What is Bitcoin?

Strengths and weaknesses of the leader in a new generation of emerging cryptocurrencies.

By Dominic Hobson

DOI: 10.1145/2510124

Control over your personal data is an important part of privacy. The Web enables personal data to be gathered, shared, and traded with unimaginable ease, and keeping a firm grasp on personal data is becoming more and more challenging.

One motivation for the mass movement of personal data around the Web is money. Before the advent of the Internet, sending money from one side of the world to the other was not as straight forward a task as it is today. But, just like personal information, the transfer of money enabled by the Web has big implications for privacy. As we have moved from cash, to checks, to credit cards—away from physical gold standards—our money has gradually become just numbers on a computer. Inevitably, that computer belongs to someone else.

Privacy, that is, the ability to be able to reveal personal information through choice, is near impossible to attain when a third party holds all your money, personal information, as well as every electronic transaction you've ever made. Part of the motivation for creating the Internet was resilience to attack through distribution with as few single points of failure as possible. Despite having such a system, users have still flocked en masse to centralized services such as PayPal. With respect to privacy, we have given all our control; our personal data regarding our transactions; our balances; and who we pay, why, and when over to a few large centralized services.

For some, this shift of monetary control has its benefits. In theory, your money is safer in a large organization's virtual vault than under your bed. For others, this hand over of monetary control has been more costly: Searching for the phrase "PayPal took my money" brings back literally millions of results.

As well as possession of money, centralized services also get possession of personal data relating to purchases. Supermarket chains can—and do—infer age, gender, household salary bracket, and more from the items you purchase in their stores to aid marketing and advertising efforts. In 2011, Visa announced a system called "Real Time Messaging," which sent offers and discounts direct to phones based on information deduced from card use, such as location.

These are just a few examples of how large companies are using personal data related to your payments and transaction to target advertising and sell more efficiently. Many people may be comfortable with this. After all, if somebody is going to try and sell something to you wouldn't you rather it be something relevant to you, which you might actually want? However, there is virtually no alternative to holding money in a bank or other centralized services—which in turn buy, sell, and profit from your personal data.

Enter Bitcoin, a pseudo-anonymous, peer-to-peer currency protocol created and released, quite fittingly, by a mysterious pseudonym, "Satoshi Nakamoto," whom has since disappeared. Bitcoin is the leader in a new generation of emerging currencies known as "cryptocurrencies," which aim to, among other things, facilitate the movement of money electronically while still maintaining a sense of privacy. Bitcoin disrupts this move to centralized money services, putting the Internet to the use for which it was originally intended—fully decentralized services.

It's been suggested that by printing our names and details on our debit and credit cards we undermine thousands of pounds of smart chip, which is a privacy enabling technology. Unfortunately the biggest group of people helped isn't ourselves, but those with nefarious intent. It begs the question that in a system where everything and everyone is represented as numbers on a computer, do we even need a name? It is this approach that gives the Bitcoin protocol one of its many strengths.

BREAKING DOWN BITCOIN

The Bitcoin protocol itself stores no personal data. Bitcoin offers its privacy by design through novel use of cryptography. Nothing personally identifiable is recorded. Instead, users have many wallet addresses, which are hashes of public keys. Users can, and are encouraged to, have as many different wallet addresses as required (ideally one per transaction). The corresponding private keys, required to authorize a transaction, are stored locally in the users wallet file.

Users maintain full control and possession of their local wallet file. But "with great power comes great responsibility." Should a user accidentally delete or lose their wallet file, they also lose any associated bitcoins. Although the bitcoins are still technically stored on a peer-to-peer network, the private keys required to authorize a new transaction are lost, effectively making the coins unspendable.

Behind the scenes, Bitcoin doesn't store each coin and who owns it. Instead, it uses a distributed ledger book system (called a "blockchain") based on the logic that if you know every transaction an address has made, then you know if it has money to spend. This may appear initially quite contradictory: A privacy protecting money system that lets the entire world see every transaction ever made. However, from a privacy perspective, it doesn't matter if everyone can see every transaction, if the only identifying information in a transaction is a seemingly random number of which everyone can have many.

Transactions are verified through a process known as "mining." The mining process also serves as the mechanism by which bitcoins are initially produced and distributed. Mining is effectively the act of adding transactions to the blockchain so everyone can agree on the same set of transactions. A node that chooses to mine runs mining software, which repeats the following:

1. Gather up all unverified transactions into a block (ensuring they're all valid transactions) along with the hash of the last block added to the blockchain and a random number called a "nonce."

