A Manifold White Paper

Enabling Offline Economies with Cryptographically-Secured Peer-to-Peer Payments

Bottom Line

Manifold Technology has solved the double spend problem plaguing offline payments.

Introduction

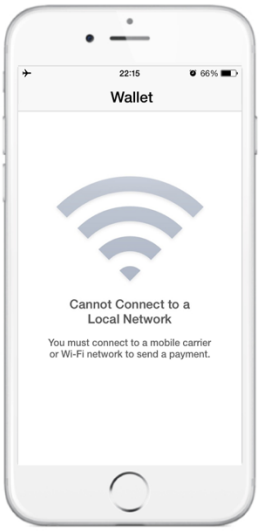
Solutions for online payments are plentiful with Apple Pay, Google Pay, PayPal, Venmo and Zelle among others; however, their peer-to-peer functionality is still highly centralized and dependent on network connectivity to provide value.

In the international market, WeChat is quickly gaining huge market share and is threatening these U.S. based payment platforms. As these U.S. players look to compete globally more effectively, they would be wise to consider exceeding WeChat's peer-to-peer capabilities rather than simply including them.

True offline payments are not currently supported by any payment app. They would constitute an impressive step forward, expand the market served by mobile payments and provide a powerful differentiator.

Problem: So Close, Yet So Far

Not having a cell signal can be pretty irritating. Can't check your messages, can't Venmo your part of the bill, can't even get that free coffee you've earned suffering through the Perka experience. But we all know these are mostly just inconveniences. In a minute you'll have service, or wifi, or someone's tethered connection to bum off of. But that's not the case in a lot of places around the world. It could be days, or weeks, before connectivity is once again available.



What many of us may not realize is that, often, those are the same places where a phone app really *is* the only way to access a bank account and use your own money. Cash is an obvious solution, but counterfeiting and theft make it dangerous. Similarly, checks don't hold the answer as they are a huge step backward when it comes to mitigating the counterfeiting problem. Ubiquitous connectivity will be nice, one day, when it finally happens. Until then, we need a more elegant solution. Some kind of actual peer-to-peer solution.

Peer-to-peer payments have come to mean something closer to "easy," or "without a bank in the middle," rather than insinuating any direct connection between peers. In an ideal world through, a peer-to-peer payment really

should only require peers. And, if it only requires peers, it shouldn't require any online connectivity at all.

Technologies such as Near-field Communication (NFC), QR code scanning and even Bluetooth provide for contactless exchanges between devices to securely swap payment details. However, these technologies remain dependent on network connectivity with financial settlement systems for payment processing. They still require an online tether to exchange value and mitigate fraud risks.

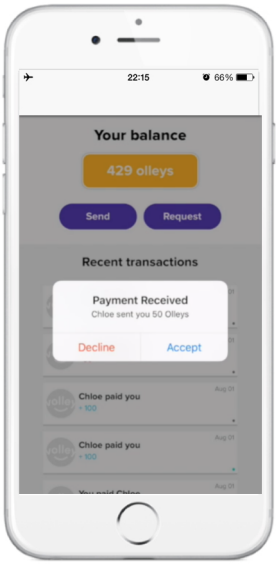
True, offline, peer-to-peer payments all run smack into the same concern: the dreaded double spend. Because executing a double spend is so trivial to accomplish with standard checks, the intensity of the focus on this problem in the digital space is interesting. Regardless, it can be addressed by modern technologies.

Challenges of P2P Value Exchanges

Exposure. Financial exposure is *the risk* of all value exchanges, but it becomes particularly acute when examining the digital payments space. There are potentially three parties exposed in any given transaction: the financial institution of the payer, the financial institution of the payee, and the payee themselves. Mechanisms for payment, or any type of value transfer, are only valid if the parties to that transaction are willing to accept the risks involved using that mechanism.

