The Irony of Bitcoin

"Trust, but verify."

– Ronald Reagan on numerous occasions, quoting one of Lenin's favorite Russian proverbs

Whom do you Trust?

One of the television ads that ran frequently during the recent Winter Olympics showed champions seeming to take a bite from their gold medals as they received them on the medal stand. The image calls to mind an old movie Western, in which some crusty character in a saloon tests a gold coin with his teeth. The idea is that real gold is much softer than base metals of the same color, so the bite test is a quick way to verify that the coin is genuine. A gold coin will yield a little to your teeth; a fake won't.

When we receive payments in cash, whether we're talking about our contemporary paper money or gold coins in the Old West, all we have to do is verify that the cash is genuine. We don't have to trust the person that paid us, or even know who it was. If the coin passes the bite test, it doesn't matter whether or not the man in the saloon trusts the person that paid it to him. Electronic payments, such as with credit cards, don't work that way. They require a trusted intermediary — the bank that issued the card — to stand behind the payment. The developers of Bitcoin, the much talked-about "crypto-currency," designed it to provide a system of electronic payments where the principle of "just verify," without that trusted intermediary, would be enough.

Bitcoin has attracted a great deal of attention and a meaningful community of users. But it has only begun to enter the broader economy in a rudimentary way. These early attempts at practical implementation, along with the spectacular failure of a large Bitcoin exchange, have shown that Bitcoin relies on trust and confidence just as heavily as any conventional form of money for acceptance as a currency. In spite of its proponents' stated goal of replacing "trust but verify" with "just verify," integrating Bitcoin into the general economy would require the development of a set of institutions on which the broad public can rely to govern its use. To see why, we'll first have to explore what Bitcoin really is, and how it works.

You Can't Hold a Bitcoin in your Hand

The paper[1] that purports to represent the design proposal for Bitcoin describes as it as a system of payments, rather than a currency. The system's objective is to create a system of electronic payments that does not rely on a bank or other financial institution as an intermediary. Rather than requiring users to trust either a governmental issuer of currency or a financial institution, it relies on a peer-to-peer network.

You may have seen photos of futuristic coins bearing a stylized letter *B* decorating news stories about Bitcoin, but those are just illustrations. You can't hold a bitcoin in your hand. Bitcoin transactions exist entirely in a great general ledger called the *blockchain*, and bitcoin holdings at any point in time are nothing but the end result of a calculation tracing all those transactions since Bitcoin Day 1, at the beginning of 2009.

The ingenuity of Bitcoin lies in the way the Bitcoin network records transactions and maintains the ledger without relying on a central, authoritative record-keeper. Bitcoin payments substitute an arbitrary unit of account for conventional currency. They replace financial institutions with a technological verification mechanism that operates over the peer-to-peer network. Any time a bitcoin transaction occurs, the relevant data emanates throughout the Bitcoin network from the transaction's point of origin to all users currently attached to the network. The basic data for the transaction include an address (think of it as an account number) for the person sending the bitcoins, an address for the person receiving them, the number of bitcoins in the transaction, and authenticating information. The authentication, both of individual transactions and of the general ledger, the blockchain, relies on concepts from the science of data cryptography (hence the term "crypto-currency.") Each individual transaction record contains a digital signature derived from a private key, which, hopefully, only the sender knows.[2] One purpose of the encryption is to authenticate the signature while preserving the privacy of this key.

Using existing cryptographic techniques to validate digital signatures on individual transactions is clever, but it doesn't avoid the need for centralized clearing or record keeping. That's because with a widely distributed network, a user could attempt to spend the same bitcoin several times before the whole network caught up with the original transaction. At that point it would become impossible to tell which was the original, and

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" available at https://bitcoin.org/bitcoin.pdf. "Satoshi Nakamoto" is a pseudonym, and "Satoshi's" true identity remains a closely-guarded secret. It's not at all clear whether "Satoshi" is an individual or a group of people. The paper looks like an academic working paper, such as a researcher might circulate professionally before submitting it for publication in an academic journal.

[2] A more complete description of bitcoin transactions is at http://www.coindesk.com/information/how-do-bitcoin-transactions-work/. The Bitcoin Foundation's site, bitcoin.org, also gives a good deal of background.

therefore valid, transaction, and it would be impossible for the putative recipients of the duplicate transactions to recover the bitcoins they thought they had received.

The most ingenious part of the design of Bitcoin is the process by which users — not a centralized party — validate transactions and commit them to the permanent general ledger, the blockchain. This is the role of the bitcoin "miners." Any bitcoin user can become a miner. All it takes is a suitable hardware rig, the right software, and the willingness to pay for the power to run them. As transactions occur and users broadcast them to the Bitcoin network, miners pick them up and assemble them into blocks. The miners verify the transactions by comparing them with the existing account (address) balances implicit in the blockchain history, and then apply a cryptographic algorithm in an effort to be first to create an encoding[3] of the new block of transactions that meets a specific set of requirements.