2. Hash this block. Look at the newly produced hash, specifically how many zeros it starts with: (a) If the number of leading zeros is less than a predefined number (known as "difficulty") then start again from step 1, incrementing the nonce to ensure a different hash is reached. (b) If there are more leading zeros than the required difficulty, then proceed to step 3.

3. The miner has successfully mined a block, adding it to the blockchain. They then broadcast their hash, along with the transactions in it and the nonce to others. The successful miner also receives newly created bitcoins as a reward in a special coin base transaction—this is how bitcoins are initially produced.

4. Other miners receive the new block and its contents. They check that all transactions in the block are valid and not double spends, and check that when hashed, they give the right result. If everything is valid, they use the new block hash and start to mine the next block with new transactions.

The mining process is effectively trial and error. As more people try mining, they would in theory be able to mine blocks more quickly. For this reason after every 2,016 blocks that are found (which happens approximately every two weeks), the predefined number of leading zeros that must be in a hash for it to be successful (the difficulty) is adjusted. This is based on the average time it has taken to mine a block. If this time is more than 10 minutes, the difficulty is decreased. This effectively restricts the mining process to a block every 10 minutes.

Bitcoin disrupts this move to centralized money services, putting the Internet to the use for which it was originally intended—fully decentralized services.

The reward a miner receives for finding a block is the sum of the transaction fees of all the transactions in that block, as well as a block reward that is currently 25BTC. This reward halves every four years, so no more than 21 million bitcoins will ever be produced. The aim of this is supposedly to mimic a finite resource such as gold. With 3,600 bitcoins being produced a day and each bitcoin worth around $100, mining has become an industry and profession itself.

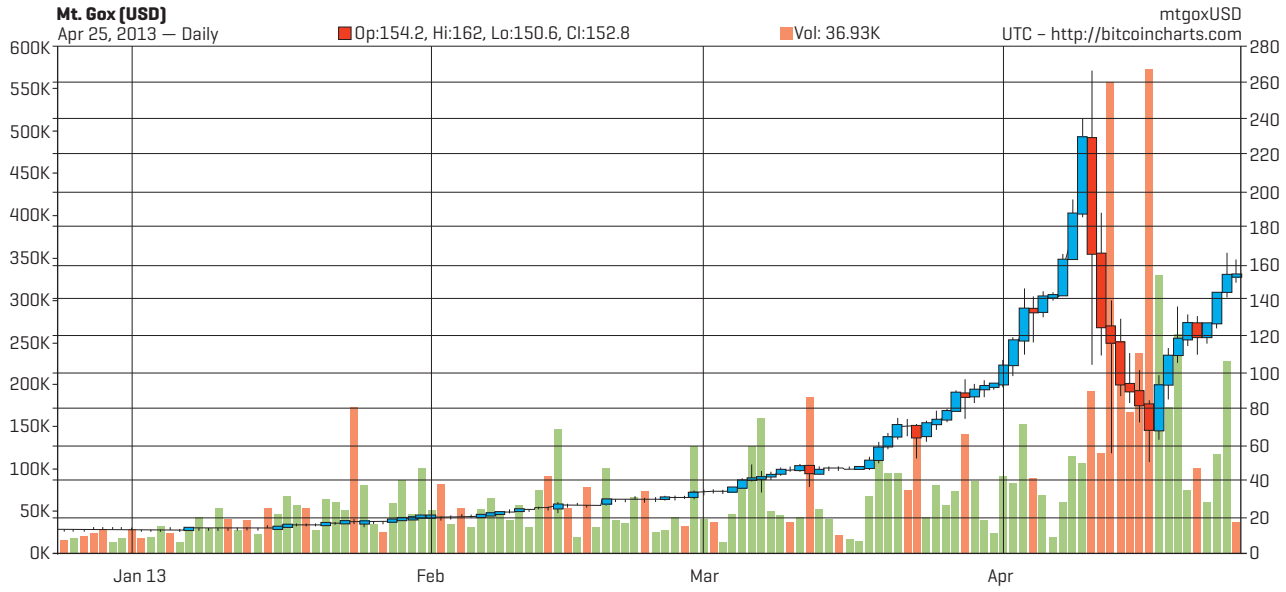
Miners typically invest thousands into their mining rigs in order to hash just a little bit faster in hope of finding a block before another miner does. People are even going as far as creating Application Specific Integrated Circuits (ASICs) that can cost tens of thousands of dollars each for the sole purpose of mining. For Bitcoin users, the more people mining and hashing, the more secure and resistant the blockchain is to attack.

