address). While Ripple Charts users themselves are creating and executing contracts – which we build from, we have also partnered with BIPS, a large European-based payment solution provider in this space."[220]

Watson is a natural-language processing system developed by IBM and was popularized in a 2011 series of competitions on Jeopardy in which it beat two championship level human opponents. IBM has subsequently improved on its abilities and plans to integrate the system in the healthcare industry.[221] In addition, automated tax tools are another relatively "simple" area that several developers and investors mentioned that could be relatively easy for development and production.

Continuing, "While other platforms have noble goals, we think a decentralized 3rd party tools creates too much unnecessary complexity for end-users."

Thus the takeaway message from Peercover's experience seems to be, "in contrast, what we think is going to win is to have a sandbox-based platform that integrates fees where anyone can create and manage – with advanced interfaces – blindingly simple contracts. For instance, we had one customer who raised $30,000 in two days with just $200 in kickstarter fees. The technical backend, how it is done is not necessarily relevant to the minds of users who do not have time or the knowledge to fine tune the infrastructure. And in the end, if your goal is to decentralize banking, keeping it simple is probably the number one issue developers and entrepreneurs should continually pay attention to."

Subledger

The ability for a centralized platform to tap into decentralized processes is also being capitalized on with another project called Subledger.[222] Subledger is an in-application accounting API that enables developers and businesses to integrate financial databases, including those based on cryptoprotocols into a double-entry real-time ledger analytics engine.

In February I spoke with Tom Mornini, co-founder at Subledger and according to him, "Applications make entries into Subledger for every transaction, in real-time if possible. It's then easy to share account records with the parties they represent, such as customers and vendors. That builds trust by eliminating the need for it, just like the blockchain does in cryptocurrencies." They have also refined segmentation so that customers have individual accounts for anything that needs to be tracked; we only aggregate during reporting. Furthermore, the system never updates old entries and completely documents each transaction to maintain an audit trail."

Continuing, "most people think accounting is about money. While it is nearly universally used to track money but it's really about tracking state changes of units of account which are not necessarily money."

Furthermore, ignoring the time to close (e.g., the lag time between the close of a quarter and the close of the books) is a huge problem with currently deployed software. "The time to actionable information is critical for all companies. The effort to audit is also greatly reduced, which also means less expensive, and auditing can now take place in real-time. Auditors could verify a percentage of transactions every day, hour or minute and, essentially, continually attest to the accuracy of the information."

He also sees at least one competitive advantage between Subledger (a trusted 3rd party) and DAOs, in his view, "the distributed autonomous organizations will be more expensive per-transaction because of the consensus overhead. If there's no counter party, there's no reason to pay that overhead, which also requires the information therein to be public knowledge. I'm not clear that a DAO would want its internal cost accounting to be shared publicly. In some cases, yes, in other cases, perhaps not."

Perhaps developers in this space can leverage a service like Subledger to provide a SaaS-based automatable system that integrates with an intranet-based cryptoledger as described later in chapter 8. In the wake of Mt. Gox's bankruptcy in February, which appears to have occurred in part due to a lack of internal accounts reconciliation practices and metrics, perhaps future exchanges could utilize a DAO or a CAO to provided quicker information to decision makers.

Where the Rubber Meets the Road

Currently it is difficult to foresee how the arbitration mechanism in a DAO would initially help anyone in China or other jurisdictions. After all, who or what would enforce its decisions? Or, if you used a DAO, what clauses could you include that hedge against the uncertainty of a potentially untrustworthy party?[223] In terms of payment, fool proof clauses must be written into a contract that specify what exact channels or addresses the funds will go through and at what specific times. While direct deposits are common on the mainland, it is not unheard of for unscrupulous employers to change bank accounts in an attempt to not pay debts. Yet, cryptoledger-based escrow and bank providers may find new opportunities in this segment.[224] And there are other options such as atomic-based transactions or atomicity in database parlance.

Michael Goldstein, founder of the Satoshi Nakamoto Institute, wrote a concise explanation of what an atomic transaction means:

> Two parties agree to exchange one cryptocurrency for another, and the transaction is done in such a way that neither side can execute their portion of the trade without releasing funds to the other party. The trade either happens in its entirety, or not at all, which means nobody can walk away empty-handed. The worse possible outcome is that no trade occurs at all and everybody keeps what they had.[225]

You can substitute "cryptocurrency" with any kind of token (metacoin, colored coin or even a smart contract) that is capable of performing the same function. Previous such atomic transactions have taken place in other systems such as with airline bookings. A potential passenger must both pay for and reserve a seat or neither pay for nor reserve a seat. A booking system will allow one option to occur and not a mix.

Using existing technology plus atomic transactions, there are several ways an employee and employer could resolve payment disputes. In a small business between friends, family and other trusted parties, the formalized contract steps could be minimized. A simple contract might look like this: working from home (it could be any arbitrary location) Bob builds a website for Alice and thereafter uses 0.0001 bitcoin (or litecoin, etc.) to generate a temporary token of arbitrary color, size or type but which represents a predetermined, pre-agreed amount of value – a temporary "labor" coin – and sends it along a cryptoledger to Alice. Later that day, Alice looks at and approves of the website quality and subsequently sends Bob a token of predetermined value worth $500 (the exact amount is based upon a previously agreed to amount) and utilizes the same cryptoledger (although it does not necessarily have to). Both tokens have a function called nLockTime built into them for twelve hours (these time values are arbitrary). If both tokens are sent and received during that twelve hour time period, then the atomic-transfer takes place and both receive the other token. Alice scraps the token she receives because it was a mere abstraction of the labor Bob provided (she can keep it for accounting purposes if she wants). Bob on the other hand can then exchange his token to any fiat exchange, token exchange (Cryptsy, Bter), or perhaps even a merchant.

Again, this was simplified to illustrate how the atomic transaction works. In this case, if one or both parties did not send their token in the allotted time – none of the tokens would be received by the intended parties. Instead, the ledger would send it back to the originating wallet address. For example, if Alice did not send a token, the next day Bob would wake up and see that he has not been paid and his "labor" token was sent back. He can then talk to Alice to find out what the issue might be; after all, he

would like to be paid for his labor. In reality, as well as this example, it is possible for both Alice and Bob to use different cryptoledgers so long as there is some mechanism like a web exchange that has the ability to process both types of tokens.[226]

And so long as there are decimal units in a particular token, the logistics of sending value can be scaled up, for all practical purposes, near infinitely and potentially infinitely (assuming scalability issues can be overcome). Even if all seven billion humans (plus DAOs) immediately began using one particular cryptochain that used just one specific base token (a bitcoin, ether, etc.), they could send fractional token sizes (e.g., 0.00001) to other parties. Each individual (and DAO) could also include a secondary attribute in a "hash" or code snippet to identify what asset this token actually is meant to represent, such as cars, commodities, "labor," and fiat (e.g., using metadata to turn 0.0001 BTC into a "blue" token or some other random attribute that acts as an abstraction to an specific asset).

Abstractions and Decimalization

Consequently because of this decimalization, the virtual economy should never run out of base tokens in the money supply.[227] This is not inflationary, as no new base token is created that is not tied to some particular asset. The underlying foundational token is still tied to the scarcity of the original money supply. Furthermore, there are built-in anti-spam functions in existing cryptoledgers that require minimum transmission values, below which a transaction is not permitted along the network – this is known as the dust limit.[228] And again, with Bitcoin, every 10 minutes 25 bitcoins are "created," in Litecoin, every 2.5 minutes the same amount is created. Other cryptochains have their own known, invariable money supply creation rates, but this is not important as the fundamental ideas are the same in that these tokens can be further subdivided into increasingly smaller decimal spaces and also given a second attribute to represent a different asset. Similarly, additional DAO-based banks and escrow services could provide functions if atomic-transactions are not agreed upon beforehand.

At a large enterprise for instance, Bob, a graphic artist, arrives at Adobe (his employer) and logs in with an RFID badge at the front door of the office. The clock sends an encrypted signature to an HR DAO run by Carol's independent escrow that creates a timestamped ledger entry on the Bitcoin network (or Dogecoin, etc.). Bob's computer is also fitted with software that can monitor his inputs, which are stored on Adobe's SAN (while this verification role is redundant, Bob could also later point to the information gleaned as proof that he worked). After completing his assignments Bob again, clocks out with his RFID badge which sends another encrypted signature that generates a token that represents one day worked. The color or type or size of token is irrelevant as it is merely a representation of an agreed upon completed condition. Alice, his supervisor can later send her own signature of approval (or disapproval), which is then sent to Carol's DAO. If approved, the token could be released and sent to another independent DAO, Dan's bank, which stores tokens held in escrow on behalf of Adobe (e.g., n-of-m). Once both tokens are received, the transaction triggers a time-based predetermined, pre-agreed settlement clause between Carol's escrow services and Dan's bank whereupon Carol sends Dan's bank the "labor" token (which could be discarded or held for accounting purposes) and Dan's bank sends a pre-agreed token (e.g., a bitcoin worth $500) to a prearranged wallet address that Bob controls with his private key (e.g., his bank account). Dan's bank could also send the token through other DAOs, this was just one illustration.

As you can tell, this type of system could be used with any amount of time lock, including years – hence the long-term potential uses of managing trust funds and the execution of wills. For example, Bob has $1,000 and would like to give it to Alice, his 1-year-old baby daughter, when she turns 21. Bob has

several choices. He can immediately exchange the $1,000 in fiat for a token (e.g., bitcoin) and place it in escrow. He could deposit the fiat into a bank and fill out a smart contract with the bank that provides a time-based disbursement condition (e.g. in 20 years, spend the $1,000 and purchase an equivalent amount of bitcoin and send it to Alice). He can deposit the fiat into a bank but then create a smart contract-based financial instrument with a fraction of a bitcoin (0.0001) which may cost him a few dollars now and send the smart contract to a DAO bank where it sits until a specific date is triggered. He could also simply exchange $1,000 fiat for a bitcoin token today and leave it on the cryptoledger using an "external state contract" because the nLockTime function is already built into the protocol and the token will automatically go to a prespecified address at a specified time (e.g., in 20 years it will be moved to an address controlled by Alice or Bob).[229] However, Bob should also be aware that if he signs and broadcasts the transaction far into the future there is a chance that some nodes may choose to drop the transaction in the memory pool. If he uses an escrow, he can also create a smart contract that lays out the specific conditions, the terms to which a token is allowed to be sent to a pre-specified address (perhaps Alice has her own address, or maybe she is given access to his in the event he dies).

Another way to handle an inheritance with the existing blockchain is through an entity called an "oracle;" an autonomous 3rd party agent. In his 2012 presentation Mike Hearn described an independent, trusted oracle system that is set up to monitor the obituaries section of a government agency or newspaper, whereupon it can relay identities and information to a contract on a cryptoledger. Or in other words, the oracle listens and uses that data to sign a multi-signature contract and in order for the contract to release funds to the beneficiaries, it needs a signature from the oracle. The contract had previously been signed by the original trustees who require a signature from the oracle to release funds to predetermined beneficiaries.[230] Last year Michael Goldstein described another oracle involving a sports bet: Bob bet that team A would win and Alice bet the other team would win.[231] An oracle holds the deciding key to a contract that says if team A wins, Bob receives the funds (bitcoins) and if team B wins, Alice receives the funds. The parties write the contract noting how the transaction should proceed in the event of disputes or potential ties. Then after the event is over an oracle signs it removing the middleman. Unlike ordinary legal disputes involving nuances and grey areas, sports betting is an objective, idealized scenario because there is no grey area as all that an oracle would have to do is have access to an ESPN data feed.

Mitigating Abuse

Other near-term uses within a cryptoledger are loyalty programs, merchant reward programs and "Frequentfliertokens" from Alice Airlines which could help prevent and mitigate the risks involved in travel hacking (e.g., getting frequent-flier miles without flying).[232] For example, United Airlines frequent-flier miles were downgraded effective February 1, 2014, due to rampant inflation caused by a combination of website vulnerability exploits and quick scheduling changes by users.[233]

Instead, Alice Airlines could offload the auditing, storage and transportation of rewards and utilize the "contract" system of a cryptoledger by using an arbitrary amount of a token (0.01 BTC), creating a "contract" that defines a set amount of mileage (which itself will likely have some predefined expatriation dates). Assuming that flyers are using cryptocurrency wallets and provide the airline with their wallet addresses, the users will be able to receive the mileage amount in their wallets.[234] In turn the users can sell and trade the reward tokens by sending a specified amount to Alice Airlines.

Other institutions can use a smart contract to issue and track its own customer loyalty program rewards.[235] For instance, in 2005, Subway ended its sub club stamp program whereby a customer would

receive a couple of stamps (stickers) for certain purchases. When a customer collected a certain threshold of stamps, he or she was eligible to receive free food (chips, drinks, sandwiches). Yet, a number of customers found a way to game the system by buying and selling entire reams of stamps on eBay, creating massive stamp inflation costing the parent company an unspecified amount in losses.[236]

Thus, coupons are another ripe area for development. According to NCH Marketing, "Consumer Packaged Goods (CPG) manufacturers distributed 305 billion coupons in 2012, the same quantity as the year prior. […] total redemption for 2012 fell 17% to 2.9 billion coupons, saving CPG companies a substantial $800 million in face value discounts."[237] While this may seem like a mundane area, consider that by 2016 Juniper Research predicts that "the total redemption value of mobile coupons will exceed $43 billion globally" because coupons are increasingly delivered by mobile apps.[238] For perspective, 48% of adult internet users in the United States redeemed a digital coupon for shopping in 2012.[239] A company providing coupons or discounts could create a DAO to manage these redemption contracts (e.g., a type of time-locked token), which will not only reduce the logistical overhead but also prevent coupon abuse and fraud (e.g., double-spending). According to the US postal inspector Roberta Williams, "for every coupon successfully counterfeited, it costs the manufacturer $1 million."[240] Initially these fake coupons are scanable but the coupon inflation ultimately forces manufacturers to redeem more than they had intended. Furthermore, the Coupon Information Corporation (CIC) estimates that coupon scams create losses of $300 million to $600 million a year – and that these costs end up getting passed onto consumers.[241] Yet, if there is one function that the algorithms governing Bitcoin money supply have proven adept at, it is preventing inflation.

While not directly related to fraud prevention, one real world case-study within this overall segment began in February 2014. PointsHound, a site that rewards travel reservations with frequent flier miles and hotel points, announced that it had begun using bitcoins in its payout system. If a user selects the bitcoin payout option, PointsHound calculates the reward based on the market price listed on Coinbase and then sends the amount to the user's wallet. According to cofounder Pete Van Dorn, "We carve out a portion of the commission to give back to the customer in the currency of your choice. It might be 5,000 miles, it might be Bitcoin."[242]

The Tao of DAO

In developed regions, market participants are familiar with computer software that uses, runs, manages, and executes nearly all of the financial instruments on electronic stock exchanges – and how there are various clauses written into them to hedge against (or prevent, or in case of) some type of counterparty risk. Below we will look at how that functionality can be designed into a smart contract with a normal contract at a normal job or even one that a Chinese migrant worker may do.

One way this might work: Bob, an employee, would use a digital key to sign a smart contract with his boss Alice, who also uses a digital key to sign it.[243] Within the contract will be a number of provisions and stipulations regarding payment time periods and clauses that hedge against the possibility that one party does not fulfill his or her end of the bargain. Perhaps there will be a clause that says how payment will actually take place: through an escrow service (BTCrow), through bank X, through address Y, or a mix of different options. This contract could be stored on a public decentralized cryptoledger (e.g., Bitcoin, Ripple).[244] If stored on a cryptoledger it is tamper proof and forge proof as it sits there immune from 3rd party interference. Again, while most people think of Bitcoin as a currency tracking tool, in arithmetic terms it is more akin to a database that can be used to track any particular dataset (e.g., a bitcoin) as long as it fits within the technical limitations. It just so happens that the sole data this past

four years has been for one particular "token" as represented by an integer on the ledger (i.e., bitcoin).[245]

While there is a way to change the way the DAO could operate by convincing the rest of those with votes to modify it with their private keys, the original contract would still be left in public view and untampered with. What could happen is that contract itself would have an nLockTime (time-based) clause or condition that after X amount of time, if certain conditions are not met (for example, payment) then it would follow some predefined termination clauses. Perhaps it would send itself to a predefined arbiter or escrow DAO. While it is doubtful that smart contracts will solve all of the problems on the edges of a network (e.g. brick-and-mortar infrastructure), it will prevent tampering with the actual contract itself thereby protecting employees (and employers) from trusted 3rd party risks such as fraud.

So in a nutshell, ignoring other aspects of asset management, the following scenario could take place:

Bob digitally signs a smart contract with Alice stipulating various expectations, terms of compensation, etc. This contract stipulates that payment will go through various channels each month, however if there is a breach of contract it will end up with Cathy's escrow service (which itself could be an independent DAO). In fact, there will very likely be several virtual escrow services that need to maintain a good, honest reputation to do business (just as they do today). Furthermore, there will likely be a dispute-mediation clause regarding independent arbitration if all else fails (just like today).[246] By “all else fails,” I mean there will be a time-based trigger: if neither Bob nor Alice re-sign clause B, C or D by a specific time in the contract located on the ledger, the contract is sent to Dan the arbiter or Eve at the public court. Dan could, like an independent escrow service, be chosen from a list of known reputable arbiters who face similar market conditions to provide unbiased service (net-ARB is a type of service like this).[247]

These types of default-based relationships and contractual stipulations take place today. While it may be difficult to initially "codify" them into software, it is likely just a matter of time: last year Coinsigner became the first cryptocurrency-focused dispute resolution service using multi-signature transactions.[248] In fact, the barriers to entry are low enough that individuals can create independent mediation resolution practice to provide objective, unbiased fair decisions and any three people can employ it, across borders. Whether these systems will be commercially viable for enterprises of significant scale is, however, as mentioned several times in this manuscript, very much an open question.
If stricter capital controls and regulations on cryptocurrencies are enacted in China (or elsewhere), by using a couple different “colored” coin chains (or other ledger contracts), Bob from Beijing could potentially transfer assets worth X amount of money to Alice from Anhui instead of X amount of money itself.[249] This could create a sort of advanced barter system which may not be as efficient in terms of actually using a cryptocurrency as a medium of exchange but it could help those in an informal economy qualify and quantify asset value and clear up some of the confusion around contracts and property ownership.[250] Yet how those contracts will be enforced is also an issue that will likely fill volumes, as any institution providing such service will be a target policy oversight, just like the exchanges are now.

At the same time, there are some uncertainties and legal risks which will vary from one jurisdiction to the next. In China, it is hard to speculate how the various townships, counties, municipalities, provinces and the central government itself will recognize this type of ledger-based asset management. Twenty years ago, most Western commentators believed that the internet would empower the average Chinese resident to maneuver around censorship, but the Great Firewall has proven very capable of stemming the flow of all information.[251] While it would be difficult for them to block such decentralized peer-to-

peer activity perhaps each government layer will instead want a small piece of the transaction and only recognize smart contracts that go through specific government-run DAOs or corporate custodial escrow and arbitration services with a contractual nexus to real assets and a national system of law and enforcement, as suggested by Preston Byrne in chapter 2.

Chapter 6: Fundraising Landscape

According to CB Insights, venture capital (VC) firms spent $74 million across 40 Bitcoin-related deals in 2013; the two largest rounds were Coinbase ($25m) and Circle ($9m).[252] Similarly, Garrick Hileman recently published data and found that roughly $97.5 million in VC funding went towards 36 Bitcoin-related startups during the same time frame and his findings are discussed below.[253][254]

Despite the increased media attention, even if these numbers are repeated again this year this may not help boost the performance for some VC funds.[255] Even with the optimistic outlook many of the VC firms apparently now have their actual results at roughly 6.2% per annum over the past decade they have underperformed the Russell 2000.[256][257] Why? This is not to disparage the VC segment, rather like all industries some VCs are not as nimble at feeling and filtering out business models with revenue generating capabilities as many angel investors are.

Changes over Four Decades

Consistent with the theme of ubiquitous adoption of open-source software as well as cloud computing that has lowered the cost of developing software and (more importantly) the costs associated with launching new companies, so too has this trend lowered the threshold for technology for startups and investments. Where previously the funding of start-ups was limited to deep-pocketed professional investors, namely VCs, the deflationary landscape has increasingly enabled greater numbers of individual investors – angels – to compete in the funding environment.

The new class of angel investors is more astute than the passive and non-tech-savvy high-net-worth investor of yesteryear. Increasingly, angel investors today have deep domain experience. Many have worked in the sector that they are funding, are entrepreneurs and experienced operators themselves and visionary at feeling out new business and innovative trends. The historical barrier to entry for angel investing is one of risk quantification (followed by knowledge and coordination) given the magnitude of investment commitment. With lower costs of starting businesses, this hurdle is largely gone. Having angels with deep operational domain expertise is disruptive to the traditional VC universe. They may be better attuned and friendlier with terms that are less predatory than the historical VC norm.

This is not to say that VCs will not flourish once again, however, as it stands, most angels began as entrepreneurs and learned how to generate sales and revenue firsthand. Furthermore, as noted above, over the past decade technological costs have driven down expenses. For example, relatively cheap cloud services like github and Compute Engine provide services (CaaS, SaaS and IaaS) that allow many tech start-ups to be leaner than before in terms of what funding they require to cover operating costs.[258] On top of this are better organized angels who now have an entire ecosystem of choices to fund through such as AngelList, 500 Startups, Plug and Play, Y Combinator, SVAngel, Bitcoin Opportunity Fund and Boost.[259] In fact, over the past six months, BitAngels.co have invested $7 million in 12 crypto-related projects globally and Plug and Play is providing both mentoring and seed funds of $25,000 to bitcoin-related ventures.[260]

Another way that cryptocurrency-related startups are being funded is crowdfunded IPOs. This includes Mastercoin, which raised (at the time) $5 million in part by 4,700 bitcoins from “investors.”[261] NXT and the upcoming Ethereum IPO have also included raising funds through bitcoin transfers.[262] While I am not necessarily endorsing any of these particular fundraising models, this illustrates how small (and perhaps large) development teams can financially cover costs without seed funding by VCs. And, in

addition to crowdfunding sites like Kickstarter and Indiegogo, there are also sites that allow individuals to receive Bitcoin funding directly for their ideas, such as BitcoinStarter and CoinFunder.[263]

Consequently, it is premature to write off VCs or claim that angels are the only source to pool funds from. In fact, a substantial amount of series funding over the course of the last two years in the Bitcoin realm has been from VC firms. For example, Andreessen Horowitz has invested nearly $50 million in Bitcoin-related startups, including leading the $25 million round for Coinbase last fall.[264] In February 2014, Marc Andreessen – the firms founding partner – explained to CNBC that,

> "[Bitcoin] is mostly new opportunity. For example, there is a lot of ecommerce today that just doesn't happen because a lot of people around the world literally aren't in modern payment systems where they can't pay for anything. There are a lot of merchants that can't be profitable in a lot of categories because transaction fees are too high. It's a huge opportunity and everybody has the opportunity. Bitcoin is an open technology, it's open source, it's freely available – anybody can participate. So every established business that wants to take advantage of it, including people like Western Union, can do so."[265]

While it is too early to predict how these investments will exit, VCs are still a potent market force.

Venture Capital Charts

In addition to the findings of CB Insights above, below are four charts reprinted with permission from Garrick Hileman which were originally published on February 24, 2014:[266]

Amount Invested ($m)

Stage of Development	2012-Present Total
First Sequence Financing	$72.50
All Other Deals	$25.00
Grand Total	$97.50

Number of Deals

Stage of Development	2012-Present Total
First Sequence Financing	35
All Other Deals	1
Grand Total	36

Chart 1: VC Investments in Bitcoin Companies, 2012 - Present

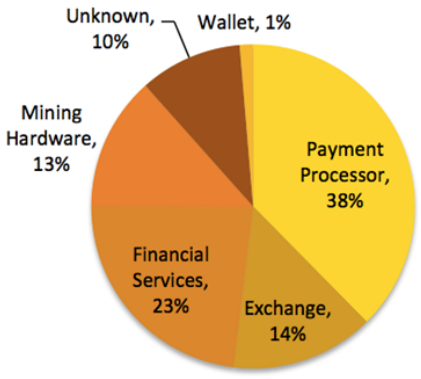


Chart 2: Sector distribution of Bitcoin VC investment

As Chart 1 (or rather Table 1) notes, this is the total of the known venture capital funded Bitcoin-related companies globally since 2012.

Chart 2 illustrates the division of what specific segments those companies are categorized under. In his analysis, Hileman noted that mining hardware companies have generated over $200 million in revenue to date. The unknown segment is for undisclosed projects that received VC funding.

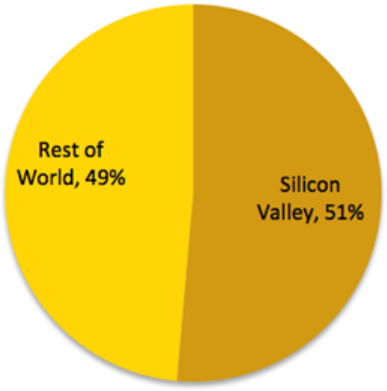


Chart 3: Silicon Valley vs Rest of the World VC $s Invested in Bitcoin Companies

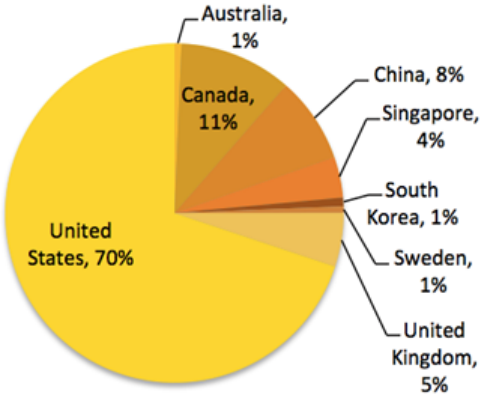


Chart 4: Country Comparison - VC $s Invested in Bitcoin Companies

Chart 3 illustrates that as a percentage of the total VC funds, what geographical location they are located.[267] Silicon Valley (i.e., the San Francisco Bay Area) based firms have received the lion's share, at 51%.

To produce Chart 4, Hileman looked at the total value of the VC-funded projects ($97.5 million) and the chart shows the geographical dispersion of these funds; US firms received 70% of those funds. While these numbers will likely continue to increase over the next year, it is unclear if the geographical trends will continue.[268]

Straight to the Source

Jeremy Liew is managing director at Lightspeed Venture Partners, which has invested in several startups in this space, including Ripple and BTCChina, and anchored the Boost BitCoin Fund.[269] According to him, "I think that there are three use cases that will lead math based currencies to mass adoption. 1) Microtransactions (perhaps for online content, perhaps for digital goods in games) which are impractical using credit cards; 2) Cross border transactions (both C2C as in remittance, and B2B for import/export and ecommerce) where transaction fees are high; 3) Leapfrogging credit cards for ecommerce and m-commerce purchases in the developing world. The developing world leapfrogged fixed line telephony to go straight to mobile telephony and that is the model that I would anticipate for math based currencies leapfrogging credit cards. Today a common form of payments for ecommerce in Russia, China and India is "cash on delivery" and that likely is the first payment method to be replaced by a math based currency."

In terms of what specific segment of this space LSVP is interested in, "We are still in the infrastructure phase, making math based currencies easier to buy (exchanges), hold (wallets) and spend (payments). And of course to speculate on. The infrastructure will need to mature a little more before applications can be built on top of them to be able to drive mass adoption. Then it would be the three themes from earlier." Yet as to trying to predict which platform or what technology like smart contracts will spring forth, "I don't know, all I know is that it will be exciting and transformative. Just as no one could predict the explosion of uses that got sparked by VoIP when we were still on POTS, so too it is impossible to predict what the "programmable" part of math based currencies will bring. But it will be awesome."