Online connectivity has allowed digital payments to reduce the risks of exposure so much that they are truly negligible for all practical purposes. Offline payments will never be able to achieve the same ubiquitous reduction in risk. However, they can, and should, allow the parties involved in the transaction to accept as much, or as little, risk as they are comfortable. In other words, offline payments should allow the payee to demand the same negligible risks as online payments, should they so desire.

Manifold's Solution

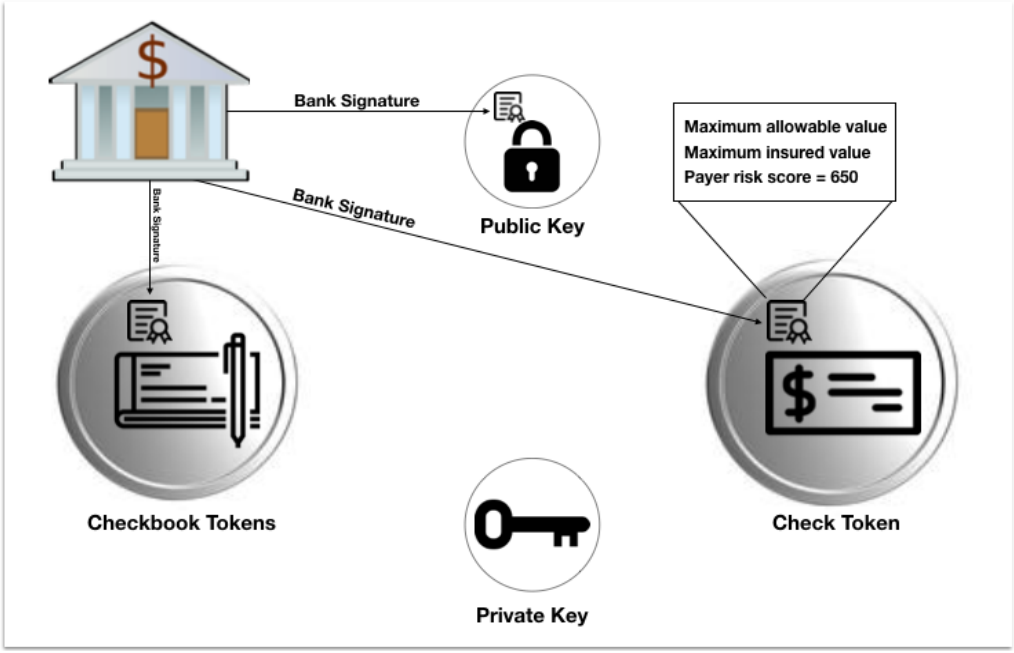


Manifold has developed cryptographically-secure wallet technology that offers secure payment and exposure controls. The solution does not address the exposure risks of the payee's financial institution as those are out of scope for the specific payment being executed (Manifold can't prevent an institution from taking an idiotic risk). However, risks to the payer's financial institution, and the payee themselves, are perfectly controlled.

The high level flow is almost identical to the old-school checkbook: the payer's financial institution issues signed digital tokens (the checkbook) which can be used by the payer to transfer value to the payee (write a check). The payee then reports this to their institution, whenever they regain connectivity, and any necessary bank-to-bank settlements occur (deposit the check).