To attack the network, a malicious actor would have to create or modify a transaction in a block and mine it faster than the rest of the entire network can mine a block. Mining faster than the rest of the network on average requires the same or more hashing power than the entire network combined, which is currently hovering at around 1500 petaFLOPS (floating point operations per second). To put that in perspective, Tianhe-2, the world's fastest supercomputer, has managed to muster a measly 31 petaFLOPS and theoretically maxes out at just 54.9 petaFLOPS.

Even if an attacker could acquire such power, malicious transactions must still be accepted as valid by other miners. With more than 50 percent of the network power, a malicious actor can only prevent transactions, and reverse or double spend transactions. Should a malicious party have more than 50 percent of the hashing power, they would earn more by legitimately mining then they could with fraudulent transactions.

Ultimately, providing you look after your wallet, your bitcoins are safe, unless somebody manages to break the military-grade cryptographic algorithm ECDSA (Elliptic Curve Digital Signature Algorithm). Even if this

Figure 1: The price of a bitcoin at the largest exchange, MtGox, in the first four months of 2013 in dollars.



were to happen, rolling out a new client and switching over to a new blockchain (called a "hard fork") would solve the problem. Even a full break in ECDSA would have little to no implication for privacy of Bitcoin as there is still no personal data stored within the protocol.

WEAKNESSES OF BITCOIN

So with such secure algorithms, what makes Bitcoin only pseudo-anonymous? One reason is that Bitcoin can't guarantee that users will not somehow accidentally or intentionally link themselves to a wallet address. For example, let's assume Alice published a wallet address of hers on Twitter for donations and received 20BTC. By looking through the blockchain, anyone can find the addresses that Alice sent her money to, and it's more than likely Alice knows the people she sends money to. Alice may wish to support a controversial group and anonymously donate. She naively sends money to an address the group posted on their Twitter feed. Anyone looking up Alice's donation address in the blockchain would only have to Google the addresses she sent bitcoins to in order to link her with the controversial group.

All the above could have been avoided if either party had used a script to automatically generate a new Bitcoin address for each individual. Unfortunately, the vast majority of the population probably doesn't know how to do that. A potential flaw in Bitcoin, as it stands, is that it is so incredibly novel and ingenious; it's not yet intuitive or easily understandable for most of the population. How can someone be expected to trust something new that they don't understand? Bitcoin was originally created and used by people with a technical disposition, so its lack of ease of use is most likely a feature of being a first generation cryptocurrency.

There are already clones of Bitcoin being created using the Bitcoin source code as the base. Although none of these improve the usability, they do offer variations in block production time and rate. Some of these "altcoin" clones offer mining algorithms that are considered fairer by hashing blocks with the Scrypt algorithm. Producing a hash using the Scrypt algorithm is more memory intensive than SHA256 and as a result doesn't benefit as much with mass parallelization provided by more expensive hardware such ASICs. Some altcoins use a variation of Bitcoin's proof of work algorithm, making them in theory more resistant to a 51 percent attack.

However, these clones still share some of the same weaknesses as Bitcoin. In order to cash out Bitcoins into a fiat currency such as £ or $, typically one must go through an exchange. The price of a Bitcoin varies. In the first four months of 2013, the price of a bitcoin went from $20 to more than $250, down to $60, and back up to $160 (see Figure 1). Such volatility is unheard of in fiat currencies and has brought Bitcoin's value as a standalone currency (i.e., not pegged to a fiat currency) into question.

Such volatility can lead to practical issues. For example, let's assume a mining hardware company accepted preorders in bitcoins on equipment worth $30,000. After missing shipping dates, some customers requested refunds. However, when some customers paid in bitcoins, the value of a bitcoin was as low as $20, whereas now they're worth more than fives times that amount. If the company has to pay back customers with the amount of bitcoins the customer paid, then they will be paying the customers more than fives times the dollar equivalent they originally paid. However, paying out the dollar value to the customer in bitcoins is also not fair, as the user will end up with considerably less bitcoins than they had before they bought the product.

The volatility of Bitcoin can be at least partially attributed to the fact that nobody really knows the intrinsic value of a bitcoin. It's been suggested there is a loose correlation with price of electricity since the act of mining uses a significant amount of electricity—one source suggests the amount of electricity put toward mining bitcoins for a single day is enough to power more than 30,000 homes. There was also speculation that the rise in price of Bitcoin early this year was linked to the Cyprus bailout. Cypriots with more than 100,000 EUR had money taken from their accounts in order to support the country. This wouldn't have been possible if Cypriots stored their money in bitcoins. However, traffic figures from exchange websites where bitcoins can be purchased suggested no notable increase in traffic from Cyprus. Other things that seem to affect Bitcoins volatility include media coverage, Bitcoin services being hacked, and downtime on popular services.