He raises a visceral point about unexpected innovations and their knock-on effects; Skype calls alone are now equivalent to one-third of all global phone traffic, providing new tools and lower transaction costs to every demographic group.[270] Similarly, digital goods such as music, movies, games and books – a market that barely existed a decade ago – is expected to reach $80 billion in turnover by 2015 in the United States alone.[271] In fact, according to Ofcom, 11% of American internet users regularly pay for digital online content.[272] During my exchange with Mike Hearn, he expressed similar sentiment in terms of the untapped business opportunities in this space, noting that "right now it seems there are a billion startups exploring every possible angle on these ideas – most of the work that needs to get done though is fairly boring infrastructure type stuff." Laying the foundations for these platforms could be a business opportunity for the next several years.

As mentioned in chapter 2, Ryan Orr is a professor at Stanford University and chairman at Zanbato that is a partner in a new crypto-based incubator called CrossCoin Ventures. He noted that, "with the recent wave of regulatory actions, I am personally feeling quite excited about how the "smart property" projects evolve in 2014. It is starting to feel like smart property could be a much lower path of resistance for the bitcoin protocol as it establishes a "non-monetary" form of use that fulfills a valuable social purpose. And thus it should not be viewed as a direct threat by regulators who are afraid of losing monopoly control of money. It is the "duality" of purpose of gold, where people can hold it under the auspices of non-monetary purposes, but also hold it for monetary purposes (eg. a hedge against inflation), that makes it so difficult for the governments to totally eliminate it as a form of money (even though the US government did try to do so in 20th century). If bitcoin can develop a similar duality, where the 'smart property' use makes it legitimate, and then people also can secretly hold it as an uncorrelated hedge against government dysfunction, then that could be pretty interesting. In sum, it feels like the 'smart property' could become the 'formal, legal, legitimate' face to the project that can develop independent of how the regulators rule on the use of Bitcoin for monetary purposes."

What Angels Are Looking For

Jeremy Kandah, Managing Partner at BitAngels, is now leading a fund focused on decentralized applications that utilize cryptoledgers. He argues that, "the new "2.0" protocols and projects like Mastercoin and Counterparty are the equivalent of computing languages such as Java and C++. Today there are hundreds of computing languages but only about a dozen that serve as platforms for large billion dollar ecosystems. If you are platform dependent you are selling yourself short and risk long-term vendor lock-in. Nearly all of the projects in this space are open-source for a reason, as it allows portability to other cryptoledgers and decentralized platforms. Open-Transaction (OT) is a good example of this as their toolkit and codebases are entirely open-source and as a consequence even if a fork were to happen with the Bitcoin protocol, which I am not saying there would be, but both the developers and users of that OT application could quickly migrate to another cryptoledger."

Kandah explained that while there is a debate over whether or not Bitcoin itself is the TCP/IP foundation for the cryptocurrency world, there will still need to be a lot of infrastructure extensions built to enable the decentralized applications that these "2.0" projects propose to build. This means that there is a continuous need for both developers and entrepreneurs to build start-ups and business models to bring value to the marketplace. As he notes, "while I am ledger agnostic, there may be even a profitable way to utilize Namecoin's functionality, especially since it uses merged-mining with Bitcoin and thus the transaction and confirmation network already takes care of itself."

Ultimately he sees significantly greater decentralization and uses for user-defined virtual tokens and that entrepreneurs providing value in this way will increase utilization rates for the entire ecosystem as a whole. According to him, "during our due diligence phase, when we look for value-added business models we look for teams that address a current market need and provide new solutions that are easy for the average consumer to interface with. For example, there is likely a way to 'gamify' – to streamline how mesh networks can operate and interact with mobile devices connected to a cryptoledger, allowing a decentralized internet infrastructure to be built ad hoc across nearly any city. Similarly, just as Uber and Lyft have decentralized the taxi industry, perhaps there is a way to utilize cryptoledgers and trustless asset management to provide package delivery services in a profitable manner yet competes with the level service from FedEx."

Another analogy both Kandah and David Johnston mentioned was to keep in mind that while there have been newer versions of HTTP, the perfect is the enemy of the good, that mind share and the network effect behind a protocol is difficult to reproduce and ultimately funds like BitAngels are looking for teams that understand the value proposition (e.g. promise to deliver and create value) for customers.[273] Customers who are more interested in security, safety and reliability of the applications that utilize a token exchange system and not necessarily the nuts-and-bolts of how a cryptoledger platform works.

In addition, I also spoke with Ben Davenport, an angel investor and a member of the monetization team at Instagram. While he does not necessarily endorse one specific project, in his view, "colored coin technology allows such centralized assets to be traded in a completely decentralized way. Every single equity in the world has a central issuer — the company itself. But imagine the power of being able to make a trustless trade of stock for bitcoin with a stranger, at a distance, with no 3rd party involved. With colored coins, I can construct a single atomic transaction which encodes such an exchange. That, to me, is the most important basic thing that colored coins can enable."

Hakim Mamoni, co-founder of Seedco.in and founder of DealCoin, an in-person Bitcoin exchange platform, takes a similar view, arguing that "the true story of Bitcoin is that it is part of a larger decentralization movement that illustrates how humans are better at organizing themselves than previous systems.[274] While 'civilization' has existed since the founding of Sumeria in 4500 BCE, generally speaking we have had the same type of top-down pyramidal structure reproduced year after year. Even after the American and French revolutions, the communities adopted previously existing centralization methods because they had pigeons and horses and not the technology we have today. Now we finally have the technological capability to reboot centralized systems and voluntarily self-organize."

One specific problem he describes that could be mitigated and changed is the role of central banks. "If you look at a person's resume and you see a poor track record of past performance you would likely not want to continue with that member on your team. And in looking back since the early 1900s, given the goal of creating stability, none of the central banks have done very well. Thus for me, Bitcoin is the current killer app – Bitcoin wallets enable anyone to send money to anyone around the world enabling people to be their own bank. Eventually other projects will create some featureset and functionality on top of that and we are currently moving towards exciting developments with projects like Ethereum, not just in changing traditional banking but in other ways to decentralize other systems such as telecommunication networks, food production and even energy production."

Wireless mesh networking is a method for decentralizing telecommunications by enabling each node to relay data for the network. Projects like Commotion and XORP are working towards providing end-users with decentralized wireless functionality.[275]

Mamoni also finds projects like Open-Transactions exciting, "I really like the ideas behind OT because users do not have to trust the server as contracts can move from one server to another in an encrypted manner. Governments were designed and set up to help protect against bad actors cheating the system. Yet if you merge governance with the new paradigm of these technologies, there is no need for these legacy regulations because everything is out in the open, everything is done by algorithm and mathematics. Thus eventually I think regulators will likely embrace these types of technologies because it prevents fraud. Consequently, Seedco.in is looking for a diverse array of startups that not only helps strengthen and grow the cryptocurrency ecosystem in general but provides bridges to the existing financial structure. It cannot be done overnight and we believe there is a lot of value during this transition period."

Another example that Mamoni sees as a use-case for a blockchain is for financial institutions that create the daily London Interbank Offered Rate (LIBOR).[276] LIBOR is an interest rate average that leading banks in London estimate they would be charged if they borrowed from other banks and is published daily at 11:30am. In 2012, a scandal arose in which it was discovered that member banks were manipulating the rate behind closed doors. Yet according to Mamoni, if each of these trades were placed on a blockchain, the rate would be impossible – or at least more difficult - to game or rig as the blockchain is both secure and transparent for everyone to see.

Non-profit organizations and NGOs could also adopt cryptoledgers for similar transparent asset tracking.[277] According to the *Tampa Bay Times*, of the $1.4 billion in donations received over the past decade, the 50 worst charities in the US spent roughly $970.6 million on solicitors.[278] A public cryptoledger would give donors the ability to audit the charity in near-real time. Coupled with a DAO, much of the administrative overhead at non-profit organizations (e.g., payroll) could be replaced entirely by AI.

This transparency could be utilized in other countries as well. For example, on May 12, 2008, approximately 69,000 people were killed during the deadliest earthquake in China for the past 30 years. Subsequently, aid and donations (totaling $11.2 billion) from around China and the world poured into Sichuan, the epicenter of the disaster zone.[279] Yet after the dust settled, several investigations discovered that various organizations and institutions had siphoned off tens of millions of dollars due to a lack of transparency and accountability.[280] The Red Cross Society of China (RCSC) itself failed to collect the funds donated to drop boxes placed throughout several hundred locations around China – four years after the quake.[281] Cryptoledgers could be used to track donations and assets of a non-profit organization, reducing fraud and providing real-time transparency and auditing. In fact, as noted in chapter 5, much if not all of the administrative overhead (e.g., paying bills, receiving donations) in such organization could potentially be replaced by a DAO. This is discussed further in chapter 8.

In January I also spoke with a marketing manager for a San Francisco bay area accelerator that is looking for early stage startups that use the Bitcoin protocol within the verticals of software-as-a-service enabled tax and accounting solutions as well as smart contracts (SaaS enabled Wills, parameter-based or DACs-like business-to-business partnerships). Or in other words, solutions that focus on small-to-medium businesses as well as consumers.

What was unique about the conversation was that they were interested in accounting solutions that involve the full cycle of automatic transfers to tax filing, which only one other group specifically mentioned and thus may be an undervalued niche. Altogether this would involve project management compensation via cryptocurrencies which is a topic discussed in chapter 7 related to Coinality.

The manager also had confidence in decentralized autonomous corporations (DACs) seeing them as the wave of the future. His teams thinks that the ecosystem will eventually outsource a majority of tasks normally allotted to many job types but specifically: accounts payable, accounts receivable, tax, other accounting processes, remittance (varying roles), emergency response (fund distribution), community investment (i.e., local school measures), REITs (community-based real estate investment), and community property management (lease interpretation for automatic service calls). Thus building a company that focuses on designing DACs in those spaces will likely attract the attention of both outside investors as well as potential clients.

Asia

I had an email exchange with Zennon Kapron, founder and managing director of Kapronasia, a large independent research consultancy focusing on the Asian financial services industry.[282] Based in Shanghai, Kapron has continual first-hand experience of the mainland marketplace. According to him, acceptance applications are and will remain very important especially in Asia. Right now, acceptance of any cyrptocurriences is still low outside of a few niche geographic areas. Why do more people have a Visa than an American Express? Largely acceptance - Visa is just accepted in more places. Especially in Asia, the point-of-sale and merchant solutions similar to BitPay are very thin on the ground. In addition, even with the myriad of exchanges out there, there are only a few that I would consider user friendly. Most require wiring money, which the average consumer might not feel comfortable with. Coinbase is an interesting example of an exchange that might have it right: you can link your bank account and make ACH transfers very easily. That comfort is very important for at least the initial adoption of cryptocurrencies, however once the larger population has a balance of cryptocurrencies and acceptance is higher, the need to move into fiat currencies will of course be lower, so exchanges are not as important."

While BitPay, BitPagos and BIPS have come to dominate large portions of the Bitcoin-based merchant ecosystem, aside from YesBTC.co, a Chinese or even Asian-based equivalent has not yet arisen to the same level. Part of this has to deal with language and cultural barriers as Kapron noted and because not many websites use or accept cryptocurrencies in Asia, specifically in China due to legal issues. In fact, after the People's Bank of China statement on December 5, 2013 regarding the banning of payment processors for cryptocurrency exchanges (and categorizing cryptocurrencies as commodities instead of as a currency), ecommerce giant, Taobao, announced that it would no longer allow stores on its platform to buy, sell or trade in wares related to cryptocurrencies.[283] Despite these hurdles it is likely that there are still opportunities on the edges in this segment.[284] Furthermore, ACH is an electronic financial network in the US – even though it processed 21 billion transactions in 2012 worth a total of $36.9 trillion – according to entrepreneurs there is still scope to compete on the margins, and among the underbanked.

Continuing, Kapron notes that, "Asia is behind the West in terms of cryptocurrency applications and solutions so startups focused on 'big' solutions like exchanges, point-of-sale merchant solutions still have viability in Asia as, outside of exchanges in mainland China, the market for these applications is far from saturated. There may be a number of start-ups running in stealth-mode that are developing these

solutions, however, besides exchanges, there have been few if any public launches or investments in cyrptocurrency start-ups. Of course some of the smaller solutions (e.g., tax-auditing plugins, bitmessage, twister, syncnet) also will have a market, but the larger solutions like exchanges and merchant acceptance solutions still have a big opportunity."

Bitmessage and Twister were briefly mentioned in chapter 3; while technically feasible, it is unclear how policy makers will react to domestic businesses that develop anonymous and pseudonymous communication tools.

In terms of smart contract and next-generation platforms, "the technology ideas and algorithms behind the current batch of cryptocurrencies are ideal for potential smart contracts and other ledger applications. These would likely also be easier to implement as they would not necessarily need to be global, but could be limited to a smaller geographical area. For example, you might have a real-estate focused ledger just for London or just for Paris. Because of the limited geographical area, these would have fewer government and regulatory approvals and governments could also be involved in the creation and maintenance of the smart contracts without weakening the appeal of the system. In other words, one of the primary goals of Bitcoin and other cryptocurrencies is that they can operate without government influence which many people believe has caused some of the current economic issues (e.g. quantitative easing in the US artificially supporting US exports through a cheaper dollar). That would not be such a concern with smart contracts as long as there was a trust that the government would act in the best interest of the people."

As noted by Preston Byrne in chapter 2, it is possible that institutions and organizations including governmental departments could build and maintain cryptoledgers to replace redundant functionaries. A speculative way a central bank could utilize one is through a 'proof-of-burn' (POB) method described in chapter 3. Just as the East German Mark (Mark der DDR) was converted and exchanged into the West German Deutsche Mark prior to reunification, the Banco Central de la República Argentina (central bank of Argentina) could one day declare that it was "issuing cryptotokens" to prevent the debasement of the peso.[285] The BCRA could ask peso holders to convert their holdings into cryptopesos. During the conversion process the physical pesos are recycled or destroyed and subsequently the virtual tokens are then tracked on a public ledger preventing double-spending and inflation as described by Wences Casares and Sebastian Serrano in chapter 2. The likelihood of this type of adoption is of course debatable.[286]

While the People's Bank of China is currently reviewing its policies involving cryptocurrencies, according to Kapron, "regulation will still drive the integration of and opportunities in cryptocurrency throughout the region. Hong Kong and Singapore are typically known as some of the more entrepreneurial hubs in the region in terms of payments and financial technology in general. If we draw generalizations from Bitcoin, the indications from regulators in both countries are very positive for cryptocurrencies and so it is likely that we will continue to see both innovative solutions for and acceptance of cryptocurrencies in both Hong Kong and Singapore. In many respects this is great for the region as although both countries have large economies, they are still relatively small, both from a geographical and economic perspective, so almost similar to a free trade zone in China, Hong Kong and Singapore could end up being test-beds for cryptocurrencies. China already does this with Hong Kong for the financial industry in general, by the allowing the Hong Kong financial sector to innovate and change even though the mainland remains somewhat constrained. In addition, both Hong Kong and Singapore have a long history of country-wide payment innovations like EZ-link and Octopus which have largely thrived for many of the same reasons why cryptocurrencies also could. The larger economies from both a population and economic size

perspective like China and India will likely follow what happens in Hong Kong and Singapore as the risks for the larger economies are much higher, especially as both economies have capital controlled currencies. Smaller economies, especially those in Southeast Asia, have enough economic and political challenges and less influence in Asia's overall economy, so will not likely influence integration."

Over the past three decades, China has created 15 "special economic zones" (经济特区) that are allowed to set their own import regulations and duties and as a consequence are relatively popular for establishing joint-ventures and foreign trade operations. Beginning last year, several other municipalities including Shanghai began laying the groundwork for 'free trade zones' which will create testing grounds for new economic reforms that are expected to further liberalize the financial sector.[287]

In January 2014 I interviewed Rui Ma, a Beijing-based angel investor with 500 Startups, a business accelerator which has invested in a number of Bitcoin-related startups including Bitdazzle and BTCJam.[288] In her opinion, "cryptocurrencies are a solution to crossborder microtransactions as they provide business opportunities in segments that have been completely overlooked by the traditional banking sector. I think mobile payments in particular are interesting for everyone – especially emerging markets – because internet finance has made large gains over the past year in China due to a lack of consumer (and small-medium enterprise) financial products in general across the board. Though, this is not a business one or two angels can probably scale alone due to capital expenditures for traditional payment mechanisms but I am certainly interested in services based on top of infrastructure, and Bitcoin is pretty ideal for that."[289]

Due to strict capital controls it can be difficult for high-net worth individuals in China to diversify abroad. This issue is compounded with a dearth of domestic financial instruments in part because the country is still developing and because its financial sector is essentially oligopolistic (e.g., dominated by large state-owned banks).[290] As a consequence it has been technology companies such as Alibaba and Tencent leading the way, creating innovations in the consumer market such as providing mobile-based mutual funds and 3rd party payment processing services. For example, last year Alipay began offering a low-cost mutual fund (called Yu'E Bao) through a partnership with Tianhong (a Chinese asset management company). With $42.6 billion in its fund and 49 million customers, Yu'E Bao has grown to become the 2nd largest mutual fund on the mainland.[291] In January 2014, Tencent, the largest internet company in China unveiled a partnership with China Asset Management, the largest mutual fund manager in China to provide a similar service called Licaitong.[292] Tencent has simultaneously integrated Licaitong with WeChat, the fastest growing social networking service globally, (with more than 600 million registered users).[293] Tencent is also the parent company of QQ, which develops the biggest social media platform in China, with 816 million monthly users.[294]

Ma recognizes these market trends and changes and how cryptocurrencies like Bitcoin can play a role in. Noting that "another issue in the mobile segment globally (not just in China) is payment infrastructure, which current protocols do not match up to the development and proliferation of devices and content and goods for consumption. Now that we can manufacture and distribute smart devices relatively cheaply and the data infrastructure is expanding rapidly, it is time for payments to catch up. And this is where I think there is a lot of friction (e.g., institutions, old infrastructure, policy) that can be decreased, removed and even erased with cryptocurrencies, which are more secure, speedier, cheaper; and due to these three main benefits, much more scalable."

I also spoke with Jack Wang. Wang is a cofounder of a Bitcoin startup called Dearcoin that is developing consumer Bitcoin applications, including Bitpass, a Bitcoin-based authentication protocol. He previously

developed a Bitcoin exchange and merchant tool and has taught a Bitcoin class for General Assembly.[295] He says that he likes "the concepts embodied in applications such as 'colored coins.' The biggest innovation that Bitcoin represents is a distributed, verifiable ledger system, and its use as a currency is just the first application. In thinking through some ways in which Bitcoin develops, I believe there are multiple potential killer applications for this kind of system, especially as we move into an age in which 1) digital property becomes increasingly valuable and 2) verification of rights to all kinds of property becomes digitized. If Bitcoin becomes the de facto system for digital property rights verification and management, the value extends way beyond just as a currency."

Wang explained this by analogizing Bitcoin to the frequency spectrum in the wireless industry. Where the ability to propagate and record digital rights onto the blockchain will depend on ownership of bitcoins, bitcoin owners can be thought of as owning these rights. And according to him, "the applications can include anything that involves rights verification - contracts, stocks, titles to houses and cars, actual keys to houses and cars, digital files (music, art, etc.). Longer term I see the fungibility, transferability, and divisibility features of cryptocurrencies replacing the use of fiat money in a lot of ways. People cannot barter today because it is infeasible to trade a car for 5,000 sandwiches, but you can do that with cryptocurrencies even if they are not just just as a currency but as a colored coin or something similar. Maybe we should start calling it cryptobarter. This opens up a cornucopia of business opportunities and consequently, once cryptocurrencies are used for things besides fiat exchange, older institutions and business models are really in a bind."

The problem, of course, is getting enough people to adopt the technology so that it can serve as a useful medium for these transactions. Eddy Travia, based in Hong Kong, is the founder of the Bitcoin Institute and co-founder of Seedcoin which is the world's first seed-stage Bitcoin startup virtual incubator.[296] And he has some ideas about how this could be done; the areas he and other angels at Seedcoin are looking for are "any application that makes exchange clear and simple to end-users, like Hive which is a bitcoin wallet with built-in applications.[297] Another area is for development teams to find out what people know and use regularly in their daily lives, for example CoinSimple will make it easier for merchants to switch among various payment processors, from BitPay to GoCoin to BIPS to BitPagos and other market players.[298] So it means more merchants can accept bitcoin and thus more clients can use their services and seamlessly use any bitcoin payment processors chosen by the merchant."

Travia adds, "we are also still busy helping basic infrastructure in certain countries, like a solid bitcoin exchange in Mexico (MEXBT) so once that part is done (exchanges and payment gateways available around the globe) the potential user base will grow significantly larger.[299] It still needs to expand so that more and more entrepreneurs have a market large enough to support the investment into their applications and also have locally customised apps (language, regulations, etc.)."

He continues, "Bitcoin is also at the intersection between finance and technology so it will not be as easy as "email" or Android; local regulations and laws have to be considered. When it comes to mass adoption, there are always laws taken into consideration. Consumers are used to it with banks, mobile operators, credit companies because we do not bother reading the fine print anymore on all the contracts and thus there will likely be fine print with bitcoin services as well – people will have to get used to it. Armed with this knowledge and understanding, Seedcoin is a channel for angel investors in a way, but also enables small players to become angels and invest into these companies."

Potential business opportunities

While many users and commentators have been relatively fixated on one data point, one use-case, arguably, where the long-term Christensen-disruption and Schumpeter's "creative destruction" will come from is trustless asset management.

The question for entrepreneurs and businesses is, as everywhere else, what are the unique value opportunities you can provide? Business analysts experienced with requirements gathering may find opportunities designing and creating specifications for a smart contract for specific needs. Similarly, programmers will be needed to take the design and implement and translate it into code in accordance with applicable regulation. Commercial lawyers will be drafted in as advisers to draft and negotiate the contracts and review the code, perhaps even following through the steps originally synthesized by Nick Szabo fifteen years ago.[300] Yet be aware that long-term, if history is a guide, it is likely that some of these smart contracts could eventually become open-source – and standardized - and thus alternate revenue streams will need to be found.[301] When I put this question to Nick Szabo, he said that "traditional contracts are already typically treated by the legal community as open source rather than as copyrighted. The vast majority of contract clauses are boilerplate and I hope the same will be true for smart contracts code. And in the cryptocurrency community (or more broadly speaking, the block chain community) we should not trust code that is not open source."[302]
In fact, there is already an initiative called Algorithmic Contract Types Unified Standards (ACTUS) that is attempting to create a standard language and contract-centric framework to represent all known financial contracts in a reference database.[303]

For perspective I also spoke with Sean Zoltek, a New York-based corporate lawyer specializing in securitization and collateralization. In terms of designing and encoding a contract into computational algorithms, "we can easily make a set of programmatic rules that have a variety of default replies based on historical track records and know with roughly 99% certainty how it would turn out. In fact, we use standardized forms all the time. Both the linguistic construct and existing legal framework have been built up over decades to support these types of contracts. For example, I could draft a contract for a small business loan to include check-boxes that provide default conditions. The user interface for such instruments already exist and have been simplified to where a party only needs to answer criteria such as type of existing loans, assets and length of maturity dates. In fact, many of the contracts at law firms are much more sophisticated than a commercial bank due to the level of detail and case knowledge that we have."

In his view this could be done today in a three or four page document or a few dozen lines of code, would be completely automatable and would not require an attorney to fill out.[304] Furthermore because of its robustness built on previous case law, a judge could look at a smart contract and it would likely be enforceable.[305] Zoltek believes that "smart contracts already can encompass this functionality. For instance, based on the context of what kind of loan it would be, the next 1,000 transactions from the same bank service segment could literally be identical. A small business loan is a good example because it typically involves $20 million in assets, $100,000 of inventory in the store or office and some kind of standard insurance policy. We would not even need to worry about electronic chattel paper or letters of credit. In addition, such a contract could accommodate would likely be fair for both parties involved because they could both provide input. This is in contrast to the relatively one-sided terms of service that most banks provide borrowers today that are non-negotiable."

According to him, since it is in the firm's interest to help small businesses succeed, with simplified interfaces and default conditions (e.g., trust, escrow), "it could absolutely be done in computer code and would definitely make certain lawyers sweat. This is in turn would mean our industry would move

towards increased sophistication and specialization. Yet on occasion there are nuances that are not entirely straightforward or streamlined. There is the law and then there is how it is applied to circumstances hence the reason some party has to make judgment calls. As time goes on and case-law is built, you eventually end up with cookie-cutter deals and which are automatable. This situation is amplified with cryptocurrencies like Bitcoin through its low or no cost transactions, clearly defined allocation of value, transport of value and open algorithmic rules that everyone trusts. You can potentially build on top of that mechanism providing more complicated transactions and instruments that are beyond what the Bitcoin protocol can currently do. Thus once you assume how a typical contract works you build above it, and I see it as beneficial to all parties involved."

In terms of open-source smart contracts, Zoltek notes, "There is an old saying in the legal profession, if you have language that works, use it. Aside from litigation cases (which involve some original creativity), there is little creativity in a contract prose themselves.[306] In fact, many briefs may reuse entire passages, citations and analysis of a previous case, this is a common practice as that material stood legal challenges. In other words, once you have a good argument, you continue reusing it.[307] Furthermore, once we produce the contract, it becomes public because it is filed with the SEC or some other institution. In fact, no contract says "copyright GE" – it is just a contract. As a consequence, if you can make our lives easier by automating things, we will have to branch off into more creative-based niches which is generally the trend the industry has been heading since 2007."

In the meantime however, there is potential for experienced financial-instrument programmers and designers to work in this segment. For instance, Sean Percival, a venture partner at 500 Startups recently explained that "[i]n the New York tech scene, a lot of engineers want to move over to startups, but their skill set is not a match. This may be a case where their financial programming skill set is going to be a great match for bitcoin companies."[308]

As noted by Szabo and others, the easy low-hanging fruit are financial instruments and other contracts executed by code, including crypto-based financial instruments that exist today. For example, using open-source Cryptotrader software, programmers have been able to build and execute arbitrage bots used on fiat-cryptocoin exchanges such as BTC-e.[309] The next logical step is to build a smart contract that interfaces with various cryptoledgers such as Bitcoin to Ripple or Bitcoin to Counterparty (or any ledger). Another smart contract could be a simple invoice – repayable in a cryptocoin – to bill clients for services rendered.[310] Another is an assurance contract, which is how crowdfunding sites operate (e.g., I will deliver this product if I get X amount of pledges made by day Y).[311][312]

During his Turing 2013 presentation, Mike Hearn mentioned that just about any repetitive work (filling out spreadsheets, opening bank accounts), anything that can be mathematically quantified and formalized can and will be replaced by automated agents. It is the creative roles that will be difficult to automate. Looking forward in time (by decades), Hearn sees other automatable segments powered by DAOs such as taxi providers, commodity deliveries (such as fruits and vegetables), units of computational time (cloud services), and even "smart roads."[313]

In a sense a DAO is an autonomous agent, a computer that owns itself as an economic actor. It earns money and pays for itself with money it generates and thus could alternatively be described as the first form of artificial life (though it is not intelligent). If a DAO is profitable and successful it can self-replicate its codebase and thereby create a "child," ceding its assets in the form of a "birth loan." If it operates at a loss, it could then "die" (i.e., purged from market). This long-term perspective is important if you are looking to make any sizable investment in the segment.