The Checkbook

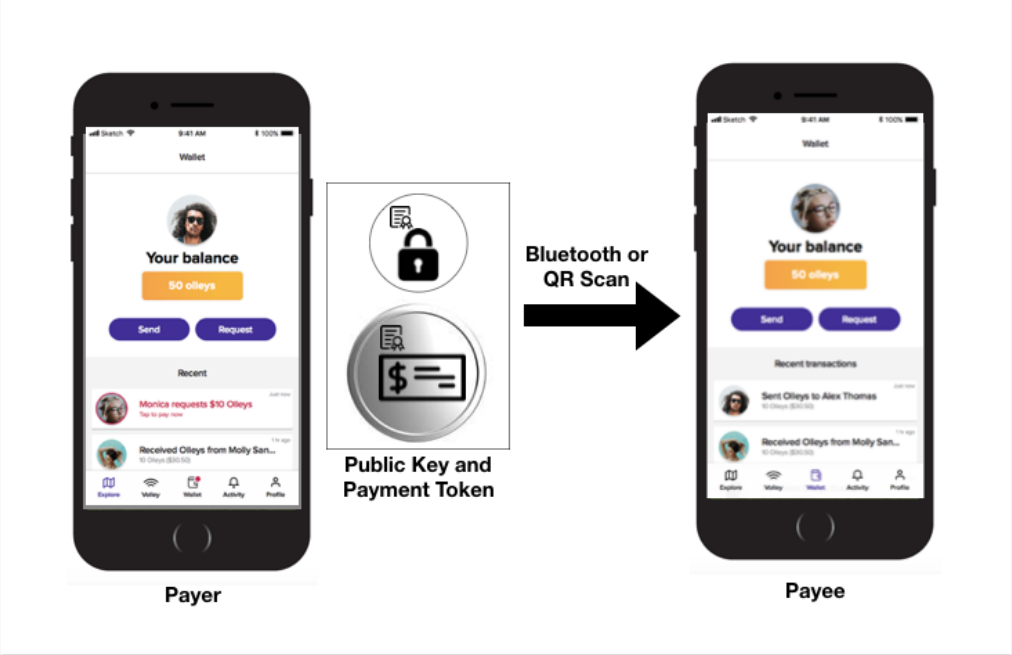
The digital tokens that the financial institution issues to the payer are significantly more robust than a simple checkbook. They are cryptographically signed by the financial institution, as is the payer's public key which we'll see more of later, and include information such as the maximum value any given token may represent, the maximum value the financial institution is willing to cover in the case of fraud, and a standardized risk profile for the payer (like a simple credit score but more nuanced).



The Checkbook

The Check

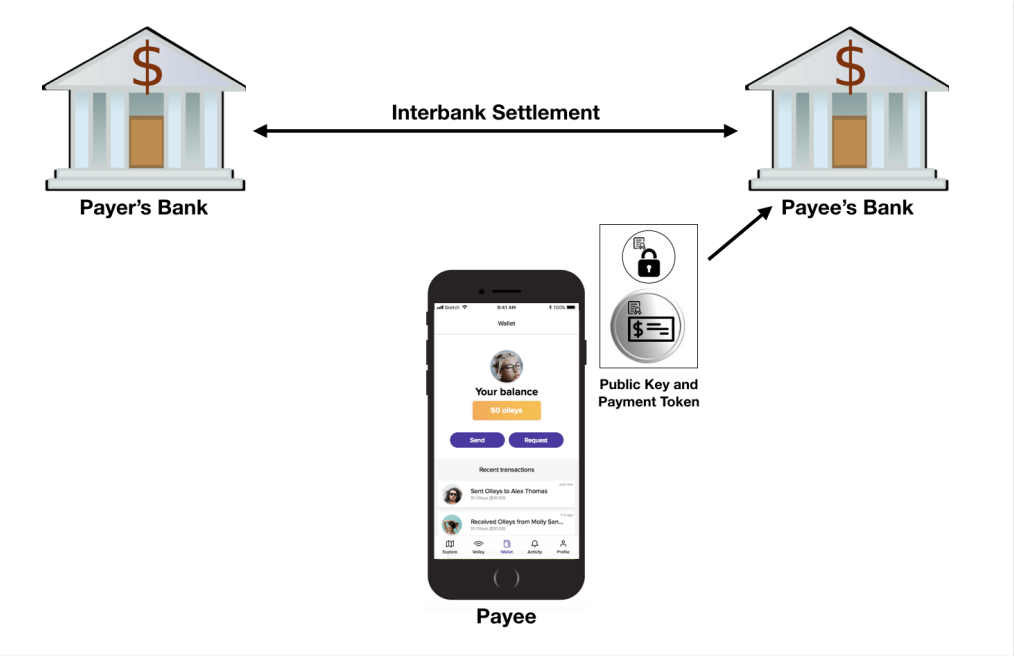
When the payer decides to authorize and execute payment, one of the issued tokens, along with the specific authorized value, is signed to the payer's public key and transferred (via Bluetooth or QR code) to the payee. Included in this transfer is a copy of the payer's public key which has been signed by their financial institution.