Running the encryption algorithm isn't particularly hard, so the Bitcoin protocol adds a "proof of work" test to increase the effort the miners have to expend. To validate a block, the encoding must meet an arbitrary format requirement — it has to start with a minimum number of zeroes. The raw data of the block won't produce that result, so miners have to find a string of nonsense data, called a *nonce* in cryptology circles, to add to the block such that the encoding of the block, plus the nonce, meets the requirement. Since a robust cryptographic encoding algorithm makes it impossible to reconstruct the original data from the encoding, the only practical way to generate the required result is by the brute-force method of successively guessing a nonce, calculating the encoding, seeing whether it works, and if not, going back and guessing another one.

Eventually, a miner will hit on a nonce that produces the required encoding. That miner broadcasts the result to the network, adding the newly mined block to the end of the blockchain. The successful miner also receives a reward (a bounty, really) of newly created bitcoins, along with any transaction fees that users sending bitcoins have offered to induce to miners to prioritize their transactions.

The Bitcoin protocol includes two parameters intended to smooth the functioning of the network. The first is the computational difficulty of meeting the encryption format requirement. As more miners apply more power, they naturally verify blocks quickly. If they're too quick, the protocol increases the number of initial zeroes required for a valid solution, increasing the difficulty of mining. The basic goal is to keep the average time interval between successes, and therefore between successive blocks, at about ten minutes. The second parameter is the size of the bounty successful miners receive. Currently, that

[3] This encoding is known in cryptography-ese as a *hash*, and the encoding algorithm is the *hash function*.

bounty stands at 25 bitcoins, worth around $14,000 at prices bitcoin exchanges[4] are quoting. The protocol includes a schedule decreasing the bounty as the total number of bitcoins accumulates. It will fall to zero when about 21 million bitcoins exist, and miners would then have to rely entirely on transaction fees, or stop mining.

Formally, once a miner broadcasts a solution for a block, that doesn't necessarily completely close the book on the block. The network as a whole — actually, as a collection of individuals — has to accept the mined block, and hence the extended blockchain, as valid. A miner accepts a new block as valid by beginning to work on the next block in the chain. The basic rule is that the longest existing version of the blockchain is the "real" one, but if enough miners chose to regard another miner's block as invalid, they could ignore that block, go back and rework it, and then overtake the first miner's version of the blockchain by successfully solving the next block. For that reason, Bitcoin advocates sometimes caution users to wait for several blocks to pass before regarding their transactions as irrevocably recorded.

So How Can I Play?

Because of Bitcoin's technical complexity, many of its earliest adopters were technically savvy individuals, who prize its use of modern data communications and cryptography. Bitcoin also holds strong appeal for people that harbor an instinctive mistrust for both governments and financial institutions, since Bitcoin generally avoids interacting with either. Since it facilitates cash-like transactions online, it has also attracted interest from those that see its potential for dealing in illegal goods and for money laundering. And the volatility of bitcoin's price in conventional currency, along with its rapid rise in price last fall, has attracted the interest of speculators.

For others, the complexity and unfamiliarity of Bitcoin may be rather daunting. You could participate directly by downloading the Bitcoin protocol software (the "bitcoin client") and the current blockchain, and then offering your computer and internet connection as a node on the peer-to-peer network operating Bitcoin. That would involve maintaining an open, two-way connection to the outside world all (or at least most) of the time, which might not strike you as especially secure. And unless you are also mining, the problem of how to obtain bitcoins remains.

If you do want to buy, trade, or use bitcoins, you need a bitcoin wallet. The wallet itself doesn't actually hold bitcoins — it merely holds an address to which a bitcoin holder can send bitcoins in a transaction. Your ownership of those bitcoins is nothing more than

[4] Bitcoins, of course, aren't convertible into conventional currency unless someone is willing to trade one for the other. Quoted prices vary rather widely.

the end result of a chain of records in the blockchain. To do anything with them, you need to know both that address and the private key I mentioned earlier. The wallet address is public; it has to be, or no one could ever send you bitcoins. You use the private key to "sign" transactions when you send your coins to someone else. The private key is the part you have to keep secure. You could store it on your computer (not ideal), on your phone (even less ideal), on a thumb drive (probably better), or even written down on a piece of paper (but don't lose it, or make a mistake copying it). Downloading the bitcoin client program to set up your computer as a node on the peer-to-peer network would give you your first wallet, but engaging the services of one of a growing number of firms that facilitate retail customers' use of Bitcoin is much easier. These firms are the wallet services and exchanges.

Wallet Services and Exchanges

Aside from mining, there are really only two ways to obtain bitcoins — by buying them for conventional currency, or accepting them in payment for goods or services. In principle, you could buy bitcoins for currency by meeting a current holder at a coffee shop, handing over the cash, and watching that person use a smartphone or laptop to enter a transaction sending bitcoins to a wallet you control. But if you're interested in having a little more security for your bitcoin transactions, you'll probably end up opening an account with an online bitcoin seller and wallet service or with a bitcoin exchange.