Remittances, Value-Added Services, and Legal Considerations

In the United States there are multiple state and federal agencies currently assessing the impact of cryptocurrencies. The exact policy implications are unclear at this time. However over the course of the past year the US Senate, Securities and Exchange Commission (SEC), Commodities Futures Trading Commission (CFTC), New York Department of Financial Services and FinCEN (among others) have held hearings to gather information and occasionally provide regulatory guidance.[314] For example, in a hearing held across two days, January 28th and 29th, the New York Department of Financial Services interviewed over a dozen witnesses regarding possible regulatory policies and witness testimony ranged across the entire spectrum.[315][316] The following day, on January 30, 2014, FinCEN independently issued two new rules that stating that both miners and investors are not money transmitters and thus did not need licenses.[317]

On February 19, 2014, California Assembly Bill "AB-129 Lawful money: alternative currency" which clarifies the possession and acceptance of bitcoin and other virtual currencies as money, passed unanimously.[318] The State of Washington recently updated its statutes to state that, "Virtual currency, also known as digital currency or crypto-currency, is a medium of exchange not authorized or adopted by a government. There are many different digital currencies being used over the internet, the most commonly known being Bitcoin. In Washington, digital currency is included in the definition of "Money" in the Uniform Money Services Act (UMSA), chapter 19.230 RCW."[319] Other countries such as China and the United Kingdom have differing laws.[320] On December 5, 2013, the People's Bank of China issued a notice that banned 3rd party processors (such as Alipay and Tenpay) from providing renminbi (RMB) transactions with cryptocurrency exchanges.[321] In contrast, on March 2, 2014, Britain's tax authority announced that it was scrap its tax on Bitcoin trading.[322]

While these issues are being sorted out, there may be other areas in which regulatory uncertainty could be mitigated. One way around logistical issues is to put transportation clauses that must be met otherwise various counterparty stipulations take effect. That is to say, what if your state DMV does not recognize a particular smart contract or token transfer as an official legitimate means for exchanging your vehicle? While you may find a legal work around, this could recreate a barter economy. For example, in the event that a fiat-exchange system is shut down and price discovery in relation to that particular token is affected, users could trade other assets worth roughly the same value instead.

Another area where cryptoledgers and policy intersect is the transmission of the token. Since tokens are transmitted on a peer-to-peer basis, they can be sent anywhere around the world near-instantaneously. Thus if Alice had friends or family working overseas and in need of money, instead of using costly remittance services such as Eurogiro or Western Union which charge high fees for no value-added, Alice could send Bob any amount of Bitcoin for almost no cost (or other crypto-based token).[323][324] In fact, in 2012 Western Union generated $4.6 billion in transaction fees and had a net profit margin of 16%.[325] A recent report from the World Bank found that the 232 million international migrants working abroad remitted an estimated $550 billion in 2013 – the top three countries for incoming remittances reached $71 billion in India, $60 billion in China and $26 billion for the Philippines.[326][327] Fees charged by various levels of middlemen providers, exchangers and compliance offices collectively add another $74 billion from this process, with no value added. For example, the average African migrant is charged 12.4% in remittance fees, thus reducing that fee to even 5% would save Africans from the continent $4 billion.[328] Globally the average fee on remittances is 9% and many banks charge an additional "lifting" fee that adds another 5% to remit it into local currency.[329]

In February 2014 I spoke with Alan Safahi, the CEO of ZipZapInc.[330] Founded in 2010, ZipZap is the largest global cash transaction network enabling consumers to use cash to buy digital currencies. In this manner it acts as a software-based intermediary between Payment Centers who collect fiat and exchanges that provide bitcoin liquidity. According to Safahi, ZipZap is building both on-ramp and soon off ramp connections from physical cash to digital currencies around the world which they hope will someday provide a free remittance network, "I want the cost for remittance to go down to 0%. Currently we have to charge fees for fiat on both ends however as time goes by eventually, we will only have to charge for fiat conversation out. Ultimately we will go to a freemium model in which basic services like remittances are free through the use of cryptocurrencies like bitcoin."

"We as an industry will have to provide value-added services on top of free remittance services to the edges that consumers would want to buy," added Safahi. "It would be similar to the online gaming community which has successfully adopted a freemium model to provide additional product or enhancements the gamers gladly pay for."

Safahi would like to turn the status quo upside down. Whereas currently a customer has to meet certain rigid standards and then pay relatively high fees if he or she remits from developing countries (and in some cases gets rejected), he wants to make it easier for customers to transmit value that they own. Accordingly, "it is my mission to make life easier for consumers, change it in a manner in which the customer comes first for any new financial services products not the service providers." ZipZap launched its global cash payment network in 2012 and has grown to 700,000 payment center locations.[331] ZipZap also recently expanded into 28,000 new UK locations and continues to partner with more Bitcoin exchanges (such as Bittylicious, ANX, Kraken, CoinMKT, and BIPS Market) to allow customers to convert local currencies into bitcoins at any of the locations.[332]

I also spoke with Charles Hoskinson, creator of the Bitcoin Education Project and member of the Ethereum core development team.[333] In terms of the impact DAOs and trustless asset management will have, he sees that, "the simplest way of looking at it is 3.5 billion people in emerging markets are faced with two configurations of property and contracts. The first is that because of how institutions are organized and incentivized, those who are well-connected or whom are willing and able to bribe government officials are able to protect their property. This is not a very stable structure as it is subject to any change in government (e.g., removal of politicians). The other configuration is a grey system, a type of informal economy based on handshakes and under-the-table dealings."

As a consequence he sees that "it is risky and difficult for residents overseas in developed countries to make educated investments because of a lack of clear rules and property rights. When you have a stronger rule of law, such as codified contracts and arbitration mechanisms, then investing is not only more transparent but also safer and more efficient. Projects like Ethereum that utilize a DAO, they present a strong 3rd option: they do not have to ask a government or institution for bribe. Users also do not have to worry about a nebulous grey area. Instead, you can put your trust on a ledger – in math – which then creates transparency. Consequently, due its peer-to-peer nature it also transcends any jurisdiction and thus can be used by anyone to track and manage any asset. This will change how business is conducted in both developing and developed markets."

Because these are autonomous systems it will also change banking and the way capital is transferred, acquired, stored and managed. Smart property tied to existing jurisdictions could likely be affected as well. According to Hoskinson, "we have begun to see this already over the past 5 years in terms of fiat exchanges interfaced with bitcoin, but a DAO will only amplify both the uses and the impact on society.

For example, since at least 1991 there has been a variety of methods for building reputation systems – webs of trust – that incentivizes users to pay back creditors.[334] With a blockchain you can now have a safe place to put an instrument or contract and people can digitally sign it. Since it is publicly audited, other users can see its history and if it is reliable thus building credit scores. In turn, business transactions based on clearly defined terms and services can be conducted on an exchange through a form of identity management. This will completely transform how the flow of capital and investment work and will be a godsend to the 3rd world. For instance, a person with a reliable DAO (or smart contract) could create a monetary instrument (a cryptocoin) and lend it to anyone on the globe in the form of a loan with specific terms and conditions. This is done in an external, tamperproof system, a cryptoledger that is not controlled by an institution capable of abuse. As a consequence, for developing countries, just as they leapfrogged copper wiring choosing to use wireless telephony, some may forgo building replicas of existing financial infrastructure and instead choose to use this virtual-based system through their mobile devices."

The most successful mobile payment system currently is M-PESA, operated by Safaricom and Vodacom and serving 30 million users in East Africa (Kenya and Tanzania), the Middle East and India.[335] It is a mobile-phone based money transfer and microfinancing platform; last summer, Kipochi integrated a lightweight Bitcoin wallet with M-PESA which enables Kenyans to bypass costly remittance fees charged by middlemen such as MoneyGram and Western Union.[336] While some may ignore the possibilities of mobile banking, preferring desktops or even physical visits to bank branches, 43% of Kenya's GDP is spent through mobile phones.[337] In fact, according to a recent *Reuters* report, "M-Pesa has enabled 67 percent of Kenyan adults to access banking. Its transactions total about $1 billion per month."[338][339] There are roughly 253 million unique mobile phone subscribers in Africa (many have two SIM cards) and an estimated 70% of the population on the continent are underbanked or have no access to a bank.[340] Therefore cryptocurrencies and trustless asset management tools built on cryptoledgers that interface with mobile phones will enable and empower an entirely new demographic and consumer base to emerge from subsistence. In fact, according to a 2009 report from Financial Access Initiative, half of the world is unbanked which leads to new opportunities for entrepreneurs.[341]

Chapter 7: How to Get Involved with the Crypto Ecosystem

No matter how you might have heard or learned about cryptocurrency, there are different ways to obtain your first tokens. You can mine them, you can buy them through an exchange (e.g., BitStamp, Kraken, BTC-e), or if you are a merchant, you can receive tokens for your wares.

Mining

Unfortunately mining Bitcoin *profitably* currently requires a significant capital investment in single-use ASIC hardware. While you could use a cloud-based hashing service such as Ghash.io or ASICMiner, you will learn very little of how the network actually works. In fact, even with an ASIC, most mining systems currently lack power to select or validate bitcoin transactions themselves; you are merely selling a computing service (hashing) to the mining pools.[342] Another lower-cost option is that you could purchase a small USB ASIC miner (e.g., Bi•Fury); however, the problem is that you would need to rely on whatever token amount you generate to appreciate in value in order to pay for the electricity you expend in mining (e.g., if you generate 0.1 BTC that is worth $80 but it cost you $85 in electricity to generate, then you would need to wait for the bitcoin to appreciate; otherwise you are at a net loss).[343]

Over the past several years, one business model has emerged in the Bitcoin mining industry: preorders. Typically what this entails is sending X amount of bitcoin to an ASIC manufacture who will then use that bitcoin to invest, design, build and ultimately ship an ASIC to you. To maximize inventory, manufacturers create batch orders with wait lists. The farther you are down the list, the longer it takes to receive the machine and hence recoup your initial investment. While you can try your luck in getting the first batch of a new ASIC prior to its release, you are probably more exposed to risks with fewer potential upsides than downsides. Your capital is tied up in a depreciating asset – a machine that unlike a GPU that can be resold to gamers and 3D designers – has progressively lower resale value and has a singular use that may or may not be delivered on time with unknown hashrate performance deltas.[344]

Or you could be thinking, just like the first people who managed to get an Avalon batch last winter or a new terahash-level CoinTerra machine in January, perhaps you might be lucky enough to get placed high on the list for the upcoming KnC Neptune; but the odds are you will not, especially if you are reading this and have not pre-ordered it.[345] One illustration of the risks is the time lapses and project delays involved in Butterfly Labs (BFL) ASIC orders last year. BFL originally announced a variety of different desktop ASIC machines in July 2012 and hundreds of customers subsequently preordered them with bitcoin.[346] Yet due to a number of developmental and testing problems shipments were continually delayed over the course of the following year.[347] For instance in March 2013, a close friend of mine who is a Bitcoin investor paid 50 bitcoins for four ASIC machines from BFL, each capable of mining at 25 gigahashes/second.[348] He received them more than six months later at the end of November. If instead, he had held that 50 bitcoins, he would have been able to sell the tokens for $40,000 – $50,000 on many exchanges.[349] Consequently, if you plug that 100 GH/s mining rate into a mining calculator, he will not even be able to mine 1 bitcoin for the next year at the current difficulty rating let alone ever be able to mine the 50 bitcoins it cost to buy them.[350] Caveat emptor.

If history is any guide, looking back at the California gold rush (the ‘49ers), the firms that ended up financially solvent were merchants and service companies such as Samuel Brannan, Philip Armour, John Studebaker, Levi Strauss and Wells Fargo.[351] Those who also made and sold mining equipment (picks, axes, shovels, sluices) had mixed results. Yet the group of people that typically fared the worst

financially was the miners themselves, as they were nearly all exposed to various types of risks (upfront capital costs, land title lawsuits, inclement weather, sickness, landslides and cave-ins) and as a consequence, most ended up bankrupt.[352] Yet, if you feel the urge to mine – to better understand the blockchain verification and network – another alternative is to mine an altcoin such as Litecoin or Dogecoin, both of which are Scrypt-based. Scrypt is a different proof-of-work (Bitcoin uses SHA256d) and requires a larger memory pool to utilize which in turn makes it more resistant to the rapid performance increases spurred by ASIC development.[353] Thus you can still use a GPU that has resale value and utility beyond mining.

Merchant Ecosystem

Chapter 2 briefly discussed a milestone in the Bitcoin ecosystem, the exchange of ten thousand bitcoins for a pizza in 2011.[354] This is considered the first publicly known transfer of value and thus became the original foundation for fiat exchange.[355]

Since then, the merchant ecosystem has grown to encompass an estimated 50,000 online vendors. BitPay is one of the largest startups in this segment, providing an electronic payment processing system with bitcoins for online merchants.[356] In 2013 it processed more than $100 million in bitcoin transactions and has signed-up more than 20,000 merchants.[357] Gyft, a digital and mobile gift-card wallet (who is partnered with BitPay) that accepts bitcoin as a form of payment, allows customers to buy, send, receive, manage and redeem digital gift cards via mobile devices and works at more than 100,000 retail stores.[358] On November 27, 2013, Shopify, a large ecommerce platform, announced that its 75,000 merchants now accept bitcoin as payment.[359] On January 9, 2014, Overstock.com began accepting bitcoin for payments. On the first day it processed $126,000 in sales with bitcoin and less than two weeks later that amount climbed to more than $500,000.[360] Subsequently, on January 23, 2014, TigerDirect announced it would begin accepting bitcoin as a form of payment and within one week processed $500,000 in bitcoin payments.[361] On February 27, 2014, Coinbase announced that it not only has over one million consumer wallets – up from a mere 13,000 at the beginning of 2013 – but that more than 25,000 merchants use the Coinbase platform.[362]

On a nearly daily basis other vendors and merchants independently add bitcoin payments as well. Zynga, the developer behind social games such as Farmville, announced on January 4, 2014, that it would begin accepting bitcoin as payment (via BitPay).[363] Previously, on May 9, 2013 HumbleBundle (in partnership with Coinbase) announced that it would begin accepting bitcoin as payment for its game bundles (later expanded to the entire store).[364] Another example, during CES 2014, Formlabs, the maker of 3D printers announced that it will now accept Bitcoin payments in its online store.[365] And on February 4, 2014 CheapAir.com announced that it would begin accepting bitcoins as payment for hotel stays (it had earlier accepted bitcoins for flight bookings).[366]

In chapter 3 I introduced, Jon Holmquist who works with Ripple as the Community Liaison, he is also the founder of Bitcoin Black Friday (BBF), the largest e-commerce day for Bitcoin-related purchases, which takes place the day after Thanksgiving filtered through one site. One of the reasons he was motivated to start BBF in the fall of 2012, "I was working with a Bitcoin merchant and we started doing various sales promotions to drum up support from the Bitcoin community yet there was – ironically – no central avenue, nowhere to funnel them to. I also noticed a lot of merchants individually conducting sales promotion campaigns and thought a central launching pad would be a great experiment to show a real empirical case-study of Bitcoin ecommerce in action."

Holmquist built and the consumers came. In 2012, the first year BBF worked with 60 merchants, 600 in 2013 and they hope to work with 6,000 this year. BitPay alone processed 6,926 bitcoin-based transactions on November 29th last year up from 99 transactions on the same day the year before.[367] Yet to Holmquist the big number that often is overlooked is the fact that BBF customers donated over $1 million worth of bitcoins to charity. If this had been done with normal credit card transactions, fees of 5% would have been assessed. Instead that $50,000 in surcharges went to a charity instead of a credit card company. While this event may be an outlier for the ecosystem, for Holmquist "this is just the beginning to enable easier transfer of value to consumers. And this is also an area where entrepreneurs and developers can continue to simplify the process for merchants wanting to support cryptocurrencies by providing turnkey services such as plugins."[368]

Perhaps this specific incarnation of virtual money (bitcoin) is a fad and merchants will drop all support for it. If that is the case, switching to another ledger would be relatively simple, as both the front end and back end of existing merchant systems could use other altcoins or altprotocols. Yet these case-studies referenced above serve as empirical examples of how value can be transferred globally, to anyone, safely, reliably and nearly instantaneously without any middlemen or institutions.

Developer, Developers, Developers

One key theme that all the investors and software architects that I spoke with has been that the ecosystem is in continuous need of competent, creative programmers. And because the space is so new, so fast and quickly evolving, the barriers to entry are very low. Thus novice coders with business acumen could potentially find entrepreneurial opportunities in the ever-growing ecosystem.

BTCJam

I spoke with Celso Pitta, the founder of BTCJam.[369] Founded in 2013, BTCJam has expanded into 131 countries, with 12,000 users who have provided $5 million in bitcoin-based loans to one another. It has done this by fusing a global P2P payment protocol with a credit score system, matching loaned bitcoins to borrowers. Pitta is originally from Brazil and previously worked with statistical models for the credit card division of Citi. He was motivated to create a P2P lending platform primarily because of the increasingly high interest rates on credit cards in Brazil, some as high as 200% a year.[370] In contrast to developed countries where credit is relatively cheap because there is a dearth of credit options in emerging markets such as Brazil, consumers are left with few alternatives.[371]

According to Pitta, "unless you have access to the FICO credit rating system, it is very difficult to receive a credit line.[372] And due to their developing status with a lack of financial institutions and infrastructure, most emerging markets do not have a credit rating system capable of accurately gauging the creditworthiness of borrowers. In contrast, by using an open registration, where a user can submit any pertinent details they want, we have built a statistical engine that can sort through the quality of their data and provide an increasingly accurate rating. Bitcoin is a perfect microlending platform in that its 8 decimalization units provide flexibility for fractionalization and the transmission is both secure and relatively fast. In contrast, with fiat, merchants and lenders not only risk fraudulent chargebacks but expensive fixed costs irrespective of amount lent (e.g., 10% fee on $1 lent). With bitcoin, there is no way for someone to game the system with chargebacks – once the token is sent, it is sent – transactions are irreversible. And while there have been cases of a borrower who is unable to pay back a loan in our system, our fulfillment rate is now at 98% compared to the global average in 92% for P2P lending."

According to its 2013 report, LexisNexis found that online merchants pay $3.10 for each dollar of fraud losses incurred via the internet (e.g., on top of fraudulent charge-backs, fraud monitoring, and bank fees, the merchant must replace the item(s) that are lost).[373] Cryptocurrencies are a solution to this problem as they cannot be recalled once sent or double-spent. Pitta thinks there are other opportunities in this segment for entrepreneurs who want to help enable the unbanked and underbanked. In fact, he has found that borrowers are very motivated to obtain a credit line and as a consequence learn and educate themselves as to what Bitcoin and cryptocurrencies are in order to use them. Yet there are still challenges as well: "The friction between obtaining fiat such as Real (R$) and the regulatory framework which is still a grey area in most countries still create barriers to entry for both parties."

For comparison US-based peer-to-peer lenders such as Prosper and Lending Club issued $2.4 billion in loans in 2013.[374] Why is this important? According to the International Payments Framework Association, through 2010 the average cash flow margin on global transaction services (GTS) was 38%, making it a steady stream of revenue for banks.[375] Attractive margins like this makes it an opportune segment for technological disruption and innovation.

Crowdequity

In February 2014 I spoke with Joel Dietz, CEO and founder of Evergreen.[376] Evergreen is a protocol layer that can connect off-ledger with Bitcoin and was designed with ease of use in mind. The protocol enables developers to build an infrastructure on top to create mobile web apps that natively accept micropayments. With this experience Dietz subsequently sees smart contracts and DAOs as having a big impact in the future. According to him, "I think many of the functions that contract designers (such as attorneys) do today can and will be automated – and that their current jobs will likely be coded away. Contracts are ultimately just code and are the new innovations and apps to this space. In fact, I think a variety of smart contracts will be available for use by the end of the year – easy to use smart contracts with escrow and verification ability. Of course, they will have to build the platform first. But I think they'll be relatively easy to create because prototype code already exists."

In his view, decentralized autonomous organizations have "many benefits from a funding standpoint as they enable organizers to simply check off the boxes. Cryptoledgers and multisignature functions provide the auditing and logistical abilities. This is a transparent, straightforward method and is quantifiably better than other crowdfunding techniques. For instance, because of the way the current system is designed, there is no way to engage and reward userbases directly, especially early adopters who contribute content. In the case of Twitter, those who tweeted and convinced their friends and families to use it were not rewarded – rather only the equity holders (the founders and investors) were able to receive compensation. In contrast, crowdequity can engage and incentivize adoption creating an early userbase with rewards for content and marketing. And the easiest, most transparent method to finance crowdequity is with cryptocurrencies managed by a DAO."

BankToTheFuture is one the first crowdequity platforms in this space and has 10 startups working on Bitcoin-related projects.[377]

Adam Levine has been working on a project involving Kickstarter coins that provides similar crowdequity functionality rewarding early adopters and users for their support.[378] In fact, Levine proposed not only a new cryptographically controlled manner by which companies and organizations can raise funds (via an initial float of brand-specific cryptocoins), but also how in the event that a company falters or fails, a reverse merger can take place utilizing these tokens:

> Even after a company has exhausted their potential ideas and abandoned such a coin, the very fact that it is so inexpensive could be its resurrection. Another company could opportunistically buy those very cheap and abandoned shares, then announce they'll be honoring them for their service or product with the rate of exchange being the characteristic that defines the intrinsic value since they are one and the same.[379]

On February 17, 2014 a new project in the crowdequity space was unveiled called, Join My IPO (JMI).[380] It was developed by Amos Meiri, a Colored Coins team member, and will issue its first coin in the coming months. The core idea is that individuals (backers) can invest in specific people before launching his or her own venture, campaign or career is launched. So for example, entertainers, entrepreneurs and artists can directly raise money through coin issuance to backers (e.g., friends, family, fans). In fact, anyone with an account can issue their own customizable cryptocurrency, offering it to anyone else who has downloaded a Chromawallet (the same wallet used for tracking Colored Coins). Through the JMI website, 'talent' can customize what kind of award to give to backers such as quarterly dividends or percentage of income, which can then provide access to wares that the talent creates (e.g., books, CDs, schwag, concert tickets).[381] And by doing so, it is expected that celebrities issuing such coins could strengthen the bond with fans. Simultaneously, these tokens can be traded on an exchange, producing real-time signals to investors and backers as to the relative strength and health of a particular talent.

While, Max Keiser, a TV host and Kim Dotcom, an internet entrepreneur have both issued 'coins' – MaxCoin and Megacoin respectively, these tokens do not offer much new functionality compared with existing altcoins.[382] Yet projects like LTBCoin and Join My IPO will enable users to not only launch a custom token through existing infrastructure, but to redeem these tokens for actual value (e.g., concert tickets, books, dividends).

Credit score

In terms of credit scores, Nick Szabo has previously described several use-cases for leases and creditor liens whereby after a set of conditions is met (or not met); control is reverted back to the original owner.[383] While cryptoledgers and cryptoprotocols currently have the ability to provide pseudonymity (and potentially anonymity through Dark Wallet and ZeroCoin), there may actually be incentives for some users to reveal their public address. That is to say, for credit score purposes (e.g., lending), the more open you are about your transaction history, the more data a potential creditor has to gauge and quantify risk with. Thus, in practice Bob may actually have a publicly traded account that he publicly lists (on business cards, websites) but then he may have several other digital wallets in which he actually stores all transactions, savings and revenue. Szabo observes a similar dichotomy, stating "there's a big trade-off between privacy and developing a reputation. Long-lived pseudonyms could also be used to develop reputations, but current regulations strongly favor 'true name' identity."[384] Thus, while it has become standard operating procedures to use a new random address for each transaction today, in the long-run the incentives to identify at least one of your accounts may outweigh privacy concerns.

Ease of use and simplification was another common theme that investors and developers reiterated. While those with enough technical acumen and computer savvy have become early adopters to cryptocurrencies, the vast majority of the population has difficulties in fully understanding not only how the virtual tokens work but also how to use, secure and store them.

Ease of use and discovery

Sean Percival, a tech-industry veteran who is now a venture partner at 500 Startups, explained to me that "when evaluating new startups in this space, I look at a number of criteria including the novelty of the service as well as the ease-of-use for consumers who will be able to interact with it.[385] To both the developer and myself, it may be easy to download and backup digital wallets, but the vast majority of consumers do not have the time or inclination to devote to learning how this new type of bank account should work."

In particular, Percival is interested in taking away complexity – moving the technical processes into the background making them invisible to users. Because he works hands-on with developers on how to make UX and UI flow easier for consumers, he sees numerous opportunities for businesses to simplify processes such as the sign-up process for a particular service (e.g., online wallets).[386] Or in his words, "providing a frictionless funnel that enables consumers to conduct commerce without needing a technical background. When you swipe a credit card at a retail store a consumer does not have to pay attention to all the intermediary steps and that's the way it should be with cryptocurrencies." Nick Szabo calls this point-of-sale invisibility, "smart fine print."[387]

While neither he nor most of the investors I spoke with are interested in fiat-token exchanges, he is increasingly interested in business solutions to concepts like proof-of-existence (i.e., whether or not a document is in a particular file) or proof-of-storage (i.e., whether or not a computer system has a certain amount of storage available). In his view, "building a team with the right combination of talent, leadership and marketing to build a profitable product that can be shipped in this space is the exception to the rule. New ideas like proof-of-storage motivates everyone to rush to the door, but only a few can get in and accelerate to consumer adoption. As a consequence, an important part of their marketing effort should be focused on user on-boarding and education that builds both trust and a "coolness" factor. You cannot force trust and coolness, once you lose it, it is almost impossible to get back."

I spoke with Dan Roseman who is the founder of Coinality, a job board where employers and job seekers can connect for job opportunities that pay in cryptocurrencies.[388] According to Roseman, "While I was familiar with cryptocurrencies in general, it was not until about April last year that I began to look for actual business development opportunities. I created the platform in September 2013 because I saw an unmet need in the community that other job boards did not have; receiving bitcoin as compensation. Since launching the platform, there are now over 1,600 registered members, with over 1,000 job applications received from job-seekers, and roughly 600 job submissions (openings). While all submitted jobs are vetted by humans, approximately 95% get published and the remaining 5% are usually spam or are irrelevant. Our team also works to find other openings on a variety of other job boards and make sure they are opened on Coinality as well."

"While I work part-time with Coinbase in customer service, I currently work full-time on building out Coinality to be a real player in this segment. As a consequence I have first-hand experience and direct knowledge of the kind of jobs that businesses and entrepreneurs are looking for. Currently the single biggest demand are for C++ and Python. C++ was the language that Satoshi originally wrote the first Bitcoin wallet in and Python is frequently used by fiat-bitcoin exchanges. There is also a lot of demand for graphic design (logos and website layout) as well as marketing experts to help drive traffic to a site. Thus if you have those skillsets you will likely be able to find a job in this quickly evolving marketplace."

Roseman pointed out why employers would want to find programmers listed on Coinality. On February 10, 2014, Mt. Gox announced that there was a bug affecting its wallet-system which could potentially enable attackers to double-spend.[389] Mt. Gox was one of the largest fiat-exchanges and its

announcement caused volatility in the marketplace. Yet the bug it announced (transaction malleability) was not only a known issue, but it had been on Gox's radar for several years (e.g., its own internal wiki had an entry for it and several core developers had pointed out this issue before).[390] The problem was not with Bitcoin itself, but rather Gox's specific (error-prone) implementation of a wallet. Gox was originally created to handle the trading of a collectible card game called *Magic: The Gathering* and while the site served its original purpose, as it moved into the cryptocurrency arena its developers were unfamiliar with the needed security toolset to protect against this vulnerability.[391] Thus, in Roseman's view, "companies looking to hire developers with the necessary skillset and awareness of such exploits can be found on our job board, which hopefully will prevent such volatility-induced events in the future." With outstanding debt of 6.5 billion yen ($63.6 million), on February 28, 2014, Mt. Gox filed for bankruptcy in Japan due in part to its internal accounting mismanagement as well as other technical issues; its creditor's fate is uncertain.[392]

Bitcloud

I spoke with Kyle Torpey, editor in chief at *Cryptocoinsnews* and member of the Bitcloud development team.[393] Originally announced in January 2014, Bitcloud is an underlying protocol for decentralized applications that require bandwidth and storage. According to Torpey, "the initial idea was to have a 'cloudcoin' through a 'proof-of-bandwidth' but after some investigation and internal development the economics of trying to use a coin to back a decentralized application rather than a cryptoasset would not work the way it was envisioned. I believe Adam Levine came to the same conclusion for his own internal project LTBCoin at *Let's Talk Bitcoin*.[394] For instance, as you build more applications, the coin would likely appreciate in value and thus make services on the cloud more expensive due to fixed supply. Similarly it would be hard to balance because early adopters would be rewarded for sitting on tokens instead of using them, causing a "free-rider" problem that exists in Bitcoin and other cryptocurrencies. We have since switched frameworks and will now be an escrow service for bitcoin transactions. That is to say, Bitcloud will be 3rd party, an escrow service for sharing storage space. The way this will be done is through multisig transaction where you have multiple parties (Bob the storage provider, Alice the storage user) and Bitcloud is the 3rd participant, the mediator in multisig transactions."

