Consumer protection – multisignature transactions

The bitcoin world, which has never been dull, is getting even more interesting with the growth of multi-signature approaches—called “ multisig”—for authorizing transactions.

This has the potential to help address one of the most significant challenges that bitcoin has raised: how can bitcoin users avoid losing their money if they authorize payment to a seller who fails to deliver, or if an exchange holding their private information gets penetrated by hackers?

These concerns drew heightened attention after Tokyo-based bitcoin exchange Mt. Gox ceased operations and filed for bankruptcy in February, leaving the equivalent of hundreds of millions of dollars of customer deposits in limbo, and likely lost.

Bitcoin transactions are accomplished with the aid of public key cryptography. Traditionally, if a bitcoin user we’ll call Alice wants to send bitcoins to a user we’ll call Bob, she uses a private key she controls to sign a message containing, among other things, the number of bitcoins she wants to transfer and a public key associated with Bob. Within about ten minutes this transaction will be verified by the bitcoin network, and it becomes, for all practical purposes, irreversible.

Bitcoin, as many people now know, is a digital currency and an associated protocol that makes it possible to send payments to anywhere in the world almost instantly and with very little overhead.

Bitcoin transactions are secured by the collective processing power of a network of widely dispersed computers, making it possible to establish trust

even when no single party in the network is trusted. It’s an ingenious approach to decentralizing trust that can be used not only for payments, but also for digital rights management, transferring ownership of digital goods, and many other applications.

But what happens if Alice thought she was buying a surfboard from Bob, and Bob, after receiving payment, decides to hang onto both the surfboard and Alice’s money? Since Alice knows only Bob’s public key but not his actual name, there’s no practical way for her to file a complaint. And, unlike if she had paid with a credit card, there’s no way for her to reverse the payment.

Multisig approaches have the potential to address this by making transactions contingent on the collective agreement of multiple parties. In the example above, the system could be modified so that Alice and Bob each provide their public keys to an escrow service, which then uses its own key to generate a new bitcoin address to which Alice can send payment for the surfboard. Moving the payment from that address requires the authorization of any two of Alice, Bob, and the escrow service. This protects Bob, because he can ship the surfboard knowing that Alice can’t unilaterally take back the money she has placed in escrow. Alice is protected because Bob can’t unilaterally extract the money from escrow. Once Alice receives the surfboard, she and Bob can jointly authorize the transfer of the money out of escrow to Bob. Or, if she claims that she hasn’t received the surfboard, or that it is defective, the escrow service can arbitrate the dispute.

Multisig can also be used to help combat unlawful payments (by making it possible for a third party to confirm that payees aren’t barred from receiving

funds) and to make exchanges and wallet services safer. In a “ traditional” bitcoin system in which payments can be authorized using only a single key, if that key is somehow obtained by hackers, the legitimate owner is out of luck. But in a multisig system, an exchange or wallet service can collect enough customer information to facilitate transactions, but not enough to enable a hacker to run off with a customer’s bitcoins.

Vitalik Buterin has a well-written, more detailed explanation of multisig transactions here.

For those with an interest in the finer nuances of multisig, Buterin’s article is well worth reading. And for all of us, multisig is an important example of how innovation in decentralized trust systems is just beginning. Unsurprisingly, multisig has led to some interesting startup possibilities. One of the most intriguing new companies in this space is Cryptocorp, founded in January 2014 by Miron Cuperman and Ryan Singer.

Cryptocorp is aiming to use multisig to enable bitcoin transactions to benefit from the same types of pre-clearance authorizations done today in association with credit card payments. Credit card companies will decline a transaction if the credit card has been reported stolen, if the seller’s merchant account has been suspended due to fraud or excessive chargebacks, or if the amount to be charged exceeds preset limits. Cryptocorp believes it will be able to offer analogous services—and more sophisticated variants of those services—to bitcoin users.