The online wallet services and exchanges have emerged as the main interface between the conventional currency economy and the Bitcoin economy. These firms appear superficially similar, but they have a range of business models. The exchanges, for example, match buyers and sellers. Other firms offer services that range from simply providing technology, to facilitating storage of bitcoins, to buying and selling bitcoins from their own inventory. Several of these firms facilitate the trading of bitcoins for conventional currency through links with traditional banks, from which customers transfer the cash they will need to pay for their purchases of bitcoins.

Because Bitcoin is a product of the internet age, bitcoin wallet services and exchanges generally have little physical presence, but do nearly all their business online. For the most part, they seem to try to give their services the familiar look and feel of online banking and brokerage. Some advertise reputable names among their backers, but others rely on a more organic, web-based process of building market awareness and reputation. The most notorious of the bitcoin exchanges is MtGox, which called itself "the world's most established Bitcoin exchange" before it abruptly went offline. MtGox started as an online exchange for the trading cards central to a fantasy game called Magic: the Gathering. The name originally stood for Magic: the Gathering online exchange.

MtGox suspended customer withdrawals of both bitcoin and conventional currency balances during the week of February 17, 2014, and shut down all of its website's functionality on February 25. As I write this, press reports are indicating that nearly 850,000 bitcoins that MtGox was supposed to be holding may be missing. Bitcoin cognoscenti now pronounce it "Empty Gox," not "Mount Gox."

Bitcoin in the General Economy

MtGox's travails illustrate a key issue in the development of the Bitcoin economy. The issue is not with the basic Bitcoin protocol, the process of transferring bitcoin balances between addresses, or the system for verification and mining. Rather, the problem lies with the service economy that has been growing up around Bitcoin. Wallet services and exchanges facilitate the purchase and use of bitcoins by individuals that prefer not to invest the time or capital necessary to participate directly in the network. In serving their customers, these firms sometimes act as custodians in the way your bank or broker does, taking possession of their customers' bitcoin positions. Just as with a bank or brokerage account, what the customer holds is a statement representing a claim against an asset (in this case, bitcoins) the exchange holds in a "house account" — a bitcoin address that it controls. The exchange takes responsibility for safeguarding the asset, or in this case, the private key, and the customer taps that asset by notifying the exchange, which makes payments from its house account and adjusts the customer's balance.

We take for granted the mechanics of ordinary banking and brokerage transactions, but they take place in the context of a well-developed operational infrastructure, and proceed according to a well-developed set of regulations and industry practices. Banks and brokers operate under rules requiring strict segregation of their customers' assets from their own. They are subject to stringent operational, audit, and regulatory examination requirements. As we know, banks and brokerages still sometimes fail, but when they do, we have a clear idea where to turn for recourse, and in many cases we enjoy the benefits of deposit insurance.

Bitcoin proponents hasten to assert that MtGox's failure is not a failure of Bitcoin itself. They point out that if those 850,000 bitcoins really are missing, they haven't just evaporated. Somewhere in the blockchain are records of the transactions that siphoned them away from MtGox. That suggests that a systematic audit of MtGox's own books, reconciling them with the public blockchain, could have prevented what appear likely to be large customer losses. Such an audit process undoubtedly would include novel forensic tests, unique to the crypto-currency world, but the principles would be the same as the ones that govern conventional financial institutions.

Having been burned (or "Goxed," as many are now saying), bitcoin holders are now realizing that the verification-only model embedded in the blockchain does not by itself make every Bitcoin-related transaction trustworthy. If Bitcoin is to have a useful purpose in the broader economy, services like the exchanges will be necessary to make Bitcoin more accessible to the general public. That public will only embrace those services if they have confidence that those services will perform as promised. That will require the creation of an institutional framework that Bitcoin users come to trust.

To date, however, the discussion on Bitcoin message boards seem to run to mining, trading, and blue-sky speculation, and less to the nuts and bolts of banking and audits. If Bitcoin is to gain broad acceptance and become integrated into the broader economy, the institutional arrangements connecting wallet services, exchanges, and the like to the broader banking and payments system must become stronger. Safeguards against fraud, theft, and money laundering must rise to the standards of the conventional banking system. Retail holders of bitcoins must be able to take possession of their holdings as easily as we now withdraw bank deposits. And firms that take custody of customer holdings must subject themselves to the levels of financial controls and auditing that we expect in the banking and brokerage system.

In other words, Bitcoin's aspiration to avoid the need for trusted intermediaries is a vain hope. The Bitcoin protocol provides a means for perfecting and verifying individual transactions without the intermediation of a central authority, but integrating bitcoin into the daily life of the broader economy would require establishing a system of trusted intermediaries, subject to conventional controls, and operating in tandem with the conventional banking and payments system.

– Jonathan Tiemann
Menlo Park, California
February 28, 2014

Tiemann Investment Advisors, LLC is an SEC-registered investment advisor based in Menlo Park, California. For more information, please send your request to information@tiemann.net or visit www.tiemann.net.