As discussed in Chapter 4, multisignature transactions involve two or more parties who must submit their digital keys to a certain address within a certain time frame for an action (e.g., releasing funds) to be executed.[395]

Torpey's team is simultaneously building the first app that can utilize Bitcloud, "We want to build WeTube, a decentralized Youtube, which lives on top of the protocol and will launch simultaneously with it. I should note though that WeTube is a working title. We need to build Bitcloud first, so what we call WeTube will probably look completely different than what we have right now. The new funding model will work through a concept called Cloudshares, where with each bitcoin transaction a user would get a share in the entire Bitcloud decentralized app (an open API). Again, while the original idea was to use Cloudshares to monetize the entire Bitcloud network, we have decided to move the monetization process to the decentralized applications on top of Bitcloud. So the shares that someone receives for hosting content for WeTube would be shares of WeTube, not shares of Bitcloud. So it is really WeTubeshares, SocialDAshares, etc. For instance, if Bob purchased storage space from Alice he would use bitcoins as the intermediary token. In exchange he would receive a share of Cloudshares which then solves the early adopter "free-rider" problem because many adopters do not provide or generate new value as speculators. Another way to think of is, Cloudshares is like a share in decentralized app which

continuously builds the entire network. In our view it is not a good idea to monetize the underlying protocol, because if you had shares in protocol layer then you would have to have dividends. Or in other words, one cannot invest in Bitcloud, only in the decentralized applications built on top of it. Thus Bitcloud is a free protocol, and we are not monetizing that aspect of it. Because that would mean the transactions between those hosting would be more expensive. Now, instead, we are putting the shares into the layer above Bitcloud, which will be divided by specific applications – including possibly a Facebook-like social networking service. As a consequence, apps themselves are not centralized in one system but rather will interact with a protocol, Bitcloud."

Coinsimple

In February 2014 I spoke with Nikos Bentenitis. Bentenitis is the co-founder of CoinSimple, vice-chair of the education committee of the Bitcoin Foundation and also creator of the MasterProtocolEducation.org project that aims to inform the community about the Master Protocol and Mastercoin. CoinSimple was briefly mentioned by Eddy Travia in chapter 6 and in Bentenitis' words, "CoinSimple makes it extremely easy for e-commerce merchants to accept Bitcoin. With CoinSimple you can use any of the existing payment processors (BitPay, Coinbase, BIPS, GoCoin) and you won't need any developer to integrate them to your e-commerce store. We have done the development for you and added customer analytics in a simple user interface."

In terms of what may be the first use-cases of smart contracts working on next-generation platforms, he thinks that it may be, "the issuance of asset-backed cryptocurrencies that can be used to fund projects. For instance, a solar energy park can be funded with the issuance of a user-defined cryptocurrency that guarantees the delivery of a certain amount of electrical power after the park is operational." Similarly, he thinks the adoption rate of cryptocurrency-related apps will vary from region largely due to existing infrastructure (or lack thereof), "For people who live in the US and the rest of the developed world, there is maybe not much that crypto-currencies can do to become killer apps. But for the rest of the world, simple payments, the ones already supported by the Bitcoin protocol, when introduced in existing devices (cellphones, bank cards) would be the killer app."

Consequently he also thinks there are untapped areas that have been overlooked, including in education, "There is so much going on in the space and even a motivated investor cannot follow the amazing opportunities that arise daily. I am certainly playing catch-up every day. Educational and research groups in the space, like the ones I am working towards with the University of Texas, the University of Nicosia and the University of Hong Kong might provide a way for investors and entrepreneurs to identify business opportunities faster."

Bentenitis raises an interesting point regarding educational opportunities in this segment. Just as programming languages and network engineering spawned numerous training programs (CNA, CCNE, MCSE, A+), there will likely be a similar market demand for trainers to provide developers and entrepreneurs with the skills needed to effectively utilize these new platforms. Perhaps your firm can create a certification process for cryptocurrency or smart contract design competency. Similarly, authors and writers may find new audiences through manuscripts published through O'Reilly Media or even 'Bitcoin 2.0 Platforms for Dummies.' In addition, Bentenitis noted during our conversation that MOOCs (massive open online courses) such as Udacity and Coursera could be utilized to provide knowledge and training of cryptoprotocols to a global audience.[396] As of June 2012 there were approximately 2.4 billion global internet users some of whom may be interested and capable in learning more about this space.

BitPay

In February I also spoke with Stephen Pair, cofounder and CTO of BitPay and board member of the BitGive Foundation. As noted earlier in this chapter, BitPay is a large merchant payment processor and it recently released an open-source fork of bitcoinJS called bitcore.[397] According to Pair, "the idea behind bitcore is to reengerize and simplify the process of developing applications that utilize the Bitcoin protocol without having to deal with C++. By using a virtual machine through JavaScript and node.js, it makes it easier for developers to run their code on any OS and platform, creating a very flexible process that fulfills our initial goal: to make it open and immediately usable by people. We now have 6 people working on it full-time and the goal there is not necessarily to create a specific app but to create a library for the entire community to build from." Node.js is a platform built on Chrome's javascript runtime enabling developers to build and scale applications.

"In some ways this is similar to the Colored Coins project because bitcore works in conjunction with bitcoind [daemon] meaning there is no need to recreate an independent blockchain or validation process yet it enables and gives developers more functionality that does not exist today. Insight[398] is a good project to that illustrates how it has real functionality and provides real value to end-users."

Just as web browsers were organically adopted for solving real needs, according to Pair "I think cryptocurrencies in general provide a better accounting system and level of security relative to existing financial systems that could be abused. As a consequence, I think it is just a matter of time before mainstream adoption occurs and that there is not necessarily a "right idea" that will catalyze this. If you look at the direction that cryptography and cryptographic accounting are heading, it will just be a matter of time before something like Bitcoin is adopted industry-wide, it just makes sense. For instance, there is a need for secure international payment systems, especially for Africa and South America and Bitcoin provides this today."

In terms of next-generation platform, Pair thinks that, "while there are several ambitious projects currently being developed to remove the perceived 'ugliness' in the current protocol, I see this endeavor as Betamax versus VHS. VHS won out in the format war despite lower fidelity and it is possible that the new innovations which arise from the '2.0' projects will be adopted and integrated back into Bitcoin. In the past, I've worked on several software projects that required a team to simultaneously solve 10 to 12 hard problems, without which the underlying functionality could not be capitalized off on. Thus, unless these teams make substantial progress on all fronts, they may be taking on too many things at one time. In our perspective, "the perfect is the enemy of the good," that is to say, HTTP is not as elegant as a lot of other projects that were being developed at the same time, but it is now widely used because it worked good enough – and because the other competing teams suffered from trying to make the most elegant, perfect solutions."

Betamax was a proprietary recording tape standard created by Sony that competed with VHS, a similar yet license-free technology developed by JVC.[399] Despite technically superior fidelity specifications, Betamax lost that 'format war' as consumer adoption was relegated to small niches. Similarly there are multiple versions and forks of HTTP, some providing better technical specs, but the one that was adopted was considered 'good enough.'[400]

Part of BitPay's long-term focus, according to Pair is, "We ultimately would like to make it easier to create and integrate multi-signature technology. This alone will make wallets more secure, easier to manage and ultimately user-friendly because right now for the average person it is virtually impossible

to secure a wallet. As a consequence, I think companies such as Apple and Microsoft will end up integrating wallets built into their browsers because of the current support for nodeJS and V8 within existing browsers such as Chrome." V8 is an open-source javascript engine developed by Google for Chrome.

Kraken

In February I spoke with Jesse Powell, founder and CEO of Payward, the parent company of Kraken.[401] Kraken is a virtual currency exchange in which users can trade several different cryptocurrencies as well as fiat.[402] According to Powell, "projects like Ethereum have some interesting claims and ideas that you cannot do today with other platforms. We have also looked at others like Colored Coins and Mastercoin as well, these are all interesting concepts. However, one of the main advantages of having a central server to trade with is that it enables high-frequency trading (HFT). In addition, one of the reasons that Kraken currently enables trading pairs with Ripple (XRP) is that, it is easier and more robust to issue an asset because the network was built for it."

While one of the low-hanging fruits of smart contracts is securities trading, it is highly unlikely that a professional trader would use a blockchain directly for an HFT. For example, in most markets, especially the very liquid ones, where latencies are counted by increasingly smaller segments of time, the pace of 1 block per 10 minutes (or even 2.5 minutes) is limiting. Currently the only way to enable this functionality is via an off-chain solution, such as Kraken, which allows users to build functionality around an internal API.[403]

In February 2014 I spoke with Salvatore Delle Palme, digital strategist at Kraken and founder of Ripple Federation. In terms of immediate business opportunities in this space, in his view, "anything that connects disparate systems is a good idea. There will be a lot of opportunity in improving the interoperability between existing digital currency systems, legacy financial systems, and cryptocurrency 2.0 protocols. Merchant integration will also take on a whole new meaning as the industry progresses. In addition, I wrote an article a while back for *Let's Talk Bitcoin* called *The Archetypes of Virtual Currencies*, where I said something about how popular culture would play a role in the success of some future alternative digital currencies.[404] I was actually ridiculed slightly in the comments for that. Fast forward six months and we've arrived at Dogecoin. A coin based on a silly Internet meme has the third highest trading volume and the fifth highest market capitalization of the entire ecosystem! Dogecoin proves that popular culture matters, and that there's room for more proof-of-work coins like Bitcoin or Litecoin. Part of the success of Dogecoin can certainly be attributed to its role as a 'tipping currency' with exponentially more units than Bitcoin. It's more fun than Bitcoin, and fun has value."

Dogecoin is based on the same codebase as Litecoin, yet its developers took a different approach to marketing – basing it solely around an internet meme – and as a consequence, its popularity measured by a variety of metrics (network hashrate, daily transactions, reddit followers) has surpassed Litecoin.

One of the common themes of the investors, developers and entrepreneurs I spoke with is that of 'rebooting' the financial system, plugging it into modern technologies. According to Delle Palme, "it's taking a while to get the financial system rebooted on the web, but I think things will start accelerating more quickly once this trend is further along. The cryptocurrency layer is being built up nicely, but the social layer is feeble. For example, we appear to be nowhere near being able to send money to a friend or a merchant over Facebook, let alone all of the other social platforms (although PikaPay is doing some interesting things with Bitcoin and Twitter). Eventually, a much higher level of cohesion will be achieved."

Another area that some investors have mentioned is that a trading platform akin to e-Trade or Scottrade is currently lacking in the cryptocurrency space. Delle Palme sees that, "Kraken's service is optimized to be a FOREX platform for digital currencies. Although, because we offer sophisticated security options, such as two-factor authentication and master passwords, Kraken is a great place to store digital currency. Furthermore, I believe Kraken was built from the ground up to be immune to issues like transaction malleability. Our developers have been aware of the issue for a long time." As mentioned previously in Chapter 3, in mid-February, several exchanges – most notably Mt. Gox – were impacted by a known bug called transaction malleability. For balance, Coinbase and Blockchain.info, the two largest web-based wallets were not affected as well.

As noted above, Kraken operates as an exchange of multiple different cryptocurrencies, including XRP, the token unique to the Ripple network. Long-term Delle Palme thinks that, "Ripple has a lot of advantages. The biggest one for me has simply been that they actually have a robust product that works. This is why I worked to bolster their community. I knew that Ripple would be successful at achieving some important things the rest of the Bitcoin community was unlikely to easily achieve, such as a distributed exchange (e.g. the Ripple system has a distributed exchange built-in) and smart contracts. XRP is fueling the growth of a great company, and Ripple offers liquidity and innovation. I suspect they will continue to gain support from open source communities and entrepreneurs around the world and eventually do amazing things." He is also looking into the potential of Ethereum as way to "marry a cryptographic asset to an original work of art, and support the value of this asset via social consensus. In general, altcoins allow for experimentation within the crypto-mining community. I think Ethereum will become the standard for altchain experimentation and provide many new uses-cases, such as an 'artcoin.'"[405] In addition to Namecoin, Bitcoin, Ripple (XRP), Litecoin, and Ven (XVN), Kraken recently added support for Dogecoin.

Chapter 8: Jack-of-All-Trades?

Can Bitcoin do everything? I spoke with Adam Levine, editor-in-chief of *Let's Talk Bitcoin* about the future of altcoins and DACP.[406] According to Levine, "unfortunately many crypto proponents are conflating cryptocurrencies (an ecosystem of protocols) with Bitcoin (the protocol) and bitcoin (the token) – yes, bitcoin is a cryptocurrency but not all cryptocurrencies will necessarily be (a) bitcoin. They are not mutually exclusive and are all part of the larger cryptocurrency ecosystem. Another way to think of it is Bitcoin is a specific reference implementation of Cryptocurrency but not the definitive technology as it does not solve all the problems, otherwise nobody would care about Ethereum, Mastercoin or Counterparty. Thus it would be imprecise to just say Bitcoin is the only real cryptocurrency because the altprotocols and "2.0" projects all learned from limitations of Bitcoin; borrowing lessons and ideas but not necessarily the code. And as a consequence, immutable algorithms employed by these improved DACPs and cryptoprotocols empower users to choose their own parameters, boundaries and even create voluntary associations."

Levine also sees Bitcoin as a type of highway and the other platforms and protocols as off-ramps. Yet, in time other protocols could also become highways and thus an interconnected series of decentralized, encrypted highways would transmit and track value globally in a frictionless manner. As he says, "it is an open source ecosystem filled with numerous competitive platforms. There will probably be a marketshare 'winner' in a few years that is bigger than everybody else and at that point, all the other participants will retarget their DAC development at the new platform. Perhaps they will fork the winner and start from there."

While not everyone agreed with method or path, the one common theme from everyone who provided insights to this guide was: do not be afraid to take risks. Nearly each person I spoke with had started a company in the past and experienced failure first hand. Do not let that stop you from trying a different approach. Learn from your mistakes and be open to changes. This might sound cliché but the world has never seen anything like a cryptoledger before and incumbent institutions are now paying attention. In fact, in its latest 10-K filing with the Securities and Exchange Commission (SEC), eBay named both BitPay and Coinbase as potential competitors to PayPal.[407] Similarly in January 2014 Wells Fargo held a meeting on how to assess and ascertain the legal and competitive issues that cryptocurrencies create.[408]

While the Bitcoin protocol has grown immensely in the past five years, it is still quite young in terms of market penetration. At the time of this writing, the market cap for bitcoins (all 12.4 million that have been mined) is roughly $7 billion. For comparison, according to the World Gold Council, as of December 2^{n} 2013, there is roughly $6.8 trillion in above ground gold.[409] And global e-commerce sales topped a collective $1 trillion in 2012.[410] While there has been a concerted focus on the token value of bitcoins this misses the forest for the trees. The potential market cap for all trustless asset management is the same sum total of known assets which is several orders in magnitude larger; the key difference is how they are managed and transferred. Some assets, such as deeds and collateralized loans, are easier to encode as a smart contract; others may be more difficult. Similarly, existing blockchains are limited in terms of what secondary attributes they can store (e.g., hashes of contracts) and, due to their confirmation periods, are not ideal for transmitting securities in an HFT manner.[411] Thus cryptoprotocols today, should be seen as works in progress with enormous potential.

With the knowledge of the previous chapters, the question that decision makers, executives and business development managers should ask is, what can cryptoledgers or smart contracts solve for large organizations with established networks, retail operations, or mobile assets? Time-stamping and HR

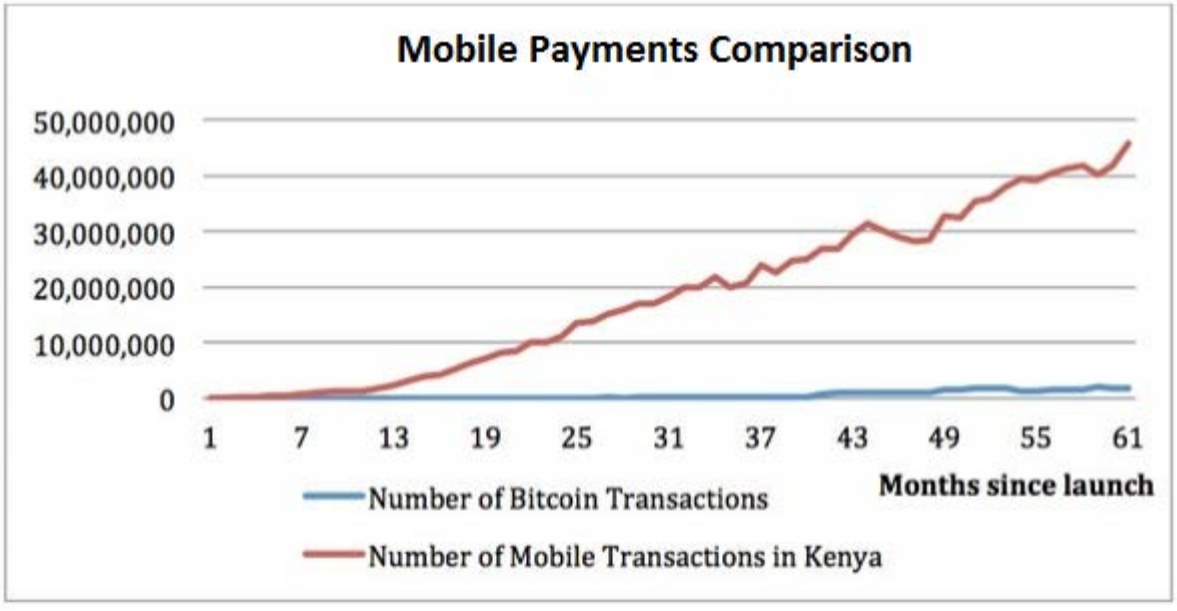
automation have already been discussed, as have customer-reward programs like frequent-flier miles, so what about monitoring car fleets? Or perhaps Bitcoin is not needed to perform every function; perhaps it will serve as a bridge for some, but not all virtual exchanges.

Niche payment processing platform

At this time, while it is very good for remittances, Bitcoin is not a competitive payment system for many parts of the world. It can be used, but it is not ideal. This is because the confirmation rate of its currency (bitcoin) is too slow and relatively expensive – the transactions per second has lagged behind the price. Similarly the protocol is less than optimal in most transactional settings because it is cumbersome, not Turing-complete, and not intended for this specific purpose, preventing developers from building transactional and contract systems, services and applications on top of it. As a consequence, its usability is still extremely limited for most mainstream payments such as point-of-sale; and software and infrastructure must be deployed to take it to a network capacity of 100s or 1000s of transactions per second instead of the current 7 per second.

This situation may be temporary and could take a few years to resolve – and at that point perhaps we will see payment adoption take off but this would require substantial changes to the protocol. For example, perhaps by that time blockchain pruning (SPV) will be implemented to eliminate all spent outputs from the blockchain (shrinking it substantially).[412]

David Evans, a law professor at the University of Chicago, recently published a payment platform comparison between M-PESA (in red) and Bitcoin (in blue).[413] Below is one figure reprinted with permission:



As Evans points out in his article, M-PESA was first introduced in Kenya in mid-2007 whereas Bitcoin was launched in January 2009. Yet as I mentioned above in chapter 6, M-PESA is so widely used in Kenya that roughly 43% of its annual GDP is handled through this mobile payment system, the same obviously has not occurred with Bitcoin yet (perhaps it could with other systems such as NXT or Ripple).[414][415]

It should be noted that the direct comparison is not entirely apples-to-apples either as the Bitcoin transactions in this chart only include on-chain transactions.[416] Coinbase and Circle use off-chain wallets which permit users to buy, sell and trade bitcoins (including micropayments) instantly that would otherwise take tens of minutes to confirm via an on-block chain implementation. An off-blockchain solution also allows users to trade below the dust limit (roughly 5460 satoshis) which is an artificial limit implemented by the developers several years ago to prevent spam from propagating the network (e.g., a malicious user could send out millions of 1 satoshi, each of which needs to be added to a block, thus taking up time and resources). BTC-e takes this off-chain approach a step further by allowing users to build bots that interact with its API, enabling high-frequency trading. None of this is possible on-chain and thus these types of transactions are not represented in the image above.

But Evans is right to bring this criticism up and it is an issue that has motivated other developers to build these 'next generation' platforms described in chapter 3. For example, Bitcoin currently has a hardcoded block size of 1 MB, or 7 transactions per second. In contrast, Visa's payment processing centers handle on average of 2,500 transactions per second and are built to process a surge of up to 10,000 to 20,000 per second.[417] Other platforms such as Ripple have a purposefully more robust payments system, in the case of Ripple its current setup, while security conscious, can handle 100 transactions per second but it is designed to handle at least 1,000 transactions per second as well.

Again, this may not be an issue in developed countries, where users have easy-access to Bitcoin wallets (both web and mobile based). And because of the relatively large fees described in Chapter 6, cross-border remittances has been one of the 'killer' apps for Bitcoin and will remain so into the future. In fact, despite the fact that it takes 10 minutes for one confirmation, it is still quicker than other existing remittance processes such as ACH which can take three days to clear.[418]

But as an RTGS, a real time gross settlement service, where transactions clear near instantaneously, it cannot compete at the same level as credit cards or M-PESA.[419] This is an issue that potential entrepreneurs should keep in mind. In fact, while there are certain days that $50-$100 million worth of bitcoins are processed along the network, that is about as much as MasterCard and Visa process in a few minutes.[420] For comparison, in 2013, MasterCard and Visa processed a combined $7.4 trillion in purchases. Together with American Express and Discover, these four companies generated $61.3 billion in revenue during the same period. While credit card companies like Visa can make the clearance of payments even offline (they download the blacklist on terminals) and M-PESA is quick and easy via SMS, the slower confirmations are a challenge for Bitcoin as it makes its way into the mobile payments space.

Usage rates

Readers may be wondering just how many users actually use Bitcoin or other cryptocurrencies. Because of the decentralized nature, it is a difficult answer to actually provide. In addition, it is difficult to differentiate between those who have exchanged a fraction of a bitcoin at any time and those who are actively using bitcoins today. For instance, according to Bitcoin Pulse, the number of cumulative individual wallet downloads hosted at Sourceforge is 5 million; yet as shown below, this is not the only type of wallet users have access to.[421] Other metrics, such as looking at popular social media sites like reddit or Bitcointalk are also inconclusive because while there may be 110,000 redditors subscribed to the Bitcoin channel, many of those are likely sock puppets. In addition, readers should keep in mind that a user of bitcoin can be defined as a user even if the amount they transmitted is a little as 1 satoshi (0.00000001 bitcoin) or as large as 1 million bitcoins.

While roughly 1.1 million Bitcoin addresses hold 99.99% of all bitcoins (as of block 285,000), this is not the equivalent to saying only 1.1 million people hold all the mined bitcoins.[422] As of this writing, 107 addresses hold 21.76% of all mined bitcoins. Again, this does not necessarily mean that only 107 individuals own roughly one-fifth of all bitcoins. For example, some of these addresses belong to large exchanges and web-based wallet services such as Coinbase and BitStamp. Because these customer wallets are off-chain it is impossible as an outsider to know exactly how many people actually own and use bitcoins behind this wall. Coinbase now has over 1 million customer wallets and it is unknown how many of these users actively trade and use bitcoins with other internal services.

Yet, there is likely a liberal upper bound estimate of roughly 10 million users on all platforms in the ecosystem today. There are two ways to derive this number, the first is from the fact that there are roughly 10 large web-based exchanges. If each of these has one million users, which they likely do not, then that is approximately 10 million users.

Another way to derive the 10 million is through the limitations of using microtransactions directly through the blockchain. Because of anti-spam provisions know as the dust limit, users currently cannot send less than 5460 satoshis on the blockchain directly, otherwise that transaction is not incorporated into a block. For users in developing countries looking to conduct in commerce and or even remit with bitcoins, there are few formal exchanges based in these regions. Thus they will likely use on-chain wallets and if they use on-chain wallets their transactions will be limited to sending bitcoin values above this dust limit. As of this writing 26.39 million addresses (95.27% of all on-chain addresses) hold bitcoin balances between 0.0 and 0.001 bitcoins. However, it is unknown how many of these addresses are actual active users or how these are abandoned addresses (e.g., forgotten about, lost private key, used as a temporary go-between address, mining transaction fees, unclaimed reddit tips, etc.). Usage rates of many other cryptocurrencies follows similar patterns. This dearth of fiat-to-cryptocurrency exchange in emerging markets presents a business and educational opportunity for entrepreneurs such as bitcoin ATM providers as discussed later in this chapter.

Decentralization for decentralization's sake

In conducting the research for this manuscript, I spoke with several investors who explained that using crypto for crypto's sake or decentralization for decentralization's sake is not a particularly efficient or effective business or even developmental model. In fact, centralization of information and assets can and is oftentimes easier to manage in most industries. Just because Bob stores data in a centrally managed Amazon cloud server, does not make his enterprise any less effective. In fact, the code probably runs much quicker due to how AWS can scale (e.g., less distance and therefore less lag between computing nodes).[423] Furthermore, just because some system can be decentralized, does not mean a business owner should do so. In fact, irrespective of cryptocurrencies' long-term potential, a total-cost-of-ownership (TCO) analysis should always be done by anyone wanting to move from one infrastructure to another. Perhaps the opportunity costs of keeping the existing system are less than switching and managing another.

Similarly, others have explained to me that making a product easy-to-use should not be the penultimate goal either; rather, developers and entrepreneurs should instead answer these questions: What problem does this solve? What need does this satiate? Why should others use it? Bob could extol the virtues of cryptocurrencies to his relatives and convince them to purchase bitcoins or dogecoin as a speculative investment, but what would they use it for in their daily life? How does it make their life any

better or easier? Just because you can decentralize, should you? These are the kind of questions that start-ups in this space need to answer.

This insight could save many people a lot of headaches in the future. Instead of forking code and reinventing the wheel, several sources I spoke with think developers should learn from the mistakes of the open-source community fifteen years ago. Where there were endless Linux distributions being rolled out and semi-funded, each had technical advantages, yet few could convincingly provide a solution to specific problems and garner mass market appeal. And ultimately after years of consolidation and market purges, the most popular Linux-based end-user package was not Ubuntu or Fedora, but Android – which simultaneously satiated customer demand and solved needs in an easy-to-access manner.[424] Thus, when looking upon potential investments, this investor will often ask startups in this space why do you need a decentralized system running in the first place. What is the burning need? In cases such as maintaining IT infrastructure they could in fact create higher costs or produce negligible gains.[425]

One investor explained to me that while critics are right to point out that there has thus far been a limited buy-in of mindshare of these new technologies, they should also acknowledge that existing system today replaced other systems and so on. Whereas previously brokers traded on the exchange floor, electronic traders were viewed as outsiders and the floor traders were the insiders. That role has reversed in a matter of decades. Like the horse-and-buggy before it, any new disruptive technology will seriously impact the landscape creating winners and losers. What entrepreneurs need to try and figure out is how they can position their firm to get on the winning side. Maybe it is blockchains, maybe it is consensus ledgers, maybe it is something else entirely.[426]

Cost benefit analysis of decentralizing

Too much of a good thing, however, can be problematic. While a lightweight proof-of-stake or Ripple-based cryptoledger could be used internally by corporates to replace auditors and accountants (e.g., reducing administrative overhead, electrical and equipment costs), an intranet-based proof-of-work cryptoledger - while possibly being able to achieve that objective - may be a solution looking for a problem.

Unlike the Internet, intranets are based on centralized network controls where all actors are known and all actors are already constantly monitored and there is trust. Because trust is enforced by administrative oversight, the problem of tracking financial and other assets is suitably addressed for normal commerce by existing technology.

Our example begins in the future, where cryptoledgers and smart contracts provide accounting and auditing but also utilize tokens to track and manage inventory and logistics internally. With this technology, inventory systems that could be compromised and abused might instead be replaced with cryptoledgers. If Bob owns a large media store, he could manage and track all of the books with embedded RFID tags; instead of building and trying to maintain a relatively costly proof-of-work infrastructure (e.g. hardware expenditures, electricity), because it could conceivably run on a smartphone, a proof-of-stake ledger could easily be maintained, powered and integrated within cash registers, point-of-sale terminals and nearly any intranet-connected devices. The cryptoledger could itself be managed by a DAO which then connects it to a larger corporate VPN to franchise locations and vendors in the supply chain, each of which have their own ledger and so forth.