The Check

The Deposit

Depositing the token is a simple matter of sending the token, and the payer's signed public key, to the payee's financial organization. The information is then verified, and the actual settlement requested via standard bank-to-bank channels as necessary.



The Deposit

The Risks

The payer's financial institution has two levers to control their exposure in the case that the payer decides to commit fraud. The first is that they control the number, and value, of the issued tokens. An unproven individual may only be given tokens which are individually worth far less than the payer's total funds, for example. The second is that, as part of the token, they declare the maximum amount they will cover in the case of fraud. That is, they explicitly state how much risk they are willing to tolerate.

On receipt of those tokens, the payee has all of the information necessary to make an educated decision about the exposure they are willing to accept. They may decide that they are only willing to accept "certified checks" (those fully covered by the issuing bank in case of fraud), that they will only accept tokens from individuals with exceptionally good risk profiles, or that they are willing to make an exception for this specific individual.

finance.yahoo.com

Zelle users are finding out the hard way there's no fraud protection

Double spending in this scenario would be very challenging. Compromising the application, negotiating the appropriate exchange protocols, etc. but it is theoretically possible. What isn't possible, is to force any exposed party to accept more risk than they are comfortable with. Because of this, while not wholly eliminated, the double spend risk can be entirely mitigated.

Use Cases

Isolated Economies
Mobile banking and messaging services have empowered the previously unbanked and unconnected, but those services still require cellular connectivity to provide value. Offline p2p payments will provide isolated communities with a continuous means of leveraging the global financial system irrespective of cellular infrastructure. Commerce can be conducted via secure device-to-device checks (i.e., tokens) and then settled with financial institutions when either party has connectivity. Isolated economies include those without infrastructure as well as those where Internet access and mobile apps are banned or restricted, such as developing markets, rural areas, repressive nation states, highly regulated jurisdictions and schools.

Customer Engagement with Poor Connectivity
Customer engagement and loyalty apps like Perka require cellular or wifi connectivity for convenient app-based reward interactions with merchants. But, waiting for a connection because of poor signal strength can create an unpleasant experience for both customers and merchants. An offline p2p capability can provide a smooth alternative, allowing convenient exchange of reward points for environments with poor connectivity.

Disaster Response
Disasters create isolated economies by depriving people of ready access to banking services and cash withdrawals. An offline p2p wallet capability can provide government and non-government organizations with a way to provide direct relief to individuals by crediting their accounts with value they can then exchange offline with their neighbors for needed goods and services. Mobile hotspots and even charging power can be hard to find, and low priorities in the period after a major disaster, but during the long-tail of a recovery having a digital payment system that only requires periodic connectivity is both practical and valuable to helping restore basic services.

Hardware-free Point of Sale
Point of Sale hardware is designed to mitigate fraud risks, but also introduces a costly barrier to entry for small merchants and increases friction to commerce. Offline p2p mitigates those same risks without the need for costly hardware, providing small merchants and individuals with a low-cost option to accept payments for their business.

Conclusion

As payment platforms continue to evolve their offerings, they would be wise to make offline payment capabilities a central differentiating feature of their platform. Offline payments solve both financial inclusion problems, as well as mere connectivity shortfalls. Such a differentiation can drive not only greater user adoption, but platform loyalty, with users continuing to expand

their engagement with new offerings. As mobile payment apps proliferate and compete globally, offline payments can become a key differentiator.