The more money that goes into Bitcoin, the more stable it is likely to become as the currency finds its value. The Winkelvoss twins—famous for claims that Mark Zuckerberg stole their idea for Facebook—recently announced they had invested $11 million in Bitcoin, giving them, at the time, 1 percent of all bitcoins in circulation. While this amount of investment is useful in some respects, with Bitcoin being a relatively small market, individuals with such large amounts could still sway the price at the exchanges.

Furthermore, the exchanges where bitcoins can be purchased and sold are not a part of the Bitcoin protocol, so they may not be as safe. This has big implications for privacy and security. Anyone can run an exchange, regardless of his or her competence, knowledge, reliability, or trustworthiness. Most exchanges are websites where a fiat currency or bitcoins are deposited, and then converted to numbers in a database. This subjects them to the same vulnerabilities as other websites, making them a target for hackers. A lot of articles in mainstream media relating to Bitcoin have focused on hacks at the exchanges and rarely make a distinction between the exchanges and the Bitcoin protocol itself.

A potential flaw in Bitcoin, as it stands, is that it is so incredibly novel and ingenious; it's not yet intuitive or easily understandable for most of the population.

Unlike the Bitcoin protocol, these exchanges are ultimately centralized: Backed and run by people against whom laws can be enforced. In most jurisdictions, exchanges are subject to "anti-money laundering" laws that require certain kinds of businesses to "know your customer" (i.e., know as AML/KYC regulations.) This involves formally identifying customers through official documentation—typically passports and utility bills—presenting yet another place where a Bitcoin wallet address can be related to a real world identity.

In reality, Bitcoin offers enough anonymity for it to become inefficient for authorities to pursue a person for small scale and minor crimes. As a result, Bitcoin has been used for trading in illegal goods and services online. Perhaps the most notable case, which was the focus of most Bitcoin related media attention in 2011, is Silkroad, described as the "Amazon marketplace of drugs." Silkroad operates on the anonymizing network Tor, and allows users to buy and sell drugs, guns, guides on hacking, forged documents, and more—all paid for in bitcoins. In 2012, research into Silkroad suggested an average of just more than $2 million worth of bitcoins a month went through the site. There are typically between $30 million and $70 million in transactions a day with bitcoins, so it's important to remember Silkroad's $2 million a month makes up just a tiny fraction of trades that take place with Bitcoin.

The protection Bitcoin provides is a strength and a weakness. On one hand, many of the things on sale on Silkroad were legal in some country somewhere in the world. A libertarian might argue people should be allowed to buy and sell what they want with their money. On the other hand, trade in guns, particularly on a black market like Silkroad, can severely impact the lives of others and attract negative attention from the press and public.

It's important to emphasize cryptocurrencies are effectively tools, and tools on their own do not break laws. Paper cash, for example, shares many of the features of a cryptocurrency—relatively anonymous, fast, and peer-to-peer—yet it is a valuable part of society. Although the way people use tools can be illegal, a lot of media attention around cryptocurrencies focuses on their illicit use, effectively labeling and criminalizing those who simply want some privacy, or a useful service.

THE FUTURE OF CRYPTOCURRENCIES

Like most privacy enabling services, Bitcoin serves its purpose when understood and used properly. However, the novel nature of Bitcoin can make it hard to grasp properly. Regardless of privacy, Bitcoin provides users with ultimate control over their money, and allows fast and secure transfers around the world with transactions fees lower than virtually all-existing alternatives. As a first-generation cryptocurrency, it still has its quirks and is ultimately reliant on third-party services, which are not yet mature enough to offer the same strengths as the protocol itself. The shallow but rapidly growing market around Bitcoin creates a level of volatility that can make Bitcoin a bit of an inconvenience in some cases. But it's still most likely the first of many emerging systems that will force us to fundamentally rethink how our money and the associated private data should be handled in the age of the Web.

Biography

Shaped by daily access to the Web from the tender age of five, Dominic Hobson has spent his life on and around the Web. After completing a degree in computing science at University of Wales, Bangor, he went on to Southampton to complete a master's in Web science, looking at criminal use of virtual payment systems. Still at Southampton, Hobson is now working toward a Ph.D., studying cryptocurrencies and their surrounding communities.