Again, the token itself is unimportant from the perspective of human agents; it is not used for some value-based exchanges but for internal bookkeeping and rationing. In all likelihood, if a cryptoledger is used internally, the tokens would all be premined. Another example of where the technology might be applied would be automobile dealerships and car rental facilities. If Alice runs a Hertz franchise she could install a proplet (a MEMS device that can interact with smart contracts and cryptotokens), with which she could control the operation of a vehicle based on the lease agreements - including reverting control of the vehicle to a new owner all via a cryptoledger. This kind of functionality extends beyond automating the movement of information – individuals can already buy, sell and rent vehicles over their mobile, but must use trusted 3rd parties and payment sites.

A cryptoledger, on the other hand, removes the necessity for 3rd party involvement. For example, Hertz could implement an internal proof-of-stake ledger at each location, and a DAO would connect the ledger via a VPN to the parent company. Each car ignition would be fitted with a proplet that can communicate with the ledger via a cryptographic handoff (a token of some kind), and therefore any customer or owner could use smart contracts to pass ownership off to other approved individuals. Or, if it is a self-driving vehicle, it could start and drive to Alice's home and drop her off at the office. The 'minting' of tokens within the POS (or POW) ledger is not important as a store of value but again, is used to track and manage inventory in an unforgeable manner.

Consequently, neither Alice nor Bob are locked in within any specific vendor of cryptoledgers, as these systems are currently open-source. Furthermore, because a DAO manages the edge of the network, they can work with decentralized exchanges that enable customers from any part of the globe to transfer one type of cryptocurrency for a cornucopia of tokens representing thousands of assets, thereby creating a frictionless environment for decentralized commerce.

But would the cost and unfamiliarity of adoption of cryptoledgers over existing technology which serves the same purpose be worth it? It is probable that for smaller businesses the opportunity cost - the new skill sets which employees would need to learn - might be prohibitively high, particularly given the dearth of software tools available for the technology. Some, however, see that businesses with sufficient scale might be employ cryptoledgers - sooner rather than later - for strategic applications of a capital-intensive nature, such as obtaining funding from the capital markets, as Preston Byrne suggests in chapter 2. "A smart contract could be written which permits vehicle immobilisation as part of security enforcement, as Nick Szabo proposed," Byrne says. "Depending on applicable local laws this could be provided as a security package for issuer SPVs. The example of Hertz is particularly instructive - while the company has embarked on whole-business securitisations in the past, this technology might improve the quality of the company's collateral to a sufficient extent that future transactions could be asset-backed instead of being backed by all of the firm's receivables, lowering its funding costs. In a broader automobile lending context such a system could be used by any lender to dramatically reduce servicing costs while providing considerably better loan-level data to prospective investors."

Thus the opportunity costs, the seen and unseen of implementing and maintaining a decentralized cryptoledger should be taken into account. Similarly, at some point traditional players could enter the market when cryptocurrency has enough traction and either build something themselves or try to buy the new established players.[427] For example, if Coinbase continues to increase in popularity, perhaps Wells Fargo would absorb it. While speculative, perhaps the upcoming launch of SecondMarket's exchange, a New York-based platform, could be acquired down the road by JP Morgan or Chase.[428]

NGO use-cases

In an exchange with Petri Kajander, an entrepreneur and a senior fellow at The Cobden Centre, an economic think tank, he sees “a lot of parallels with the dotcom boom and also with the mobile boom. They also started with basic protocol and infrastructure levels and built up from there to the more sophisticated services once the basic layers were settled and established. It is sort of a similar story here. You cannot aim too high at the beginning since the basic building blocks are still not in place. Also, even though you might be anticipating the right services and needs - your timing might be off. The end users are just not there yet. The sweet spot might be still years away - even though the technical capabilities could be in place. There is going to be a lot of trials-and-error, and huge amount of luck involved, for some. The trick is to try and monetize throughout the journey. For instance, the most boring applications may be the most profitable in the beginning; like a financial back office and corporate administrative solutions providing the biggest savings in the first phase. Market participants should also be aware and cognizant of regulatory bodies and policies – they do play a role in the development and deployment zigzag. And different governments have different incentives and approaches to the matter. This may have interesting tipping points and "good enough" technology selection and market approval choices, even by pure chance.”

Mundane applications such as tracking inventory or coupons as described in chapter 5. Perhaps integrating a CRM API with a ledger could allow companies to track customer sales, or as mentioned in chapter 4, figuring out ways to integrate EDI with a ledger could likewise enable robust and secure supply chain management with all vendors. Kajander also sees some of the current crypto-based solutions hammer-like, or in his words, “everybody in the field is excited and has a proverbial hammer in their hands. And there seems to be so many nails all over the place, or at least that what they seem to see.” Not every solution needs a new ledger or needs to be decentralized.

One comparison that Kajander used involves the disintermediation of the entertainment industry, “if you look at Napster and BitTorrent, both created disruptions to the marketplace and after the dust settled, it was iTunes and Netflix that became the platforms adopted by mainstream consumers. Similarly Orkut was incredibly popular with specific countries like Brazil and India but was completely passed over by the larger social networking consumer-base. In many ways, these platforms being built today could start as a Napster but end up as iTunes. In fact, while there was a lot of idealism in the ‘90s about what the internet could do or should do, the actual long-term use-cases involved a balancing act between capabilities and policy making.” Netflix and Youtube combined now account for roughly half of the bandwidth consumed during peak-hours in the United States.[429]

Kajander and several others I spoke with, see an intersection between cryptoledgers and non-profit organizations as well. As noted in chapter 5, there was a notable example of fund mismanagement in China related to the 2008 Sichuan earthquake. According to Kajander, “in the future non-profits such as the William and Melinda Gates Foundation could utilize cryptoledgers to track their donations projects or even funds throughout the globe, providing a transparent and real-time auditable framework to their initiatives. Perhaps even a Kiva and Bitcoin-like mashup could emerge for similar emerging markets.” Kiva is a non-profit organization that allows people to send and receive money via the internet to entrepreneurs and students in underserved countries. Other charities could benefit from this transparency as it also reduces administrative overhead by removing the need for several functionaries.

Continuing, “the blockchain is virtually incorruptible, it cannot be changed or reversed. So in the future, having elections could be as easy as each user submitting their digital signature for a particular policy or candidate and the election could be both quickly verified and difficult, if not impossible to cheat. Voting is not limited to national elections either, as villages, classrooms, any organization could use a token-based cryptoledger system to provide a transparent mechanism for the electioneering process. All someone needs is access to a mobile phone or laptop.”

Specific examples could be community organizations that hold votes to release funds to improve hospitals, schools and libraries. Coupled with the assurance contracts discussed in chapter 2, voters or voiceholders as Adam Levine describes them, could review the votes and act on the consensus. Thus as Kajander and Hakim Mamoni have explained, you can remove middlemen, bureaucracies and allow direct involvement between two or more parties (e.g., reduce the hierarchy between the borrowers and lenders; recipients and donors).

Another way that for-profit companies can utilize this token system is through a matching campaign. For instance, if you purchase $50 of Nike products online, a cryptocurrency could be issued and sent to your wallet. In an offline situation, the product could have a scanable QR code that serves the same function. They can then be sent to a charity or NGO of your choice and Nike will redeem and donate a certain amount of prearranged money to the recipient. In Kajander’s words, “these initiatives could be for a particular purpose (e.g., infrastructure for clean water, new trees planted) and could scale into the hundreds of thousands, even millions through the use of smartphones.” Again, as described in chapter 2, these tokens do not necessarily have to have some kind of fiat value attached to them, but rather serve as a virtual representation of a vote.

China

At a basic level there appears to be a lack of clear property rights and contractual rights in China. While some jurisdictions like Shanghai are more transparent and modern than others, no one actually owns property for more than 70 years, after which it is automatically reverted back to the state.[430] In many cases, the actual property may only have a 40 or 50 year lease left because of the different staggered stages of post-Mao liberalization. Furthermore, at any given time some of these titles can be revoked or modified by a 3rd party without due recourse.[431]

As a consequence, despite reforms over the years, land confiscation is still common. For example, each year approximately four million rural Chinese are evicted from their land.[432] Why? Because, according to an HSBC report, local governments generate 70% of their income from land sales much of which are ill-gotten gains for one or more party (e.g., state-owned firm’s pressure local leaders to evict farmers from land).[433] Through the adoption of cryptoledgers, each level of government could benefit, not only by being able to track and manage the funds of its associates, but by being able to track these land titles in a transparent, unforgeable manner.

Additionally, a 2004 report from the OECD found that roughly half of all urban Chinese workers primarily migrant workers from the inner provinces participated in the “informal” sector.[434][435] They might benefit if their payroll and compensation was managed by a decentralized autonomous organization (DAO), a cryptographically controlled AI agent, rather than a human boss (*laoban*) who could arbitrarily change his or her mind or otherwise abuse the relationship (e.g., change the contract *ex post*).[436][437] For instance, without an urban household registration (*hukou*), most of these migrant workers are left without any legal recourse in the event that their contracts are tampered or ignored.[438] Yet with an

independently run DAO these same individual could potentially still be automatically paid based on previously agreed to condition or at least bring the issue to an arbiter; and if they are recognized, a government court.

While it remains to be see how policy makers will react to these new innovations, these cryptoprotocols could provide new tools for everyone to reduce costs and secure value.

Startup Cities Institute

Zachary Caceres is the executive director of Startup Cities Institute (SCI), a non-profit research center at Universidad Francisco Marroquín located in Guatemala.[439] In an email exchange I asked him why an NGO and specifically his project would find cryptocurrencies of use. In his words, "at SCI, we are most excited by the humanitarian possibilities of cryptocurrencies. Many of the world's poorest face high inflation and instability in their national currency. Despite all its volatility right now, cryptocurrencies may actually prove to be a better choice than politicized money in some developing nations. In countries like Guatemala, where we're based, security is also a constant problem. Robbery is common, especially in poorer neighborhoods. Cryptocurrencies could be a safe alternative to store your savings."

As noted earlier by Alan Safahi as well as Wences Casares and Sebastian Serrano, one of the areas that cryptocurrencies can already disrupt is the remittance marketplace. In 2012, approximately 1.5 million Guatemalans (roughly 10% of the population) worked abroad and remitted $4.8 billion back home, making Guatemala one of the largest receivers globally; and remitting through Bitcoin or Ripple could reduce the fees substantially.[440] As Caceres notes, "With Bitcoin or another digital currency on both ends of the transaction, you could have instantaneous transfers at a much cheaper rate. Perhaps something like a debit card could be loaded from the U.S. and then cashed out in a developing nation. There is a huge market opportunity here."

One challenge that his team is facing with their new incubator, *SCI Ventures*, is developing an ATM. Their goal is to bring cryptocurrencies to developing countries and thus because most people do not always have a computer or reliable internet access, in their view "people will need an easy interface, either by phone or ATMs." So how could they make a secure Bitcoin ATM ubiquitous in the streets of cities like Mumbai or Nairobi? "It's still too expensive. There's a long way to go. But we're working with some entrepreneurs and designers to try to push this along."

Other projects and vendors in the Bitcoin ATM space include Lamassu, Skyhook, Genesis and Robocoin.[441]

And how does this tie in with the rest of the guide? According to him, "this interest in cryptocurrencies ties in to our broader project, Startup Cities. What if law and governance is just a technology like any other? Smart property and smart contracts raise this question clearly. If law and governance is just a technology, then perhaps it could be open to disruptive innovation. What we are developing at SCI is the idea of using small zones to pilot comprehensive reforms in the legal, political, and economic systems of nations. Instead of trying to fix the whole country, just make several small, competing zones with different institutions and let people vote with their feet. Some may fail and others may be spectacular successes, just like in any other startup environment. The startup municipalities that work can grow by attracting money, talent, and capital. Nations can then bring good reforms to the national level. This is a low-cost, low-risk way to bring major improvements to the developing world. It does not force anything on anyone, and respects human rights each step of the way."

Startup Cities has a unique entrepreneurial approach to public policy that is being pursued by other independent groups including Blueseed and the Urbanization Project (e.g., Charter Cities).[442]

Another issue he brought up was one that Preston Byrne, Hakim Mamoni and Petri Kajander have also discussed: using cryptoledgers to provide transparency for organizations including governments. In his view, "we have the broad outlines of a transparency platform we call MuniBit. It seems possible that with public Bitcoin wallets or another transparent cryptoledger, you could bring near-total transparency to a government's finances."

Another obvious application of transparent internal accounting would be for NGOs themselves because, "the governance structure of Startup Cities could also be enhanced by cryptographic technologies. At least in principle, municipal governments could be held as something like a DAO. Citizens could actually become shareholders in their local government. Citizens could make political decisions through transparent digital processes and interfaces set up around a DAO."

While it remains to be seen whether or not a DAO could provide such functionality, multisignature addresses and oracle based wallets, or Hierarchical Deterministic Multi-signature (HDM) wallets, such as CryptoCorp already exist, providing small organizations the ability to perform some of these functions such as securely voting and releasing funds.[443]

Chapter 9: Conclusions

Even with some froth that has arisen, greater functionality is coming, with a clear consensus emerging that this technology will reduce friction – and overheads – for business if thoughtfully designed for financial applications. Some platforms may succeed, others may fail – it is entirely possible that the platform which will introduce this technology into the mainstream has not even been coded yet. As Yogi Berra purportedly said, "it's tough to make predictions, especially about the future."[444] Perhaps these matrices can help, at least for now, to prevent paralysis by analysis:

Platform Matrix

Table 1:

Decentralized blockchains without smart contract functionality enabled (SCFE)	**Decentralized blockchains with smart contracts natively implemented**
Bitcoin Litecoin Dogecoin NXT Namecoin (merged mining)	Ethereum Invictus (ProtoShares, BitShares)
Protocols built on top of a blockchain or connected to a ledger	**Non-blockchain distributed consensus network**
Colored Coins Mastercoin Counterparty Open-Transactions	Ripple

Table 2:

Platform	Blockchain-based	Consensus ledger	SCFE*	Turing-complete	Open-source	Decentralized	Distributed
Bitcoin	X		**		X	X	
Litecoin	X		**		X	X	
Dogecoin	X		**		X	X	
Namecoin	X				X	X	
NXT	X		X		Partial	X	
Colored Coins	***		X		X	X	
Mastercoin	***		X		X	X	
OT			X		X	X	
Invictus	X		X			X	
Counterparty	***		X		X	X	
Ethereum	X		X	X	X	X	
Ripple		X	X	X	X		X

*SCFE means 'smart contract functionality enabled' – the protocol can use smart contracts

** The protocol has the functionality for SCFE but it has not been turned on by the development team

*** CC, MSC, and CP all rely on a parent blockchain, such as Bitcoin, for transportation and storage

Table 3:

Platform	Genesis	Core founders	Outside funding	TMST**	Market cap of tokens***
Bitcoin	January 3, 2009	1	-	12.4 million	$6.99 billion
Open-Transactions	January 2010	1	-	-	-
Namecoin	April 18, 2011	1	-	8.16 million	$27.3 million
Litecoin	October 13, 2011	1	-	24.6 million	$354 million
Ripple	February 2013	2	$6.5 mil USD	99.9 billion	$1.33 billion
Mastercoin	July 31, 2013	1	4,700 BTC	563,162	$29.4 million
Invictus ProtoShares*	November 5, 2013	4	-	1.55 million PTS	$11.4 million
NXT	November 25, 2013	3	21 BTC	999 million	$44.9 million
Dogecoin	December 8, 2013	2	-	55.6 million	$57.4 million
Counterparty	January 2, 2014	4	2,130 BTC "burned" (POB)	2.64 million XCP	$11.8 million
Colored Coins	TBA, 1H 2014	4	-	-	-
Ethereum	TBA, 1H 2014	4	Up to 30,000 BTC	-	-

*Invictus released ProtoShares (PTS) before BitShares which is still being developed

** Total mined supply of tokens as of March 1, 2014

*** Total market cap of tokens (MS x daily value) in USD

Synthesis

If you, the reader, are now asking yourself: "which platform is the best?" "Which platform should your team or business adopt and integrate into?" The only honest answer is that no one can say.

The goal in writing this guide is to provide readers an overview look into an often-hyped, but nonetheless dynamic and rapidly-moving area in technology, law, and commerce, and in writing this guide I have tried to be as unbiased and diplomatic as I can, giving equal time to different viewpoints, approaches and platforms. What they all share is enthusiasm, which can be found in abundance on the part of developers, entrepreneurs, investors, and thinkers alike.

My suspicion, on overview, is that as the technology evolves over the next two years, there will be a considerable amount of energy devoted to the sector – though there will not necessarily be a clear set of 'winners' and 'losers' in terms of platform market share and ledger-rot.

Where existing protocols all pursue ambitious goals, they remain subject to significant – and known – technical limitations and, at least to date, a lack of funding and manpower to address them. Additionally, while it would appear that there is some profitable low-hanging fruit with immediate applications, such as betting and gambling, gearing app development towards these market sectors will involve significant legal overheads and diminishing returns as there are already a number of active participants in this 'math-tax' segment.

If the goal of cryptoprotocols is to provide frictionless mechanisms to foster real economic growth, then creating applications that provide genuine increases in productivity to end-users that replace expensive existing infrastructure is likely an area for ripe business development (e.g., if gambling actually created real growth, then Las Vegas and Macau would replace New York City and Shanghai as economic centers for growth). The United States casino industry generates roughly $125 billion in revenue a year, yet most people do not gamble in part to the 'math-tax.'[445] Simultaneously there are more than 1 billion bank-issued cards in the US – most of which are replaced on a semiannual basis.[446]

How, then, can firms tap into the wider consumer ecosystem – where cryptoprotocols have not yet seen widespread adoption? Some veterans in the sector suggest entrepreneurs who are new to the space initially work on projects that do not have high compliance overheads – such as exchanges or money transmitting business - or to look at different geographical corridors to address the needs of the unbanked and underbanked in the developing world.[447] One of the reasons why WordPress began accepting bitcoin, for example, was because not everyone in the world has a Visa card and PayPal blocks user access in over 60 countries; WordPress wants to reach places where these services are not.[448] Other experts have suggested keeping the idea and execution simple: before trying to obtain a million customers, try to provide a high-quality service to a few hundred, and learn from the experience.

Alternatively, others suggest focusing on purely commercial applications, in high finance or in business-to-business platforms, due to the complexity of money laundering and consumer protection laws which apply when dealing directly with the general public. Perhaps being a software provider that does not hold the tokens, or exchange tokens for fiat, could be a safe middle ground or creating easier point-of-sale merchant accessibility with QR codes. Or as Sean Percival suggested, redesigning interfaces for consumers so that cryptocurrency becomes more accessible.

There is also a growing impetus to build bridges between existing financial infrastructure and cryptoprotocols. While enormous amounts of capital (human and financial) have been invested in this space, some projects are likely redundant – reinventing the wheel as it were – and others may be based in political, rather than commercial, motivations. Anyone wanting to get involved in his space should therefore ask: what profitable business application can be built on top of these systems? Is building another proof-of-work-based blockchain an effective use of resources or can your team sync your features to an existing ledger? Is it possible to provide new value to larger customer bases without having a Turing-complete protocol? Do you necessarily need to use a decentralized processing framework instead of a distributed or even centralized (in the case of intranets) systems? Can your development team work remotely, reducing overheads, or do they need to be located in a specific office or housing complex? Can formal partnerships with existing market participants be forged to secure more funding and better cater to their needs?

There will likely be $100 million in formal start-up funding this year however even if they can answer all of these question some of these projects may no longer be relevant once they ship code.

Instead of having to stand in one location to call another fixed location - as the landline-era has conditioned us to think of commerce - decentralization brought about by mobile phones enabled users to call and connect with specific individuals from anywhere. Smartphones and tablets subsequently opened up the ability to perform and use productivity apps, empowering new demographics to utilize virtual offices, leapfrogging the need to use traditional brick-and-mortar office parks. Cryptocurrency is similarly disrupting the way we use money and, more generally, asset management. It is one of the few areas over the past twenty years that has not been radically transformed by new digital technology – but this will likely change, as both Naval Ravikant and Eli Dourado recently analogized, Bitcoin is not money – it is the internet of money.[449] While there may be banking apps on phones, at the end of the day it is still essentially a virtual bank teller or ATM. On the other hand, Bitcoin and its progeny empower individuals to be their own financial institution – much like how Linux platforms enabled ordinary users to potentially utilize more powerful use-cases than Windows.

The interviewees for this book – and indeed all of us – are participants in an unprecedented, cryptographic, mathematically constrained experiment that is likely to impact nearly every industry. Yet it is clear that decentralization is not necessarily the answer, the silver-bullet or panacea to every economic problem; it is merely a tool, a solution for some things, but not for all, and corporations, organizations, firms and institutions can still benefit from the technology while employing centralized management systems (e.g., IT support). Furthermore, skepticism is warranted for bold claims about specific future events such as the need to reinvent the ledger-based wheel with a flavor of the month. For every project listed here there are two or three more that could have been surveyed and analyzed. As Carl Sagan once said, extraordinary claims require extraordinary evidence. And based on my interactions with the teams detailed above, I believe that many if not all of them are capable of achieving the milestones and goals they have set.

Community views on cryptocurrency's future are varied and heterogeneous; it seems likely that entry into constructive, and technical, dialogue with global policymakers is a necessary prerequisite of wider adoption for virtual currencies in some countries – but that is a topic for books others will inevitably write. While decentralized apps geared towards illicit markets may be popular and profitable with certain segments and niches, the key to mass adoption will likely be providing real value by addressing real needs (e.g., why would your mother want to use it; why would a bank use it; how do we empower the unbanked?).

Each of these platforms, even the 1.0 generation, has the potential to provide a trustless storage and transportation mechanism for asset management. Yet, despite the hype and promise, it remains nonetheless entirely plausible that the technology may not meet the expectations of its most zealous advocates, and the only decentralized app that is still popular a decade from now is still relegated to the world of peer-to-peer torrents. It is my view that cryptoledgers have the potential to make smart contracts, smart property and trustless asset management a reality for all.

Exciting days lie ahead in the unfolding “mathematical industrial revolution.”

And you can be a part of it.

About the author

Tim Swanson is a graduate of Texas A&M University and worked in East Asia for more than six years. He is the author of Great Wall of Numbers: Business Opportunities & Challenges in China. He can be reached at: tswanson@gmail.com

Keep up to date with further information at: www.OfNumbers.com and Twitter: @ofnumbers

Endnotes

[1] Guanxi (关系) is a confluence of connections and relationships. While "knowing" the right person is always helpful in any country, the cultural and economic influence of guanxi is magnified in China. Even with the proper funding and proper forms, if you do not have guanxi with the right officials or bosses (*laoban*), your project may never get off the ground.

[2] Tim Swanson Talks About China, Bitcoin, And Smart Contracts from Newfination

[3] Can PayPal Beat Apple, Google, Amazon And Icahn In The Wallet Wars? from *Forbes*

[4] Contracts in legal terminology are required to have 'offer,' 'acceptance' and 'mutual acceptance' – this is called 'meeting of the minds.' Whether the 'smart contracts 'used in cryptoledgers will be recognized or stand legal scrutiny is an on-going area of discussion and speculation.

[5] The task of trying to encode all the possible legal subtleties that underlie even the most basic contract could potentially be difficult from a designing perspective and will likely run into hurdles with mainstream commerce.

[6] While several state legislatures (California, Washington) recognize cryptocurrencies as alternative currencies and it may technically be used as a 'currency' in the economic sense, as of this writing, no United States court has categorized 'bitcoin' as a currency yet; rather in legal terminology it could be treated like a commodity. Furthermore, in the United States it is currently not categorized as a stock or bond or an investment contract (a security). These issues are being debated by policy makers and it may be some time before a consensus builds within each jurisdiction. One source I spoke with used the analogy that trying to pigeon-hole cryptocurrencies under existing laws is equivalent to how regulators at the turn of the 20th century applied cruiseline laws to the nascent airline industry. Similarly, it took a decade to build up regulatory framework surrounding credit cards – which are essentially, preapproved electronic loans (e.g., a line of credit). Perhaps a 'BitLicense' will become integrated with the New York Uniform Commercial Code Article 4-A: Funds Transfers. See New York considers creating a 'BitLicense' for Bitcoin businesses from *The Verge*

[7] All assets have at least one form of 'moneyness' including: medium of exchange, store of value or unit of account. The question over whether or not a virtual asset can have all three is an ongoing debate. See Bitcoin now 'unit of account' in Germany from *The Guardian*, Bitcoin More Speculative Than Real Currency, Study Finds from *Bloomberg*, Economics of Bitcoin: Is Bitcoin an Alternative to Fiat Currencies and Gold? by Peter Šurda as well as the writings of JP Koning

[8] Stylistically many other writers use hyphenated words (e.g., crypto-currency, crypto-ledger). I use a hyphenless style throughout strictly for aesthetic purposes.

[9] There are multiple different ways to describe a Decentralized Autonomous Organization. Some call it an Agency, an Application, a Corporation or even Consensus. A thorough explanation can be found in "Application Specific, Autonomous, Self Boot-Strapping Consensus Platforms (And the DACs that live on them)" forthcoming by Adam Levine.

[10] There is also no standard, consistent definition for what a DAO is and is not. Mike Hearn describes it differently than Vitalik Buterin (see chapter 3). Perhaps, speculatively, as time goes on, developers can build more complicated features creating more robust functionality beyond that of what a contract can execute.

[11] The 8 identities of Bitcoin by William Mouyagar

[12] Nick Szabo's Essays, Papers, and Concise Tutorials

[13] Economics of Bitcoin: Is Bitcoin an Alternative to Fiat Currencies and Gold? by Peter Šurda and The Economics Of Bitcoin – Challenging Mises' Regression Theorem by Michael Suede

[14] The Bitcoin Central Bank's Perfect Monetary Policy by Pierre Rochard

[15] Cryptocurrency gets real by Preston Byrne

[16] One reviewer of this manuscript sees symbolic parallels with the works of Jean Baudrillard, a French philosopher, with respect to those who value and view cryptocurrencies as a sign rather than a repository.

[17] For hundreds of years humans have used paper as an abstraction layer to describe, secure and exchange assets. Many securities like shares of stocks and bonds are electronically traded globally. But they use a trusted party framework requiring many middle men to provide auditing, approval and authentication.

[18] See Namecoin and What are Namecoins and .bit domains? from *CoinDesk*

[19] Merged mining

[20] After attempts to modify Namecoin it became clear that a more elegant, native solution for asset tracking was needed in order for one blockchain to manage different "colors" or contracts.
[21] I pronounce dogecoin, dogecoin. See How Do You Pronounce "Doge"? from *Slate*
[22] While nearly anyone with internet access and a bank account can currently purchase bitcoins for almost any amount of fiat, the psychological factor of receiving numerically large amounts of tokens as you mine (or hash) a block is evidently a self-rewarding mechanism. And for new, inexperienced users, this entry point often serves as a jump off node into the Bitcoin ecosystem afterwards. Thus if the goal for Bitcoin adopters and cryptoledger developers is to attract (e.g., marketing) and get more people interested in crypto-based services and solutions, then the community as a whole should be enthused that more people are joining the community through these new conduits. Perhaps some users will get disenchanted if and when a memecoin like doge fails to live up to expectations (e.g., "to the moon") but it is their subjective preferences and valuation of utility that determine market adoption, not by "rational" planners in any community.
[23] Litecoin was invented and released by Charlie Lee on October 13, 2011. Charlie has since left Google and is now at CoinBase. See Ex-Googler Gives the World a Better Bitcoin from *Wired* as well as Charlie Lee's Litecoin presentation at BTC Miami Conference (video) (slides). Dogecoin is essentially a Scrypt-based Litecoin clone released by Jackson Palmer in December 2013 based off the Doge internet meme. While there are now hundreds of altcoins some of the other "first" were IXCoin, IOcoin created by Thomas Nasakioto (anagram of Satoshi Nakamoto), SolidCoin/SolidCoin 2 and GeistGeld which had 15 second blocks. The experiment with GeistGeld shows that if blocks are generated too fast miners do not have a chance to catch up and end up working on "orphans" that have already been mined.
[24] They Never Said It: A Book of Fake Quotes, Misquotes, and Misleading Attributions by Paul Boller and John George
[25] Wet code and dry by Nick Szabo
[26] Arbitration Scorecard 2013
[27] Fulbright's 9th Annual Litigation Trends Survey Report and Fulbright's 9th Annual Litigation Trends Survey: Litigation Bounces Back; Regulation Hits High - U.S. Release
[28] In June 2010, Paul Ceglia sued Mark Zuckerberg (creator of Facebook) claiming that a 2003 contract entitles him to an ownership of most of Facebook. In March 2013 a judge recommended dismissal of the lawsuit as the contract was a "recently created fabrication." See Facebook Lawyer `Unsure' Whether Founder Mark Zuckerberg Signed Contract from Bloomberg and Judge recommends dismissal of Paul Ceglia's Facebook lawsuit from *c|net*
[29] A type of securities exchange existed during the Roman Empire, societates publicanorum, which were organizations of contractors and leaseholders who performed services for the government.
[30] The term smart contract is sometimes used as a bit of a misnomer, because it likely undersells the capabilities of a DAO. An 'active contract' or 'live contract' explains that the contract itself is the mechanism that monitors and actively controls the prior agreement per the terms. See also: WorkingWithContracts from bitcoinj
[31] According to Mark Miller the first smart contracting system was AMIX, the American Information Exchange.
[32] More concisely, smart contracts are about reducing default (e.g., counterparty risk). The standard historical view has been that the state was necessary to enforce contracts (forward contracts as opposed to spot contracts). However, Anthony de Jasay's contends that Rousseau is misunderstood regarding the "public goods problem." The common view is that the optimal strategy is for both parties to default and that this somehow proved the existence of market-based contract failure. Yet as de Jasay contends, the proponent of such a few employs a form of hedonic calculus in order to quantify the "incremental pleasure he expects to derive from having the state arrange the production of the correct amount of order and other public goods, instead of relying on a possibly quite inadequate patchwork of spontaneous arrangements, must outweigh the pain of coercion he thinks he will suffer at the state's hands." See Inventing the State: The Social Contract by Anthony de Jasay
[33] It has been called a platform, scaffold, foundation and a number of other nouns. See Bitcoin: It's the platform, not the currency, stupid! by Sander Duivestein and Patrick Savalle and Bitcoin 2.0 Explained: Colored Coins Vs Mastercoin Vs Open Transactions Vs Protoshares by Kyle Torpey
[34] While smart contracts can technically self-execute, whether or not policy makers allows or recognizes them is another matter entirely.
[35] Smart Contracts by Nick Szabo

[36] This issue can involve entire papers and books in terms Subjective Theory of Value and preferences. See Economics of Bitcoin: Is Bitcoin an Alternative to Fiat Currencies and Gold? by Peter Šurda and The Economics Of Bitcoin – Challenging Mises' Regression Theorem by Michael Suede

[37] Wet code and dry by Nick Szabo

[38] See Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto. Bitcoin also solves a long-standing mathematical thought experiment called the Byzantine General's Problem which involves how independent parties (and strangers) can arrive at consensus as noted by Paul Bohm:

> The Byzantine Generals' Problem roughly goes as follows: N Generals have their armies camped outside a city they want to invade. They know their numbers are strong enough that if at least 1/2 of them attack at the same time they'll be victorious. But if they don't coordinate the time of attack, they'll be spread too thin and all die. They also suspect that some of the Generals might be disloyal and send fake messages. Since they can only communicate by messenger, they have no means to verify the authenticity of a message. How can such a large group reach consensus on the time of attack without trust or a central authority, especially when faced with adversaries intent on confusing them?
>
> Bitcoin's solution is this: All of the Generals start working on a mathematical problem that statistically should take 10 minutes to solve if all of them worked on it. Once one of them finds the solution, she broadcasts that solution to all the other Generals. Everyone then proceeds to extending that solution - which again should take another ten minutes. Every General always starts working on extending the longest solution he's seen. After a solution has been extended 12 times, every General can be certain that no attacker controlling less than half the computational resources could have created another chain of similar length. The existence of the 12-block chain is proof that a majority of them has participated in its creation. We call this a proof-of-work scheme.
>
> If that sounds confusing, don't worry. What it means is just that consensus is reached, because computational resources are scarce. You vote with work. To rig the vote an attacker would need to control more computational power than the honest nodes. To ensure it's more expensive for an attacker to purchase the computational power needed to attack the system, Bitcoin adds an incentive scheme. Users who contribute computational power get rewarded for their work. If the value of a Bitcoin rises and thus attacking the system becomes more profitable, it also becomes more profitable for honest users to add computational resources. At any given point, one would expect miners to invest as much resources into mining as is profitable for them. Bitcoin is a currency, because it needs incentives to protect the consensus process from attackers. This computational process ("mining") is not wasteful at all, but an incredibly efficient way to make attacks economically unprofitable. Bitcoin never uses more computational resources than neccessary to protect the integrity of its interactions.

[39] What Is Seigniorage? by David Kestenbaum

[40] Core Development Update #5 by Gavin Andresen

[41] An example is BTProof

[42] See How do bitcoin transactions work? from *CoinDesk* and How the Bitcoin protocol actually works by Michael Nielsen

[43] There is arguably actually a third key as well, a hash of the public key. See Bitcoins the hard way: Using the raw Bitcoin protocol by Ken Shirriff

[44] Cryptographers at GCHQ, the British intelligence agency had independently invented and used the public-private key Diffie-Hellman technique several years prior to 1976. As a result of this and other mathematical schemas, the entire global financial industry, every diplomatic corps, cloud services and all e-commerce (to name a few) currently rely on cryptographic methods to securely transmit data.

[45] Elliptic curve cryptography was first introduced by Victor Miller and Neal Koblitz in 1985. While Diffie-Hellman can be used for public key encryption, not many people actually use it that way. Also, Diffie-Hellman cannot do digital signatures which is what Bitcoin uses public key encryption for. Furthermore, Bitcoin uses parameters set by secp256k1 (not the exploitable secp256r1). See NSA Backdoors and Bitcoin by Chris Pacia, The Cryptography of Bitcoin by Edward Yang, An Overview of Elliptic Curve Cryptography by Julio López and Ricardo Dahab, ECDSA from

StackExchange, Why can't Diffie-Hellman be used for signing? from StackExchange and Cryptography and Contracts by Daniel Krawisz.

[46] A Merkle tree is used to "store" the large transaction history (at the time of this writing, the blockchain is roughly 14 gigabytes and growing). Technically transactions are not actually "stored" in a hash tree per se, but rather the proof-of-work that says a block is valid is based on hashing the Merkle tree input of all the transactions.

[47] Bitcoin uses a modified version of Hashcash which was originally proposed in March 1997 by Adam Back; the actual cryptographic hash function is SHA256d. It should also be noted that he recently voiced some vulnerability concerns regarding implementing a Turing-complete language with a cryptoledger, see Turing complete language vs non-Turing complete (Ethereum vs Bitcoin).

[48] Or in short, mining as done today has very simple requirements: hard to produce results, yet easy to verify and relatively hard to hardware optimize. This last aspect has changed with the advent of ASICs, yet due to competition there is an "arms race" between semiconductor designers. See The Bitcoin-Mining Arms Race Heats Up from *Bloomberg Businessweek*

[49] Washing virtual money from *The Economist*

[50] There are actually four groups that ultimately provide "consensus": miners, holders of tokens (anyone with a wallet), merchants and web-based services such as exchanges. While miners are usually considered the most powerful (because without them, there would be no network, ledger or authentication) each of these other groups hold some sway. Without exchanges, many participants would be unable to trade bitcoin for fiat or other alt tokens. Without merchants, many participants would be unable to trade bitcoin for goods and services. There is also room to distinguish a "hasher" and a "miner." In the long-term "hashers" may end up causing centralization of network resources into central pools that diminishes the ability for the network to stave off outward attacks. Most "miners" today lack power to select or validate bitcoin transactions. Modern miners simply sell a computing service (hashing) to the mining pools. Decentralized pools like P2Pool would help alleviate some of that concern yet there are financial incentives for "hashers" to use larger pools that create imbalances that are discussed in Hashers are not miners, and Bitcoin network doesn't need them. See also Block chain entry and Selfish Mining: A 25% Attack Against the Bitcoin Network from *Bitcoin Magazine*. The Ethereum project plans to use functional data structures and the trees are called "uncles." See Grokking Functional Data Structures by Debasish Ghosh

[51] Operating a node is not the same thing as mining, running a full node ensures the integrity of the network. Full nodes keep a copy of the entire blockchain. Pool miners do not operate as nodes as they communicate with the pool owner which does operate as a full node. See Bitter to Better -- How to Make Bitcoin a Better Currency by Barber *et. al.* and What can an attacker with 51% of hash power do? from StackExchange

[52] One of the best explanations of how hashing works can be found in: Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics by Chris Pacia

[53] See Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics by Chris Pacia and The Marginal Cost of Cryptocurrency by Robert Sams

[54] This effectively means that there could be billions of contracts, not just 21 million.

[55] The pictures used on television news stories of a silver or golden 'bitcoin' are usually a Casascius coin. The company that made them (Casascius) shutdown in 2013. These were physical coins (or rather 'containers') plated in either silver or gold and a 'private key' to a bitcoin address was embedded on a card within it. In a sense, this was a type of physical wallet that was intentionally made cosmetically similar to a traditional coin.

[56] An air-gapped computer is one that is physically isolated from an insecure network. This is done to protect trade secrets and prevent potential abuse such as hacking or espionage. To prevent this kind of theft, there are off-site, cold-storage techniques involving using a paper-wallet to store bitcoins. Blockchain.info created a guide that explains how to do that: Practical Paper Wallets. In a different industry, in March 2012, *Businessweek* published a widely circulated report (China Corporate Espionage Boom Knocks Wind Out of U.S. Companies) about corporate espionage of a US wind turbine supplier (AMSC) conducted by its Chinese client, Sinovel. In short, while AMSC attempted to isolate its trade secrets and proprietary software code outside of China (using an 'air gapped' facility), Sinovel still managed to use social engineering (e.g., bribery) to lure one of AMSC's key Austrian-based programmers to China. An 'air gapped' facility in their case meant the proprietary code – "secret sauce" – was only accessible at a workstation that was not connected to the internet. Using the 'defense in depth' IT security strategy (e.g., multiple firewalls and secure zones nested within one another) AMSC purposefully built this facility

with the sole intention of building a physically isolated silo that could not be easily compromised. See also, FAA: Boeing's New 787 May Be Vulnerable to Hacker Attack from *Wired*

[57] I would like to thank Stephan Kinsella for articulating this particular thought experiment.

[58] According to Black's Law Dictionary entry for, "possession is nine-tenths of the law":
This adage is not to be taken as true to the full extent, so as to mean that the person in possession can only be ousted by one whose title is nine times better than his, but it places in a strong light the legal truth that every claimant must succeed by the strength of his own title, and not by the weakness of his antagonist's.

[59] Coinbase is technically not an exchange. It is an online wallet that purchases tokens through other exchanges like BitStamp.

[60] Approximately 26 million litecoin's have been mined creating a market cap of about $500 million as of this writing. In addition, some people forget their passwords or forget to back-up their digital wallet when discarding older computers which permanently makes those tokens unspendable. See Missing: hard drive containing Bitcoins worth £4m in Newport landfill site from *The Guardian*

[61] Depending on what kind of wallet or service you use, the time between sending and receiving a bitcoin could range from a few seconds to 10 minutes. Each transaction and confirmation requires about 10 minutes to be processed by the network. If you use a 0-confirmation method (e.g., Electrum), this time is cut down to seconds (although there is a security risk); see, How secure is zero confirmations? from StackExchange.

[62] This Pizza Cost $750,000 from *Motherboard*

[63] This asset tracking is not the same a referential datapoint such as the annual Big Mac Index compiled by *The Economist*

[64] Grass Hill Alpacas was one of the first companies to sell its wares for bitcoin. CoinDL is another long-standing company in the digital goods-for-bitcoin space. Both of these were mentioned in an interesting interview between Pieter Wuille and Stefan Thomas several years ago.

[65] Smart property implies that there is some issuer, and Bitcoin has no issuer. Bitcoin is a fiat medium-of-exchange by design, that aspect is not an organic evolution.

[66] While there may be technical and social hurdles with their endeavor, it is a very unique spin of alts, see: Humint Hopes to Custom-Build Altcoins for Brands from *CoinDesk*

[67] See Coingen and Razorcoin. While some altcoins were originally intended to be part of some kind of "get rich quick" pump-and-dump scheme, this is not to say that they are forever useless or without utility. Value is subjective and determined by individual market participants and their preferences. As observers, we cannot know *a priori* what market participants will ultimately use the token ultimately for. Obviously enormous inertia is behind Bitcoin but we do not know what risks and market conditions necessarily lay ahead decades from now and how those unknowns may impact the crypto ecosystem.

[68] One reviewer of this manuscript suggested that there are even more similarities between the spontaneous, emergent order of Bitcoin and the vision of Visa as laid out by Dee Hock. Hock described the success of Visa's distributed payment processing network as "chaordic," a blend of "chaos" (e.g., competition between member banks for merchants) and "order (cooperation between the banks in honoring the transactions across borders and currencies). See Birth of the Chaordic Age from Dee Hock, The Trillion-Dollar Vision of Dee Hock from *Fast Company*, The Bitcoin Blasphemy by Joe Nocera and Hayek's Liberalism and Its Origins by Christina Petsoulas

[69] Creative destruction is an economic term originally coined by Karl Marx and later popularized by Joseph Schumpeter. Its original usage has changed and is currently used to illustrate how market forces purge and reallocate capital towards other more productive uses. See Creative Destruction by W. Michael Cox and Richard Alm

[70] On BlackBerry 10's 1st anniversary, BlackBerry's U.S. market share hits 0% from BGR

[71] For the technical specifications see the genesis block. Note: Satoshi signed the block with the statement "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" – which is based on a real article from *The Times*, Chancellor Alistair Darling on brink of second bailout for banks.

[72] Blockchain address: http://blockchain.info/address/1EXoDusjGwvnjZUyKkxZ4UHEf77z6A5S4P

[73] All mastercoins (MSC) were minted during a fundraiser for the month of August 2013

[74] Backed by $5 Million in Funding (4,700 BTC), Mastercoin Is Building a Flexible, New Layer of Money on Bitcoin from *MarketWired*

[75] Since the genesis block people have included text, images and even files in the blockchain. See Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software by Ken Shirriff.
[76] Bitcoin Core Development Falling Behind, Warns BitcoinJ's Mike Hearn from *CoinDesk*
[77] Almost Half a Billion Worth of Bitcoins Vanish from *The Wall Street Journal*
[78] The private provision of public goods via dominant assurance contracts by Alexander Tabarrok
[79] Citizinvestor, ZenFunder, neighbor.ly
[80] KinsellaLaw
[81] One of the intentions of the smart contract system is to recreate the banking system. Even if it worked, it could take many years to move beyond the current financial realm.
[82] One common question people ask is how does fiat get into and out of a decentralized exchange (DEX)? More than likely, at first there will be fiat pointers which are a non-redeemable token used to represent an asset marked for redemption. For instance, with respect to mastercoins, reputation markets will develop as those who have to honor turning a mastercoin asset into fiat currency on demand. Thus, in the long-term a DEX offsets the current centralization, yet the trust problem still exists on the edges; fiat will likely always need a 3rd party provider since it is provided by a 3rd party already. In addition, one source explained that centralized exchanges will likely not disappear as users cannot connect to the Caribbean islands with a decentralized approach, or in their words, "Foreign exchange controls will prohibit the decentralized open nature and land people in hot water. Centralized, regulated exchanges allow users to fly above the law."
[83] Argentina's Economic Crisis: Causes and Cures from Joint Economic Committee, United States Congress
[84] Simpson on Sunday: Argentinians summon up the ghost of Peron in hard times from *The Telegraph*
[85] Argentina Unraveling from *The New York Times* and Accommodating an army of garbage pickers from *CNN*
[86] Argentina to Nationalize Pension Funds from *The Washington Post*
[87] BitPagos
[88] Argentine Social Money Movement by Sergio Lub and Thomas Greco and Los clubes del trueque en la Argentina, una experiencia útil de secesión económica by Jorge Aldao
[89] One likely problem may then be online theft instead – it is much easier for a hacker to get your virtual assets than fly over there and steal your physical notes.
[90] Argentina to Replace Bogus Inflation Index to Mend IMF Ties from *Bloomberg*
[91] Bitcoins in Argentina: A New Safe Haven? from *The Argentina Independent*
[92] The Big Mac index from *The Economist*
[93] For more on Title-transfer theory of contract see A Libertarian Theory of Contract: Title Transfer, Binding Promises and Inalienability by Stephan Kinsella
[94] Public spending and pay by Crawford, Cribb and Sibieta, p. 165
[95] In One Month, Everyone In Iceland Will Own Cryptocurrency from *Motherboard*
[96] Mazacoin Aims to be Sovereign Altcoin for Native Americans from *CoinDesk*
[97] Formalizing and Securing Relationships on Public Networks by Nick Szabo
[98] Learning by Transduction by Gammerman *et. al.*
[99] Formalizing and Securing Relationships on Public Networks by Nick Szabo
[100] Hopkins doctor suspended after charges in Silk Road case from *The Baltimore Sun*
[101] CoinLab's Incubated Startup, Alydian, Files For Bankruptcy from *TechCrunch*
[102] Numerous proposals have been submitted by core developers to improve the functionality; one common analogy used is that Bitcoin core development right now is trying to upgrade the original Wright Flyer to a Boeing 787 without landing. While many advocates want Bitcoin to be an answer to all payment problems, these limitations likely impair it beyond the role of store of value and remittances. See chapter 6 for more on remittances and chapter 8 for payment processing details. See also Hardfork Wishlist
[103] Bitcoin Core Development Falling Behind, Warns BitcoinJ's Mike Hearn from *CoinDesk*
[104] See The Bitcoin malleability attack graphed hour by hour by Ken Shirriff and Ripple Labs Chief Cryptographer David Schwartz Talks About Malleability In Bitcoin from Newfination
[105] There are other projects currently under development such as eMunie or even released such as Freicoin.
[106] Colored Coins

[107] Chroma Wallet
[108] Losing the private key to a smart contract (or Colored Coin in this example) could be problematic. Currently bitcoins are still being lost and stolen despite awareness of web-based wallet vulnerabilities. If security does not improve, growth might be difficult for smart assets.
[109] eToro
[110] Counterparty.co
[111] See Reality Keys: Bitcoin's Third-Party Guarantor for Contracts and Deals from *CoinDesk* and a slightly different idea but in a similar segment, RealityShares
[112] BitcoinBusiness
[113] The Mastercoin protocol supports the OP_Return function. One way the user-defined assets are tracked in the Bitcoin blockchain is by sending a certain amount of satoshis (5430), just above the dust limit. Note however, that the dust limit was originally announced at 5430 but was subsequently discovered to be 5460 which may impact some mastercoin transactions. See Dust limit defined as 5460 satoshi instead of 5430 in Bitcoin core at github
[114] How is this functionality achieved? There is not any 'syncing'. Nothing is every 'synced' with any blockchain. Mastercoin does not use 'OP_RETURN,' though it plans to add support for it eventually. Counterparty supports `OP_RETURN` now, but it cannot really be used until Bitcoind 0.9 comes out. Both Counterparty and Mastercoin support using multi-signature transactions to store data in the Bitcoin blockchain. Just to clarify one misconception, there is no such thing as the '0.9 protocol' -- there is a 0.9 Bitcoind. Also, Bitcoind uses LevelDB and Counterpartyd uses SQLite3.
[115] $1 Million-Plus in Prizes, Contracts at Texas Bitcoin Conference Hackathon from *MarketWired*
[116] BitAngels
[117] See NXT :: descendant of Bitcoin from Bitcointalk and What is NXT?
[118] There's a £60m Bitcoin heist going down right now, and you can watch in real-time from *NewStateman*
[119] There are ways that peers could be compromised vis-à-vis Sybil attacks. See Establishing the Trustworthiness of Nodes without External Tokens (eg Passports) and Selfish Mining: A 25% Attack Against the Bitcoin Network by Vitalik Buterin
[120] Personal correspondence, Nextcoin.org
[121] NXT – Proof of Stake and the New Alternative Altcoin by Adam Hofman
[122] The potential for such an occurrence is being argued in academic literature; see It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency by Houy Nicolas. A state agent, under the direction of a central bank and simultaneously uninterested in seeing their assets appreciate in value could conduct such an attack. Otherwise it would likely be cost prohibitive for nearly any other value investor. In addition, Nicolas' argument is problematic in that it requires sufficient liquidity, that is to say even if the state actor would be willing and able to spend any amount of funds to acquire the tokens, he or she would still need to induce liquidity to participants holding 90% of the tokens.
[123] Personal correspondence, February 25, 2014. See also Interview with Graviton, Nextcoin.org Community Founder from *Cryptocoinsnews*
[124] Satoshi Nakamoto recognized this shortcoming but deliberately chose to use Script to mitigate potential abuses (e.g., infinite loops freezing the blockchain). One reviewer of this manuscript mentioned that developers should also realize that hypothetical constructs like a DAO essentially involve coding organizational law into programs. While this may sound easy, law was built to enable release valves of forgiving judgment. Code is not forgiving. Thus if something happens in the real world, even the simplest unforeseen effect could derail an otherwise streamlined exchange process.
[125] Bitcoin Magazine
[126] For an example of Ethereum sub-currency contracts see this video from Joel Dietz and Joris Bontje. See also Writing a Contract in LLL by Gav Wood
[127] I have a friend who used the following method to generate bitcoin addresses and store the keys: 1) in offline mode store the private/public key pairs on USB sticks with Truecrypt partitions, with paper as backup (encrypted and printed out). To a certain extent this mirrors what Coinbase does. 2) To reduce the chance of vendor back-doors, each of these drives should be different brands bought from different locations. 3) To generate the actual keys you have to deal with the issue of true randomness, plus not leaving any reproducible trace (e.g., logic stored

in cache or writing on carbon-copies) thus an individual could buy a dozen non-loaded dice and use this to generate private keys. 4) For users who might be suspicious of the entropy coming from the Linux random number generator (RNG) you could randomly mash the keyboard, turn on the webcam and simultaneously run commands and programs from the start menu to generate some additional entropy. 5) Then use an air-gapped laptop with a freshly boot distribution of Linux. Here in particular you have to be careful as you would need to only use an in-memory distribution (e.g., boot from thumbdrive), because a user does not want the private keys cached anywhere at all on disk. 6) In addition a user would also want a distribution which will work with a standard USB printer for printing purposes because you never want the private keys to go over the wire.

[128] See Scalability and Thin Client

[129] Vitalik Buterin has recently written several more article detailing what he thinks DAOs can and cannot do, see: DAOs Are Not Scary, Part 1: Self-Enforcing Contracts And Factum Law and DAOs Are Not Scary, Part 2: Reducing Barriers

[130] See Mike Hearn, Bitcoin Developer – Turing Festival 2013 video

[131] Intel SGX for Dummies (Intel® SGX Design Objectives) from Intel

[132] Invictus Innovations is leading the development of BitShares; whitepaper

[133] CNRS is part of Groupe d'Analyse et de Théorie Economique. See The economics of Bitcoin transaction fees by Nicolas Houy

[134] Zanbato

[135] While a completed technical white-paper has not been released, the development team has published The Counterparty Protocol

[136] They had successfully released 'callable assets,' stating that, "Assets are now callable, if they are set to be so upon first issuance. An asset may be able to be 'called back' by its issuer at a fixed price from a particular date." See Counterparty Protocol, Client and Coin (built on Bitcoin) – Official from Bitcointalk

[137] Personal correspondence, February 4, 2014 via Bitcointalk

[138] This terminator address is based on Vanitygen. Based on known computational technology it would purportedly take 93,215,140,000,000,000,000,000,000,000 years to generate the private key to 1CounterpartyXXXXXXXXXXXXXXXUWLpVr with an i5 processor. For critics who claim that the Bitcoin network is insecure, they could prove their skepticism by trying to generate the private key to that address. See also Wallet security: why only 128 bit for secret seed? from Ripple

[139] See I burned BTC through blockchain.info, how do I access my XCP? from Counterparty.co and the exact address was 1CounterpartyXXXXXXXXXXXXXXXUWLpVr. On the first day a user would receive 1500 XCP for 1 BTC. By the end of the fundraiser, it was 1000 XCP for 1 BTC. Ultimately 2,648,756 XCP were created in total.

[140] See Paul Bohm's detailed explanation of this mathematical problem.

[141] Personal correspondence, January 29, 2014

[142] See Bitmessage and Bitmessage Sends Secure, Encrypted, P2P Instant Messages from *Lifehacker*

[143] See Twister and Out in the Open: An NSA-Proof Twitter, Built With Code From Bitcoin and BitTorrent from *Wired*

[144] Maidsafe, SyncNet, Bitcloud and Bitcloud developers plan to decentralise internet from *BBC*

[145] Monetas and Open-Transactions

[146] While the XRP are centrally issued, the gateways are distributed. The process for being a gateway for a 'coin' generally works as follows: 1) announce you are issuing a coin, 2) anyone can "trust" you for the coin, 3) accept the real coin, 4) make a Ripple payment for the coin. Thus you can create fully backed precious metals on the Ripple network. Ripple itself does not send USD, EUR, CAD or other currencies. It actually sends IOU's for these currencies which must be redeemed by specific issuers who are acting as "gateways" into and out of the legacy banking system.

[147] One way to audit and verify if a 3rd party gateway (and exchanges in general) is not running a fractional scheme is to implement a 'proof of reserves' process Greg Maxwell recently proposed. Another option that could happen is that exchanges may hire independent auditors in order to become covered by insurance; these audits could then be posted. An unnamed insurance company purportedly provides services to one Bitcoin vault called Elliptic, which protects against a failure in a business' storage methods, with customers opting for a "liability limit" for how much they want covered. Another idea being discussed is some sort of FDIC-like insurance. A company in beta

called Inscrypto, which is located in Boston, claims it will be a "privately funded, decentralized version of the FDIC," to help you "reduce or completely eliminate the risks of owning bitcoin." It is likely that following the Mt. Gox bankruptcy, many exchanges will seek such independent measures and likely have an incentive to do so (e.g., satiate consumer demand, provide transparency as a precursor to being acquired in the future). See also Proving Your Bitcoin Reserves by Zak Wilcox, Bitcoiners Demand Greater Transparency in Exchanges from *Cryptocoinsnews*, Audit Report: Transparency and Accountability from Coinkite, After the Mt. Gox fiasco, calls for regulating bitcoin from *Pandodaily* and Will Bitcoin's Libertarians Pay for Private Deposit Insurance? from *BloombergBusinessweek*

[148] Introducing Ripple by Vitalik Buterin

[149] See Making Money from *Technology Review* and Ripple Charts

[150] Ripple credits

[151] Chris Dixon of Andreessen Horowitz was one of the first persons to use that term. Naval Ravikant founder of AngelList popularized the term "programmable money" which has a similar meaning. See Real money starts to pour into math-based currencies like bitcoin from *Quartz* and Inside Bitcoin, The Programmable Currency For Our Digital Future from *TechCrunch*

[152] A successful double-spend attack could be conducted against a proof-of-work-based algorithm if 51% of the hashrate is controlled by a malicious agent; and a similar attack is theoretically able to successfully take over a proof-of-stake if 90% of the token is controlled by one agent. But there are many ways to recover from it (e.g., hardforks) and this topic has filled countless volumes already. Yet, for an objective view on this matter of network attacks, I asked Nick Szabo (Personal correspondence, January 25, 2014), who had some original insights about how to prevent and mitigate this issue:

> One contingency is to have a bunch of different cryptocurrencies around […] and if one gets successfully attacked users switch to another. We already have enough cryptocurrencies around for this purpose, but this doesn't help the people holding Bitcoin or who've made other Bitcoin-specific investments. And there are substantial costs in switching to a new cryptocurrency, and such a crisis might persuade many merchants to give up on cryptocurrencies generally rather than switch.
>
> A practical means of disaster preparedness is for a number of independent engineers and auditors to keep copies of the block chain, as up-to-date as possible, even if they aren't participating as a miner or mining pool. Just the fact that a few good engineers have up-to-date copies of the block chain should be enough to dissuade most 51% attacks. 51% is enough to persuade the cryptocurrency algorithms to believe a lie, but it's not enough to persuade engineers (or auditors with suitable tools) who manually inspect the block chain, if the payor or payee who've been blocked or defrauded resend the original payment instructions directly to those engineers. Of course we don't want to rely on such a manual process in the normal course of business, just for dire contingencies.
>
> In the event of a 51% attack there is a fork in the block chain, and the job of these engineers or auditors would then be to persuade users to use the minority but correct block chain and exclude the incorrect majority. It would be expensive but doable. Not something you want to normally see happen.
>
> Another way to put it is if there is a 51% attack we have to fall back on methods of ensuring integrity that, like the traditional financial system, are manual and expensive, and the big cost savings from the automated security are temporarily lost. You might call this [ad hoc solution] "proof by engineer," which would be replacing proof-of-work in the temporary emergency for the purposes of the transactions being disputed in the block chain fork.

[153] CrossCoin Ventures

[154] The way the current system is setup, remittances and funds sent abroad go through multiple institutions via 'correspondent accounts' or 'correspondent banking.'

[155] Ripple Developer Conference 2013: Future Focus of Our Engineering Team presentation by Stefan Thomas

[156] Peer-Assisted Key Derivation Function (PAKDF) by Stefan Thomas

[157] See What is Homomorphic Encryption, and Why Should I Care? by Craig Stuntz, Blind Signatures for Untraceable Payments by David Chaum and Untraceable electronic mail, return addresses, and digital pseudonyms by David Chaum

[158] Blind Signature Scheme by Asanka Balasooriya and Kelum Senanayake

[159] I designed it with Creately; the image is released under Creative Commons 4.0 Attribution license.

[160] A Turing-complete solution proposed by NXT is to use the Automated Transaction Specification

[161] Another category that was not highlighted is the proof-of-work algorithms: both Bitcoin and Namecoin are SHA256d based and Litecoin and Dogecoin use Scrypt.

[162] Personal correspondence, January 24, 2014

[163] The Euronext merger with the NYSE was completed on April 4, 2007. In turn, Intercontinental Exchange completed the acquisition of NYSE Euronext on November 13, 2013.

[164] Proplets -- Devices for Controlling Property by Nick Szabo

[165] That 'Internet of Things' Thing by Kevin Ashton and Open Source Solution for the Internet of Things into the Cloud

[166] See Your Door Is About to Get Clever: 5 Smart Locks Compared from *Wired*, Smart Refrigerator from *Mashable*, Nest Thermostat, Nest Protect, LG Hom-Bot Square review from *C|net* and Spotlight on LIFX LED bulbs from *C|net*

[167] The 'Internet Of Things' Will Be Bigger Than The Smartphone, Tablet, And PC Markets Combined from *Business Insider*

[168] In one notable example used by Mike Hearn, he describes how a Bitcoin user could use the microtransaction capability of Bitcoin to open and close doors equipped with such devices. See his Bitcoin 2012 London video. The new OpenLibernet is a project that is trying to make this a reality, by fusing bitcoin microtransactions with decentralized mesh networking.

[169] Personal correspondence, January 24, 2014

[170] The Idea of Smart Contracts by Nick Szabo

[171] Ethereum Introduction from BTC Miami

[172] Personal correspondence, January 24, 2014

[173] On March 18, 2013, the Financial Crimes Enforcement Network (FinCEN) which is part of the US Department of Treasury issued guidance (pdf) related to Anti-Money Laundering Laws (AML) which specifically discussed virtual currencies such as Bitcoin. See History of Anti-Money Laundering Laws. For KYC and MSB see also, Understanding global KYC differences from PriceWaterhouseCoopers, FinCEN Brings KYC Requirements To Bitcoin? from *Bitcoin Money* and FinCEN Declares Bitcoin Miners, Investors Aren't Money Transmitters from *CoinDesk*

[174] Last year alone, nearly all Bitcoin-fiat exchanges were shut down due to legal reasons in the US. See Dwolla Account Seizure Reveals Mt Gox on Brink of US Indictment from *Contrarian Compliance*, Bitcoin Foundation Receives Cease And Desist Order From California from *Forbes*, Bitfloor: Largest U.S. Bitcoin Exchange Shuts Down from *Mashable*, OKPay suspends payment processing to all Bitcoin exchanges from *The Register*, Transferwise suspends operations from *TransferWise*, BitCoin Mining, Other Virtual Activity Taxable Under US Law from Slashdot and Fixing Bitcoin's shaky exchange infrastructure from *CoinDesk*

[175] Another question is: what happens if they are stolen? Does Alice, a hacker in Russia now own Bob's car? While there are ways to sign transaction by multiple parties before they get sent, it is still a long way to go for this, asset management system to become trusted and adopted by the average consumer.

[176] Each political jurisdiction is different. For example, in Israel the "DMV" (Misrad Harishui) serves to license drivers only. The tracking of vehicle related registrations happens at the post office (e.g., license plate's transfer with the vehicle, not the registrant. If Bob sells Alice his car, they would both go to the post office and make notice of the transfer of the ownership, and Alice would drive away with the existing plates).

[177] "Will the last miner please save a copy of the blockchain before leaving the room?"

[178] Again, a user would not need to purchase 1 BTC or 1 LTC, you could use a fraction of a token which is then used to represent and track the smart contract. The costs of obtaining this fractional token could be minimal.

[179] Much as standardized shipping containers (ISO intermodal container) have served as the backbone for global commerce over the past five decades, the potential for building light-weight but tamper-resistant packaging (e.g., polycarbonate, thermoplastic) coupled with embedded smart property features allowing near-real time tracking,

may enable cryptobarter to germinate. See The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger by Marc Levinson

[180] On the blockchain, nobody knows you're a fridge by Richard Brown

[181] In economic terms these are called "transaction costs." See The Nature of the Firm and The Problem of Social Cost by Ronald Coase and Transaction Costs by Douglas Allen.

[182] Formalizing and Securing Relationships on Public Networks by Nick Szabo

[183] Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb

[184] Kevin Mitnick is perhaps the most infamous example of the early 'hackers.' Mitnick was a hacker in the 1980s who used social engineering (e.g., manipulating secretaries to give him secure access) to compromise corporate networks such as DEC and Motorola. See The Art of Deception: Controlling the Human Element of Security by Kevin Mitnick and Takedown: The Pursuit and Capture of Kevin Mitnick by Tsutomu Shimomura

[185] For more about EDI see, Electronic Data Interchange (EDI): An Introduction by Roger Clarke

[186] Ingram Micro Buys Shipwire, The Cloud Logistics And Supply Chain Management Platform from *TechCrunch*

[187] Pacejet raises $4.5M to bring shipping to the cloud from *VentureBeat*

[188] Formalizing and Securing Relationships on Public Networks by Nick Szabo

[189] This is from Goethe's *Faust*. The actual quote is, "grey, dear friend, is all theory, and green the golden tree of life."

[190] See Mike Hearn, Bitcoin Developer – Turing Festival 2013 video and Bitcoin Developer Mike Hearn and Amex VP Michael Barrett Join Circle Team from *CoinDesk*

[191] There is a keyboard shortcut and browser extensions called a 'boss button' which quickly switches the screen to hide certain programs (like a computer game or video).

[192] Companies can receive analytics that provide reports on all file and network. Some examples of such software are Ultra VNC, eBlaster and Screenshot Monitor. See Are You Being Monitored At Work? by Becky Worley

[193] Teaming up with "check-in" providers such as FourSquare could be a method.

[194] Gregory Maxwell uses the term 'agent' in his StorJ proposal; see StorJ, and Bitcoin autonomous agents

[195] BitcoinStarter and CoinFunder are two current services in the crypto crowdfunding space.

[196] It is currently unclear what the arbitrary distinction between an "advanced" smart contract and a barebones DAO lies. Both use a blockchain to conduct and manage their organizational operations. Furthermore, to use the TCP/IP and SMTP analogy it is unclear at this time whether Bitcoin is merely one type of crypto app (like SMTP) or if it is more general purpose – a foundation – like TCP/IP is. The '2.0' projects in the broadest sense (like Mastercoin, Colored Coins, Invictus, Ethereum, etc.) are an attempt to create a more general platform more akin to TCP/IP that other services are built on top of.

[197] See BitPay, Coinbase and Bootstrapping A Decentralized Autonomous Corporation: Part I by Vitalik Buterin

[198] Bitcoin and the Three Laws of Robotics by Stan Larimer:

> Bitcoins can be viewed as a small "share" of the total market cap of the Bitcoin "corporation". The "mining" services that validate transactions and secure the network are paid for in new bitcoins that slowly dilute the "stock" as the corporation's market cap ebbs and flows. You can generally trade your shares for other currencies, goods, and services. Operating rules for the corporation cannot be changed unless a majority of stakeholders vote for them by switching to another version of the software. Interestingly, it is not the holders of existing shares that get to make this decision, but only those "employees" who are contributing their computer resources (mining bots) to run the company.
>
> Nothing says a corporation can't be structured to distribute voting rights this way, and that's exactly what Bitcoin has done. Shareholders get equity growth. Employees get voting rights. All "revenue" is paid to the employees as compensation for their work. There are no profits.

[199] An early concept of a larger voting-based system built on a DAO is the Bitcongress Foundation. Furthermore, David Johnston of the Mastercoin Foundation articulated this same software development centralization problem in a January 24, 2014 interview, episode 80 – Beyond Bitcoin Uncut from *Let's Talk Bitcoin*. See also DAC Index

[200] Vitalik Buterin labels it a prototype, stating:

> As *Let's Talk Bitcoin's* Daniel Larmier pointed out in his own exploration on this concept, in a sense Bitcoin itself can be thought of as a very early prototype of exactly such a thing. Bitcoin has 21 million shares, and

these shares are owned by what can be considered Bitcoin's shareholders. It has employees, and it has a protocol for paying them: 25 BTC to one random member of the workforce roughly every ten minutes. It even has its own marketing department, to a large extent made up of the shareholders themselves. However, it is also very limited. It knows almost nothing about the world except for the current time, it has no way of changing any aspect of its function aside from the difficulty, and it does not actually *do* anything per se; it simply exists, and leaves it up to the world to recognize it. The question is: can we do better?

[201] Richard Feynman first popularized this superficial hand-waving phrase 40-years ago through his memorable lecture, Cargo Cult Science. The name is derived from the actions of a South Pacific tribe located on the island of Tanna in Vanuatu. See In John They Trust from *Smithsonian*.

[202] See The Shareholder vs. Stakeholder Debate reconsidered by Rüdiger W. Waldkirch and How to Bureaucratize the Corporate World by Ben O'Neill

[203] See Sanitizing Bitcoin: This Company Wants To Track 'Clean' Bitcoin Accounts from *Forbes* and Coin Validation misunderstands fungibility and could destroy bitcoin by Adam Back. Technically Zerocoin was already in development months before the Coin Validation announcement; at the end of the year Dark Wallet held a successful crowdfunding campaign.

[204] While the miners could collectively fork and begin hashing a modified Bitcoin that integrated with Zerocoin, they have yet to do so for a variety of reasons, namely the $1 billion in capital investment (hardware) that would have to be written down because Zerocoin uses a new ledger and proof-of-work. See Anti-Theft Bitcoin Tracking Proposals Divide Bitcoin Community from *CoinDesk*, Bitcoin Anonymity Upgrade Zerocoin To Become An Independent Cryptocurrency from *Forbes* and Hopkins researchers are creating an alternative to Bitcoin from *The Baltimore Sun*

[205] Shared Coin was originally called CoinJoin, see this tweet from Blockchain.info. In addition there is a difference between on-chain (e.g., Blockchain.info) and off-chain wallets (CoinBase and Circle). See Roger Ver on Blockchain's Past, Present and Future from *CoinDesk*

[206] While the project is still in its early stages, the Ethereum blockchain will unlikely include the anonymity features of Zerocoin. Rather, there may be ways to create smart contracts and DAOs which can provide some level of anonymity (e.g., shell companies).

[207] While these decisions provoke strong opinions and feelings, forks are also a potential as well. Several "next generation" platforms may be compelling to some niches because of potential DAO functionality that could in turn use a contract or DAO to create 'holding firms' or even 'shell companies' (though obviously it is still on paper and has not been made). Yet, even if something like Ethereum worked as stated and the Bitcoin development team coded in significant protocol and proof-of-work (PoW) changes, it is unlikely you would get even a plurality of Bitcoin ASIC miners, let alone 90% to agree with moving to a new PoW algorithm because that would make their capital investments worth exactly zero (because a Bitcoin ASIC is tuned to one particular PoW, SHA256d). One recent estimate suggests that there is roughly $1 billion invested in existing hardware for mining globally including ASIC R&D. See The Bitcoin-Mining Arms Race Heats Up from *Bloomberg Businessweek*. Again, while "forking" comes up in conversations, ultimately the value is not necessarily the software code itself, but the infrastructure and mind-share behind it (the ecosystem).

[208] Adam Levine coined this acronym for descriptive purposes. Portions of his upcoming essay "Application Specific, Autonomous, Self Boot-Strapping Consensus Platforms (And the DACs that live on them)" are rephrased and reprinted with his permission.

[209] This term is used to describe anyone controlling more than a certain amount of tokens that interface with a DAC(P). The concepts of "exit" and "voice" were described in Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States by Albert Hirschman. These ideas have gained new prominence due in part to the decentralizing abilities and functions created by the software community. See Software Is Reorganizing the World and Silicon Valley's Ultimate Exit (slides) by Balaji Srinivasan

[210] See Why are m-of-n transactions not used today? from StackExchange, What are multi-signature transactions? from StackExchange, Bootstrapping A Decentralized Autonomous Corporation: Part I by Vitalik Buterin and the Ethereum whitepaper.

[211] This is called two-factor authentication (2FA) or two-man rule. See also Shamir's Secret Sharing.

[212] For a technical overview of how multisig works, I recommend watching a video explanation by Andreas Antonopolous (Taariq Lewis put together this slide deck of Andreas' notes).
[213] Bits of Proof and Bullion Bitcoin to Launch Gold-Bitcoin Exchange from *CoinDesk*
[214] Peercover
[215] The team is also involved in a new broadcast marketing initiative at OpenXRPTalk
[216] Personal correspondence, January 31, 2014
[217] Ripple is officially open-source!
[218] Compliance Program Design Presentation at First Virtual Currencies Compliance Conference in NYC by Juan Llanos
[219] See Accredited investor and the JOBS Act
[220] BIPS (Bitcoin Internet Payment System)
[221] Doctors seek help on cancer treatment from IBM supercomputer from *Reuters*
[222] Subledger
[223] If the "clawbacks" over the past decade are any indication, local townships and provinces will likely be a hurdle until they see the utility such ledgers could provide their own administrations. See China's Turn Against Law by Carl F. Minzner
[224] See Example 2: Escrow and dispute mediation
[225] Lex Cryptographia and Satoshi Nakamoto Institute
[226] These sites already exist: BTC-e, OKCoin, Cryptsy and Bter are among the largest multi-token processors.
[227] Bitcoin has 8 decimal places, the last of which is called a satoshi. In Ethereum, the last digit is called a wei. Note: in all examples, each user uses a cryptoledger as the mechanism for transport and audit.
[228] The dust limit has changed over the years and was implemented to prevent transaction spam (e.g., tens of thousands of transactions each amounting to 0.00000001 BTC). The current limit is around 5460 satoshi. See DustTransactions and What's the minimum transaction with bitcoin? from StackExchange
[229] Using external state
[230] The trustees do not necessarily need to be humans, as a DAO or Digital Oracle could technically act as a party and signatory authority. For example, see the whitepaper Securing wallets by integrating a third-party Oracle from CryptoCorp
[231] Michael Goldstein Explains How The Bitcoin Block Chain Enables Smart Property from Newfination
[232] The Ultimate Travel Hacking Guide from *Lifehacker* and How to Be a Travel Hacker by Nomadic Matt
[233] Recap of United's Downgrades: Award Charts, ExpertFlyer and Meals from Frequently Flying
[234] It could simply be a hash of an embedded URL that sends you to a screen on Airline Alice with the actual amounts along with the Terms of Service. Colored Coins have this potential capability as do other projects like Ethereum.
[235] This is not to say that a company needs to build and maintain its own cryptoledger for a rewards program. For example, assuming that Cocacolacoin is *not* using the Ethereum blockchain (or Bitcoin) but rather uses its own independent PoW blockchain, it may be hard to incentivize network hashrate which creates network security (which prevents a 51% attack). That is to say, instead of trying to incentivize Bob the Miner to exchange hashrate for Coca-cola swag only, Coca-cola could simply use a common, independent cryptoledger (like Bitcoin).
[236] Fraud Sinks Subway's Sub Club from *Wired*
[237] CPG Coupons: U.S. Market Analysis from NCH Marketing
[238] Mobile Coupon Redemption Values to Exceed $43bn globally by 2016, Driven by Better Targeting and Mobile Apps by Juniper Research
[239] Leader In Fast-Growing Digital Coupon Industry Sets Debut from *Investors Business Daily*
[240] New coupon scam is costing U.S. companies millions of dollars from *Fox6*
[241] Start Your Own Online Coupon Or Daily Deal Business by Richard Mintzer
[242] Rewards Program Tries Bitcoin from *The New York Times*
[243] Public/private digital key
[244] BTCrow

[245] One of the primary reasons this was the case is because Satoshi Nakamoto intentionally created Bitcoin for that purpose, hence the full name of the paper "A peer-to-peer electronic cash system" – the first section of the whitepaper discusses the problems people have with paying for things online; it was not a manifesto.
[246] See Example 2: Escrow and dispute mediation
[247] internet-ARBitration
[248] A Decentralized Bitcoin Exchange Process Dreamed up and Executed from Coinsigner
[249] See Colored Coins project and Colored Coins: NYDFS Reviews Ways To Transfer Ownership With Bitcoins from *International Business Times*
[250] Many of these "crypto exchange" ideas trace themselves back more than 20 years both in academic literature (Nick Szabo) and in science-fiction (Neal Stephenson). In fact, Stephenson wrote three novels in the 1990s which include crypto-based themes as an integral part of their plots (not cryptoledgers or cryptocurrencies, neither of which were foreseen). These are *Cryptonomicon*, *Snow Crash* and *The Diamond Age*. Prior to these publications, one non-fiction document that is historically seen as significant in the development of anonymous digital currencies and electronic privacy is *The Cyphernomicon* by Timothy May.
[251] The Great Firewall (防火长城) is an ongoing multi-decade project by several Chinese governmental institutions to filter and block undesired information from the mainland. The GFW is very effective for the most part; without a VPN, I was directly impacted every day for 5 years. I discuss this in Chapter 20 in *Great Wall of Numbers.* See also The Master Switch by Tim Wu
[252] See Bitcoin Startup Investing Snapshot: VCs Deploy $74M Across 40 Deals in 2013 from CB Insights, Bitcoin startup Coinbase receives $25m investment from a16z from *ZDNet* and Circle Raises $9M Series A From Accel And General Catalyst To Make Bitcoins Mainstream from *TechCrunch*
[253] Following the Money: Trends in Bitcoin Venture Capital Investment by Garrick Hileman. Note: Hileman used different chart numbering in his original publication.
[254] Despite the enthusiasm, competence and funding, the likelihood of success is not a given for any startup. And based on years of experience there are ways to try and mitigate and plan around known issues of founding a new company. See Death and startups: Most startups croak 20 months after their last funding round from *Venture Beat*, The Venture Capital Secret: 3 Out of 4 Start-Ups Fail from *The Wall Street Journal*, Fighting co-founders doom startups from *CNN|Money*, Why Small Businesses Fail: SBA from *About.com* and How Many New Businesses Fail in the First Year? from *eHow*
[255] Kauffman Foundation Bashes VCs For Poor Performance, Urges LPs To Take Charge from *The Wall Street Journal* and Most venture capital funds lose money from *CNN|Fortune*
[256] See Venture Survey Finds Big Jump in Investor Optimism for 2014 from *The Wall Street Journal*, Venture Capital's Sluggish Performance from *DealBook* and Venture capital kingpin Kleiner Perkins acknowledges weak results from *Reuters*
[257] See the annual MoneyTree Report from PricewaterhouseCoopers and the ever-growing list of funded Bitcoin companies listed on *CrunchBase*
[258] Compute Engine, github and Urbit
[259] AngelList, 500 Startups, Plug and Play, Y Combinator, SVAngel, Bitcoin Opportunity Fund and Boost. Each of these organizations provide different types of services, some are networking tools others are accelerators and incubators for entire development teams. For example, see Seven bitcoin startups pitch for funding at Boost VC demo day from *CoinDesk*
[260] See BitAngels Goes Global, Closing $7 Million (7,000 BTC) in Funding for Bitcoin Startups from *MarketWired*,Plug and Play Unveils Bitcoin Startup Incubator With Expert Mentors from *CoinDesk* and Currency Kings by *Entrepreneur*
[261] Backed by $5 Million in Funding (4,700 BTC), Mastercoin Is Building a Flexible, New Layer of Money on Bitcoin from *MarketWired*
[262] See What is Nxt? and Ethereum
[263] See BitcoinStarter and CoinFunder
[264] Why Bitcoin Matters by Marc Andreessen and Coinbase Raises $25M Led By Andreessen Horowitz To Build Its Bitcoin Wallet And Merchant Services from *TechCrunch*
[265] Marc Andreessen sings Bitcoin's praises from *CNBC*

[266] Following the Money: Trends in Bitcoin Venture Capital Investment by Garrick Hileman. Note: Hileman used different chart numbering in his original publication.
[267] Following the Money: Geographic Dispersion of VC Bitcoin Investment by Garrick Hileman. This is part 2 of his analysis, he uses different chart numbering.
[268] In addition to Garrick Hileman's data for Bitcoin Venture Investments, another open database of investment information can be found with The Bitcoin Database. See also: Exclusive: State of Bitcoin 2014 Report Analyses Emerging Trends from *CoinDesk*
[269] Lightspeed Venture Partners, Lightspeed Anchors Bitcoin Startups in Adam Draper's Incubator from *The Wall Street Journal* and Why Lightspeed Venture Partners Sees Bitcoin as a Good Investment from *CoinDesk*
[270] Skype calls now equivalent to one-third of global phone traffic from *ArsTechnica*
[271] Global Digital Goods Opportunities by Sam Kwong
[272] The Communications Market Report: International from Ofcom
[273] Shakil Khan, founder of CoinDesk uses the analogy that Bitcoin has the potential to be an IP address for money. See Shakil Khan: Bitcoin can be "money over IP", but services must get more intuitive from *CoinDesk*
[274] DealCoin
[275] Commotion, XORP, 802.11s, Wireless Mesh Networking
[276] My thwarted attempt to tell of Libor shenanigans by Douglas Keenan
[277] BitGive Foundation, Bitcoin Not Bombs and Sean's Outpost are probably the three most well-known charities that accept cryptocurrency donations. See Bitcoin Helps Homeless Charity Sean's Outpost go from Strength to Strength from *CoinDesk* and Jason King of Sean's Outpost on Bitcoin and Charity interview by Jeffrey Tucker
[278] The 50 worst, ranked by money blown on soliciting costs from *Tampa Bay Times*
[279] China gets 76 bln yuan in donations for Sichuan quake from *People's Daily*
[280] County vows to correct misuse of post-disaster relief money from *China Daily* and Quake zone hit by yet another relief scandal from *South China Morning Post*
[281] For more on this issue related to China, see Chapter 18 in *Great Wall of Numbers*. See also, Red Cross donations not collected for 4 years from *China Daily*
[282] Kapronasia and Bitcoin Singapore 2013 with Zennon Kapron
[283] The December 5th notice does not really say that merchant services are forbidden. It says that financial companies and 3rd party payment processors cannot deal with Bitcoin, and also says that bitcoin is not a currency. The prevailing thought at the moment is that exchanging goods and services for bitcoin is like bartering, so merchant services should be fine. The industry will only really know once something like BitPay actually takes off in China. China Bans Payment Companies From Clearing Bitcoin, News Says from *Bloomberg* and 淘宝新增比特币等虚拟币等禁售规则公示通知 from Taobao. It may also be instructive to read 虚拟货币本质上不是货币 from Sheng Songcheng, the head official of investigation and statistics at the PBOC.
[284] A type of chicken and egg problem – the important point is whether domestic users can pay for wares in a cryptocurrency. Since the majority of ecommerce in China is managed through Alibaba and Tencent, who in turn have backed out of supporting this crypto space, in the short run may only work for Chinese residents buying products abroad but in China itself there are several hurdles to adoption.
[285] The German Monetary Unification (Gmu): Converting Marks to D-Marks by Peter Bofinger
[286] Outside of academia, over the past years various people have discussed the role a cryptocurrency can play with respect to integration with central banks, including using to fulfill the bancor concept (international reserve system). One recent example is the Bitnote thought-experiment from Wolfgang Münchau. For more on bancor, see Reserve Accumulation and Intern ational Monetary Stability from the IMF, The Global Currency Conundrum and the "Babel Fish" of Money by Chris Larsen and Our flawed financial system is reflected in Bitcoin from *Financial Times*
[287] Shanghai liberalises offshore yuan borrowing in free-trade zone from *South China Morning Post*, Shanghai Free Trade Zone: The next Shenzhen? from *The Economist*, China approves 12 more free trade zones from *Xinhua*
[288] 500 Startups, BitDazzle, BTCJam
[289] Interview on January 12, 2014

[290] Both citizens and expats are limited to international transfers of $50,000 denominated in foreign currencies per year. For more details see Chapter 5 – Financial services in *Great Wall of Numbers* and Animal Spirits with Chinese Characteristics by Mark DeWeaver.
[291] Tianhong's Alibaba mutual fund grows to second largest in China from *South China Morning Post*
[292] Text, Chat, Profit: Tencent Launches Investing on WeChat from *The Wall Street Journal*
[293] And at least 272 million monthly users. See China's WeChat App Targets U.S. Users from *The Wall Street Journal*,China banking war heats up with launch of online investment app from *Financial Times* and How WeChat's 600 Million Users Spell Out Big Profits For Brands from *Jing Daily*
[294] See Tencent: China's hottest tech company from *CNN|Money* and Chapter 12 – Social Media and marketing your brand from *Great Wall of Numbers*
[295] Dearcoin, General Assembly and Bitpass
[296] Bitcoin Institute and Seedco.in
[297] Hivewallet
[298] CoinSimple
[299] MEXBT and The bitcoin industry embraces what it was built to avoid—rules and regulation from *Quartz*
[300] 'Trustless attorney' is probably a marketing term lawyers will avoid using; instead, digital currency attorneys may become the nomenclature.
[301] With the advent of 'zero-knowledge' proof, there may be techniques like 'obfuscation' cryptography and homomorphic encryption that could enable proprietary contracts (e.g., obscuring information and applications in such a way that discerning the code would be impossible, thus the complete opposite of open source). See Cryptography Breakthrough Could Make Software Unhackable from *Wired*, IBM's homomorphic encryption could revolutionize security from *InfoWorld* and Cryptographic Code Obfuscation: Decentralized Autonomous Organizations Are About to Take a Huge Leap Forward by Vitalik Buterin
[302] Personal correspondence, February 4, 2014
[303] Smart contracts will need data standards and the first six Contract Types are (PAM, ANN, SWAP, STOCK, OPTION, FUTURE). See Project ACTUS, The Importance of ACTUS from Stevens Institute of Technology and Improving Systemic Risk Monitoring and Financial M arket Transparency: Standardizing the Representation of Financial Instruments by Mendelowitz *et. al.*
[304] Designing financial instruments could become straightforward with ACTUS standardizations. In contrast, a disproportionate allocation of resources is currently spent on arbitration, compliance and fraud protection associated with the contracts and instruments.
[305] For example, the New York Uniform Commercial Code already has a body of precedents covering payment systems, electronic bank deposits, debit cards and a default set of laws involving electronic transactions within Article 4-A: Funds Transfers.
[306] If you plagiarize a litigation brief, this is considered verboten. Similarly, while using Westlaw and LexisNexis, the search results are copyrighted, but the actual content is not (i.e., how you got there is copyrighted). In contrast, once a judge uses wording from a contract, it is in the public domain and others can use it.
[307] In a termsheet the precedents remain the same as the only thing that is usually different are the items explicitly listed. Other areas of law that are considered off-limits for copying are covenant analysis or collateral analysis. According to Sean Zoltek and several other lawyers consulted on this manuscript, attorneys in general look for methods to reduce repetition and reduce the amount of drafting done on a set of documents. Thus they may build a document 70% and then reuse or recycle portions of previous document which has a great set of covenants for the other 30%.
[308] '500 Startups' Recruits Ex-MySpace VP to Mentor Bitcoin Businesses from *CoinDesk*
[309] Cryptrade is the open-source repository on github, Cryptotrader is a community of programmers and architects creating bots used on exchanges (e.g., for HFT arbitrage). Be aware that anyone claiming to sell you a turnkey bot capable of arbitrage is likely scamming you, if it worked as stated, they would be using it instead.
[310] Andreas Antonopolous used this as an example of smart contract he would build if and when Ethereum is launched. See *What is ethereum?* (video)
[311] Mike Hearn uses this in his presentation (video) as an example of how a DAO and smart contracts can be used to replace taxation for public goods.

[312] The private provision of public goods via dominant assurance contracts by Alexander Tabarrok

[313] Mike Hearn (video) calls the initial phase of this DAO infrastructure the "TradeNet." He later uses hardware examples, yet it is the software that controls the smart property functionality within the hardware. By "dying" he means that an inefficient taxi service-based DAO could sell itself as salvage material (to pay off debts) and/or restart and turn back on during potentially different market conditions. Eventually there could be a "MatterNet" in which quadcopters can transport goods (e.g., like the Amazon air delivery) or urban infrastructure that rearranges itself based on real-time demand (e.g., automated vending machines being lifted by quadcopters to new locations based on market demand). All of this again, is controlled by DAOs that may or may not reside virtually on a cryptoledger.

[314] See Regulating Bitcoins: CFTC vs. SEC? from Mondaq, CFTC's Chilton on Possible Regulation of Bitcoin from Bloomberg, Here's how Bitcoin charmed Washington from *The Washington Post*

[315] One of the topics discussed at the hearing was KYC which is 'Know Your Customer,' a banking regulation enacted to collect customer information for statutory compliance. See Community Debates What's Next After New York Hearings from *CoinDesk* and Understanding global KYC differences from PricewaterhouseCoopers

[316] In February 2014, The Law Library of Congress published a detailed look into 40 jurisdictions with respect to the regulation of Bitcoin, "Regulation of Bitcoin in Selected Jurisdictions." See also Bitcoin's Legality Around The World from *Forbes* and BitLegal which provides a color-coded map of each jurisdiction with relevant regulatory information. KPMG recently published a thorough article regarding tax implications surrounding Bitcoin, Chomping at the Bit: U.S. Federal Income Taxation of Bitcoin Transactions. In addition, several of the 2.0 platforms have created an industry association called Consortium of Decentralized Applications (CoDA) to discuss and navigate the legal framework of various jurisdictions. Similarly, the Digital Asset Transfer Authority (DATA) is a new self-regulatory organization focused on creating regulatory proposals and interaction with policy makers.

[317] FinCEN Publishes Two Rulings on Virtual Currency Miners and Investors from Financial Crimes Enforcement Network

[318] AB-129 Lawful money: alternative currency from the California Legislature. Perhaps a 'BitLicense' will become integrated with the New York Uniform Commercial Code Article 4-A: Funds Transfers. See California House Passes Bill Declaring Cryptocurrency Legal Tender from *AltCoin|Press*

[319] Money Transmitters and Currency Exchangers from Washington State Department of Financial Institutions

[320] Singapore's government is currently taking a hands off approach towards cryptocurrency right now whereas Denmark plans to regulate and oversee its use. At the end of February, Vietnam's central bank issued a statement warning banks and credit institutions from using it. See Singapore government decides not to interfere with Bitcoin from *Tech In Asia*, Bitcoins Spark Regulatory Crackdown as Denmark Drafts Rules from *Bloomberg*, Vietnam Warns Against Bitcoin, Invokes the Ghost of Gox from *CoinDesk*

[321] China Bans Payment Companies From Clearing Bitcoin, News Says from *Bloomberg*

[322] Britain to scrap Bitcoin tax from *Financial Times*

[323] The Bitcoin network does charge a small nominal fee for some transactions, although most are processed without any fee. A transaction drawing bitcoins from multiple addresses and larger than 1,000 bytes may be assessed 0.0002 BTC as a fee. Furthermore there is a hardcoded block size of 1 MB, or 7 transactions per second. For comparison, VISA's payment processing centers handle on average of 2,500 transactions per second and are built to process a surge of up to 10,000 to 20,000 per second. In order to change this, a hard fork must be implemented. Long-term this creates a problem dubbed a "crypto tragedy of the commons." Ken Griffith recently pointed this out, noting that "Bitcoin transactions cost above $50 per transaction, which is very high, but it feels low because this cost is paid for through the creation of new bitcoins that equally dilute everyone's bitcoins. The person making the transaction doesn't pay the fee, all holders of Bitcoins pay what amounts to an inflation tax out of dilution of their Bitcoin value. From the user's perspective of sending money with Bitcoin, it feels practically free!" While the actual transaction cost fluctuates (has been in the range of $40-$90 over the past 3 months), he does have a valid point that is usually glossed over. See Transaction fees, On Transaction Fees, And The Fallacy of Market-Based Solutions, Bitcoin – A Jack of All Trades is the Master of None by Ken Griffith, Bitcoin needs to scale by a factor of 1000 to compete with Visa. Here's how to do it. by Timothy Lee and Top secret Visa data center banks on security, even has moat from *USA Today*

[324] The way the current system is setup, remittances and funds sent abroad go through multiple institutions via 'correspondent accounts' or 'correspondent banking.'
[325] Will Migrant Workers Drive Bitcoin's Mundane Future? from *Bloomberg*
[326] Is Bitcoin the future of remittances? from *CCTV* and Remittance Prices Worldwide from World Bank
[327] Migrants from developing countries to send home $414 billion in earnings in 2013 from World Bank
[328] African Migrants Could Save US$4 Billion Annually On Remittance Fees, Finds World Bank from World Bank
[329] Will Migrant Workers Drive Bitcoin's Mundane Future? from *Bloomberg*
[330] ZipZap
[331] MoneyGram Joins ZipZap's U.S. Payment Center Network from *PRWeb*
[332] You Can Now Pay Cash For Bitcoin at 28,000 UK Stores from *CoinDesk*
[333] Bitcoin Education Project and Bitcoin or How I Learned to Stop Worrying and Love Crypto at Udemy
[334] PGP (Pretty Good Privacy) was released in 1991 by Phil Zimmermann, see: Cypher Wars from *Wired*
[335] M-PESA and Enabling financial transactions for consumers and businesses: Safaricom's M-PESA mobile money service by Filippo Veglio
[336] Kipochi launches first Bitcoin wallet in Africa with M-Pesa integration from Kipochi
[337] From oil painter to the C-suite from *Financial Times* and M-Pesa helps world's poorest go to the bank using mobile phones from *The Christian Science Monitor*
[338] Insight: African tech startups aim to power growing economies from *Reuters*
[339] According to an email exchange with Michael Youssefmir, an engineer at Google who has previously published mobile data pricing on Ghana, "MPESA was successful because Safaricom had a monopoly and regulators failed to regulate before the system took hold. Successful mobile money systems in the class of MPESA must become defacto standards. The fragmentation and regulation that occurred in other African countries is exactly why we keep having to talk about Kenya and only Kenya. As a defacto standard that is resistant to regulation, bitcoin is an ideal currency and system to serve as mobile money in the developing world."
[340] Fewer than one in three Africans has a mobile phone from *Reuters* and The Sleeping Giants Of African Mobile Payments from *TechCrunch*
[341] Half the World is Unbanked from Financial Access Initiative
[342] This is a paraphrase from Jeff Garzik, a Bitcoin developer. Furthermore, decentralized pools like P2Pool would help alleviate some of that concern, yet there are financial incentives for "hashers" to use larger pools that create imbalances that are discussed in Hashers are not miners, and Bitcoin network doesn't need them.
[343] An example is Bi•Fury from Crypto Store. In terms of electricity, this has always been an issue even as far back as 2011, see Bitcoin Mining Update: Power Usage Costs Across the United States from *PC Perspective*
[344] Other questions that need to be answered about new ASIC announcements: Has it passed verification process? Has it been taped out? What about maskmaking? See: Automate and Control the Functional-Verification Process from *Chip Design*, Interview: Adnan Hamid Addresses Trends In Chip Verification from *Electronic Design* and Chip verification made easy by Laurent Fournier
[345] See Engineering the Bitcoin Gold Rush: An Interview with Yifu Guo, Creator of the First Purpose-Built Miner from *Motherboard*, That Swedish Bitcoin Mining Company Has Sold $28 Million-Worth Of Its New Mining Hardware from *Business Insider* and CoinTerra Ships First Terahash Bitcoin Mining Rig from *CoinDesk*
[346] Butterfly Labs Announces Next Generation ASIC Lineup from *PRWeb*
[347] BFL ASIC Status from Butterfly Labs and Butterfly Labs Shipping Still A Year Behind, Broken Promises from *igotbitcoin*
[348] Personal correspondence, November 30, 2013
[349] Martin Meissner recently brought a lawsuit against BFL over a similar issue, for failure to deliver on two 1,500 GH/s miners he paid $62,598 for which he allegedly never received. See Butterfly Labs Faces $5m Lawsuit Over Unfulfilled Order from *Coindesk*
[350] Difficulty rating for Bitcoin adjusts every 2016 blocks or roughly every 2 weeks. See Bitcoin mining profitability calculator
[351] Contrary to popular myth Sears & Roebucks did not exist at this time and in fact was founded much later in its modern form in 1893. It was Richard Sears' father, James who went to California during the gold rush and failed to "strike it rich."

[352] Or 'fragile' as Nassim Taleb would likely classify their predicament (as opposed to anti-fragile); (video).
[353] I have written several articles on how to build and use Scrypt-based mining systems, see: 12 Step Guide: Easiest and fastest way to start mining Scrypt-based tokens for Litecoin and Dogecoin and Should you buy an Alpha Technology ASIC for Litecoin mining?
[354] This Pizza Cost $750,000 from *Motherboard*
[355] Shelling Out -- The Origins of Money by Nick Szabo
[356] BitPay also includes functionality that allows users to synch and import bitcoin sales into Quickbooks. Another example of integration and adoption was in March 2013, Expensify added support for Bitcoin payment which allows companies to reimburse international workers with bitcoin. See Import your Bitcoin Sales into Quickbooks from BitPay and Expensify Now Offers Support For Bitcoin, An Alternative To PayPal For International Contractors from *TechCrunch*
[357] BitPay Exceeds $100,000,000 in Bitcoin Transactions Processed from BitPay and BitPay Announces Bitcoin Payroll API from *BusinessWire*
[358] Gyft doubled its accepted locations in six months during 2013. See Gyft Launches Rewards Platform to Give Consumers Up to 3% Back on Gift Card Purchases from *PRNewswire* and Gyft Opens Bitcoin Acceptance to 50,000 Merchant Locations from *PaymentsSource*
[359] Shopify Merchants Can Now Accept Bitcoin from Shopify from Shopify
[360] In First Day With Bitcoin, Overstock Does $126,000 in Sales from *Wired* and Here Is What Bitcoin Users Are Buying On Overstock.com from *Forbes*
[361] Tiger Direct Processes $500,000 in Bitcoin Payments from *Josic*
[362] A Major Coinbase Milestone: 1 Million Consumer Wallets from Coinbase
[363] Games Giant Zynga Starts Playing With Bitcoin from *CoinDesk*
[364] See Humble Bundle now accepting Bitcoin using Coinbase bitcoin merchant tools from Coinbase
[365] Formlabs releases PreForm 1.0 and begins accepting Bitcoin payments from *The Verge*. I f you would prefer someone else print your 3D wares, individuals can patronize CryptoPrinting.
[366] 200,000 Hotels Now Accept Bitcoin Through Online Travel Agency CheapAir from *CoinDesk*
[367] BitPay Drives Explosive Growth in Bitcoin Commerce from *BusinessWire*
[368] Even if a company is not necessarily interested in becoming involved within the cryptocurrency community, it is relatively easy and straightforward for a merchant to accept bitcoin as a payment option. In less than 15 minutes a merchant could download a plugin from Coinbase or BitPay and the transactions will move seamlessly through the store.
[369] BTCJam
[370] Credit-card debt may threaten Brazil's boom from *Bloomberg Businessweek*
[371] While credit would likely still be cheaper in developed countries, because interest rates are centrally planned by various institutions, this creates distortions in time-preferences for market participants (e.g., zero-interest rate policies encourage the usage of capital instead of the accumulation of capital; risk is subsidized by one or more parties). See The Theory of Money and Credit by Ludwig von Mises
[372] FICO is an acronym for Fair, Isaac and Company. In 1989 this firm created a rating system that is used by the largest credit reporting bureaus (e.g., Experian, Equifax and TransUnion).
[373] 2013 LexisNexis True Cost of Fraud Study
[374] US P2P Lenders Issue $2.4 Billion in Loans in 2013 from Lean Academy
[375] Bitcoin is far more than a currency for speculators from *Financial Times* and Riding the wave of global transaction services and payment systems from IPFA pgs. 11-12
[376] Evr.gr
[377] See BankToTheFuture.com and Equity Crowdfunding – Building The Bitcoin Infrastructure from IamSatoshi
[378] See Kickstarter Coins and LTBCoin by Adam Levine. In some ways, this is also a cryptographically controlled process to subsume penny-stocks and over-the-counter instruments. Other hypothesized tokens include 'couch surfing coins' and tokens representing digital assets in games such as EVE Online and World of Warcraft.
[379] Ibid
[380] Join My IPO

[381] FrostWire, a company that makes BitTorrent software, recently integrated Bitcoin, Litecoin and Dogecoin into their software. Users can directly donate and support content creators. See Bitcoin Donations Now Integrated into BitTorrent Client from *TorrentFreak*
[382] MaxCoin and Megacoin
[383] The Idea of Smart Contracts by Nick Szabo
[384] Personal correspondence, January 24, 2014
[385] I interviewed him on February 6, 2014. See also '500 Startups' Recruits Ex-MySpace VP to Mentor Bitcoin Businesses from *CoinDesk*
[386] UX means 'user experience' and UI means 'user interface.'
[387] Smart Contracts by Nick Szabo
[388] Coinality and 12 Days of Bitcoin: Get Paid in Bitcoin from *Bloomberg*
[389] Is this "transaction malleability" really an issue? from StackExchange
[390] Contrary to Mt. Gox's Statement, Bitcoin is not at fault by Gavin Andresen and Mt. Gox Blames Bitcoin – Core Developer Greg Maxwell Responds from *Cryptocoinsnews*
[391] Bitcoin Exchanges Under 'Massive and Concerted Attack' from *CoinDesk*
[392] The story is likely more complex and details are still forthcoming. See Unilateral Statement Regarding Mt. Gox from an Insider by Jesse Powell, Inside Japan's Bitcoin Heist from *The Daily Beast*, Mt. Gox Exchange Files for Bankruptcy from *Bloomberg*, Mt. Gox files for bankruptcy, blames hackers for losses from *Reuters* and The programming error that cost Mt Gox 2609 bitcoins by Ken Shirriff
[393] The development team has published a public wiki describing the specifications and functionality. See Bitcloud Project
[394] Adam Levine has been working on an interesting side project involving reputational callable tokens. See Kickstarter Coins and LTBCoin
[395] A recent public example of multisignature transaction is from the Bitcause initiative to provide humanitarian aid to Ukrainians. The three key holders are Edan Yago, Ron Gross and Elizabeth Ploshay. See Bitcause and Only Bitcoin can reach them!
[396] In addition to Udacity and Coursera, readers may be interested in projects like Khan Academy, CodeAcademy and Duolingo.
[397] Introducing Bitcore from BitPay
[398] Insight.bitcore.io
[399] The Betamax vs VHS Format War from Media College
[400] HTTP 2.0 is currently in the standardization phase at this time.
[401] Kraken
[402] Once a user has been authorized, one of the unique features of Kraken is that they can eventually conduct leveraged and margin trading.
[403] While the latency and logistical issues are being discussed, the Open-Transactions (OT) project attempting a different approach to HFT through the ability to create 'centralization' via federated servers and 'voting pools' – essentially there would be off-chain exit nodes that transfer to HFT clusters.
[404] The Archetypes of Virtual Currency by Salvatore Delle Palme
[405] The Ephemeral Artcoin by Salvatore Delle Palme
[406] Let's Talk Bitcoin
[407] eBay Views BitPay and Coinbase as Potential PayPal Competitors from *CoinDesk*
[408] Wells Fargo calls Bitcoin summit on 'rules of engagement' from *Financial Times*
[409] See Demand and supply statistics from World Gold Council
[410] 3 Infographics on the Future of Digital Retail from JCK and Ecommerce Sales Topped $1 Trillion for First Time in 2012 from *eMarketer*
[411] It should also be noted that while the low-hanging fruit of smart contracts is securities trading, it is highly unlikely that a professional trader would use a blockchain directly for an HFT. For example, in most markets, especially the very liquid ones, where latencies are counted by increasingly smaller segments of time, the pace of 1 block per 10 minutes (or even 2.5 minutes) is limiting. Open-Transactions (OT) has the ability to create safe 'centralization' through federation and 'voting pools.' Essentially there would be off-chain exit nodes that transfer

to HFT clusters. See Voting Pools: How to Stop the Plague of Bitcoin Heists, Thefts, Hacks, Scams, and Losses from *Bitcoinism* and How can Open Transactions benefit Bitcoin? from StackExchange

[412] See also Chapter 3 on the discussion of Simplified payment verification (SPV) and How explicitly can the blockchain be pruned? from StackExchange

[413] Professor Evans uses a different title "Chart 1" than what is in this manuscript. See Bitcoin Payments: Igniting Or Not? by David Evans

[414] From oil painter to the C-suite from *Financial Times* and M-Pesa helps world's poorest go to the bank using mobile phones from *The Christian Science Monitor*

[415] NXT currently has a maximum rate of 255 transactions per block and 1 block is processed every minute, so roughly 4 transactions per second. However, 'transparent mining' is a new feature that is being developed by NXT which will enable it to compete with Ripple and other payment platforms. See Transactions per block and maximum transactions per second from Nextcoin.org and Transparent mining, or What makes Nxt a 2nd generation currency from Bitcointalk

[416] Another reviewer suggested that this was not an apples-to-apples comparison because SMS functionality is built into the feature-phones that Kenyans have. Thus a Bitcoin app would have to be on every phone and there would need to be people willing to accept Bitcoin in order for this to be a fair comparison. While this may be the technical case, the larger issue is that media coverage of Bitcoin dwarfs similar M-PESA coverage in nearly every market, yet despite this, there has been very little adoption due to the reasons discussed in this manuscript (e.g., cumbersome wallets, security vulnerabilities on the edges, no 'smart fine print').

[417] Visa's system has an uptime near 100% during peak times of up to 20,000 transactions per second and encrypts every transaction separately; key hashes expire roughly three seconds later reducing exploits to zero (e.g., zero money stolen off the wire, or out of merchant accounts). According to Visa, it spent $425 million on IT expenses for the year ending on September 30, 2010. While decentralized systems have some advantages, in computer science, they cannot currently simultaneously fulfill the following guarantees: consistency, availability, partition tolerance (called the CAP theorem). They can provide two-of-three but usually not all three simultaneously. In addition, while it may be reduced later, the infrastructure costs of maintaining this proof-of-work system is significantly higher than Visa's. See Comparing VISA and DoD I.T. by Paul Strassmann

[418] ACH stands for Automated Clearing House, which is an electronic financial network in the US. In 2012 it processed 21 billion transactions worth a total of $36.9 trillion. See ACH Payment Volume Exceeds 21 Billion in 2012 from NACHA

[419] This issue was recently highlighted in a very articulate article, Bitcoin – A Jack of All Trades is the Master of None by Ken Griffith. There are other financial startups in the payments space including Coin (a swipeable card) and Ricardo. In addition, Apple is including functionality with new iPhone hardware and software that allows Bob to scan barcodes at stores and instantly pay with his phone instead of going to the checkout. Bob can also pay with a photo of the item. See Bitcoin vs. Coin: Which will have the most success in 2014? From *The Next Web*, Ricardo - An Executive Summary and Apple Pushes Deeper Into Mobile Payments from *The Wall Street Journal*

[420] See Bitcoin Seen as Little Threat to Payment Firms from *Bloomberg*. MasterCard recently launched a new location-based service called Syniverse. See MasterCard Creates New Payment Product With A Company Most Have Never Heard Of. by Brian Roemmele

[421] Bitcoin Client Num Downloads from Bitcoin Pulse

[422] The actual number as of this writing is 1,307,387 addresses that hold 99.99% of all bitcoins. Again, these are addresses not users. These addresses can be managed by exchanges which have thousands or even millions of users. See Bitcoin Distribution by Address at Block 285,000 from BitcoinRichList

[423] AWS is both centralized and decentralized depending on your perspective. The datacenters themselves are distributed globally in specific geographic locations. Yet a user can split databases and computation into decentralized nodes/instances within these datacenters. See Amazon Architecture from High Scalability Customer Centricity at Amazon Web Services from *All Things Distributed*

[424] While Mint, Ubuntu and Fedora are more popular on desktops, in terms of overall usage and penetration, Android is far and away the leader in Linux-based adoption. See The most popular end-user Linux distributions are... from *ZDNet*

[425] Centralized versus decentralized information systems : A historical flashback by Mats-Åke Hugoson, Centralization Versus Decentralization: A Closer Look at How to Blend Both by Shelly Heiden, Decentralized Information Technology Requires Central Coordination! By Sarah Michalak, Julio Facelli and Clifford Drew, Mae Gets A New Job from *Library and Information Center Management* and Gartner Identifies 10 Key Actions to Reduce IT Infrastructure and Operations Costs by as Much as 25 Percent from *Gartner*

[426] The disruptive potential of smart contract for the entire financial industry, not just fiat credit facilities, is enormous. Charles Stross, the British sci-fi author, recently criticized Bitcoin and the cryptocurrency endeavor, wishing that it die a quick death (in fire no less). While his contentions were fallacious on a number of counts (especially regarding the environmental impact), ironically, he previously predicted seven years ago that near-future sci-fi authors are still probably missing something disruptively as large as the Internet 20 years ago or the smartphone was this past decade. In other words, just as rewatching older sci-fi films that failed to foresee drones and self-driving automobiles seems dated, the portrayal of centrally managed financial products may one day be viewed as an anachronism of our not-so-quaint analog past. Thus, Stross' prediction of another unforeseen invention could very well be these smart property applications and digital financial instruments that are managed and transported by the very same cryptoledgers he dreamt of burning. See Shaping the future and Why I want Bitcoin to die in a fire by Charlie Stross and Charles Stross takes on the Bitcoin community by Tim Swanson

[427] While it may be contentious to claim, the cryptocurrency industry may end up following the banking industry development, perhaps meeting with the current system somewhere in between. For example, there will likely be whole liquidity providers (market makers) and clearing houses. Arguably the easiest and perhaps quickest that can happen is incumbents entering the market.

[428] SecondMarket jumps to give legitimacy to Bitcoin from *USA Today*

[429] Netflix and YouTube are the Internet's bandwidth consumption kings from BGR

[430] See Chinese Land-Use Rights: What Happens After 70 Years? from *China Smack*, China's Real Estate Riddle from Patrick Chovanec, You May Own your Apartment, but who Owns the Land Underneath Your Feet? by Thomas Rippel, If Beijing is your landlord, what happens when the lease is up? from *China Economic Review* and Chinese fear homes are castles in the air by Stephen Wong

[431] See China's Land Grab Epidemic Is Causing More Wukan-Style Protests from *The Atlantic*, China Tackles Land Grabs, Key Source of Rural Anger from *The Wall Street Journal*, China land price fall threatens local finances from *Financial Times* and China's land-seizure problem from *Chicago Tribune*

[432] See China's Land Grab Epidemic Is Causing More Wukan-Style Protests from *The Atlantic* and China Tackles Land Grabs, Key Source of Rural Anger from *The Wall Street Journal*

[433] See China land price fall threatens local finances from *Financial Times* and China's land-seizure problem from *Chicago Tribune*

[434] This is between 120-150 million workers, see Internal Migration in China and the Effects on Sending Regions from OECD

[435] It should be noted that the term 'formal' versus 'informal' economy boils down to whether or not economic activities are tracked and taxed by a government agency. The majority of global economic trade and exchange has and is conducted informally, that is to say "untaxed." For example, transactional exchanges that are not monetized – consulting with friends, families and even strangers – are not taxed. In many cases 'informal' activity is just as transparent and efficient as 'formal' sectors, yet for many migrant workers, a lack of property rights and contractual structure creates abusive situations. Most social capital activities would fall under this definition yet the actual activities can be both productive and economically rewarding for the participants. System D is another name for it. See The Shadow Superpower by Robert Neuwirth and Could Bitcoin Become the Currency of System D? by Jon Matonis

[436] See Computer corporations: DAC attack from *The Economist*, Bootstrapping A Decentralized Autonomous Corporation: Part I by Vitalik Buterin and Bitcoin and the Three Laws of Robotics by Stan Larimer

[437] DAX is another term for the overall idea, decentralized autonomous 'x' where the 'x' can stand for corporation, organization, application, etc. For a spirited conversation regarding this topic involving Charles Hoskinson (Ethereum), David Johnston (Mastercoin) and Daniel Larimer (Invictus/Bitshares) see episode 80 – Beyond Bitcoin Uncut from *Let's Talk Bitcoin*.

[438] Hukou system and China: Urbanization and Hukou Reform from *The Diplomat*
[439] See Startup Cities Institute and Hacking Law and Governance with Startup Cities by Zachary Caceres. Interested parties can contact Mr. Caceres at: startupcities@ufm.edu
[440] Remittances flows to Latin America and the Caribbean remain stable at $61bn from Inter-American Development Bank and Remittances to Guatemala increased by 14.5 percent in January from *The Tico Times*
[441] Lamassu, Skyhook, Genesis and Robocoin
[442] See Blueseed, Urbanization Project, Software Is Reorganizing the World and Silicon Valley's Ultimate Exit (slides) by Balaji Srinivasan
[443] Securing wallets by integrating a third-party Oracle from CryptoCorp
[444] The perils of prediction, June 2nd from *The Economist*
[445] Casino Industry Accounts For Significant Slice Of U.S. Economy: Study from *The Huffington Post*
[446] Point-of-Sale Terminals Should Revolutionize Credit Card Payments by Dave Wilkes and Hack-resistant credit cards come at a price from *San Francisco Gate*
[447] As mentioned in Chapter 6, the Philippines is the 3rd largest remittance-receiving country. Nearly 10% of the population works abroad and most of these workers send money home, yet are faced with fees each month. Reducing and eliminating these fees could be a way cryptocurrencies can provide value and increase adoption. See Hong Kong money senders battle for Philippine trade from *BBC*
[448] Pay Another Way: Bitcoin from WordPress
[449] See Bitcoin – The Internet of Money by Naval Ravikant and Bitcoin isn't Money—It's the Internet of Money by Eli Dourado