The problem with Bitcoin

Danny Bradbury

Danny Bradbury, freelance journalist

The Bitcoin network was launched in 2009 by the mysterious Satoshi Nakamoto, a developer who worked extensively on the project but only interacted with people on developer forums. At the end of 2010, Nakamoto disappeared from view, announcing his departure and handing off the project to the open source community. No one knows his (or her) true identity, but what is known is Nakamoto's wealth. He is said to have roughly $100m worth of bitcoins by today's value, and hasn't spent any of it.

Reinventing money

Bitcoin is a crypto-currency, designed to reinvent the way that money works. Money started as the exchange of commodities, such as silver and gold. These commodities had at least one of the properties of money – you can trust them. But they are difficult to transport and maintain. Fiat currency was designed to solve some of those problems. It still carries trust, (they don't call it the almighty dollar for nothing), and it has some liquidity. But it is inflationary, fragmented and increasingly difficult to move around, thanks to heavy banking fees and transfer regulations. When it can take tens of dollars simply to move money from one country to another, argue Bitcoin supporters, something is broken.

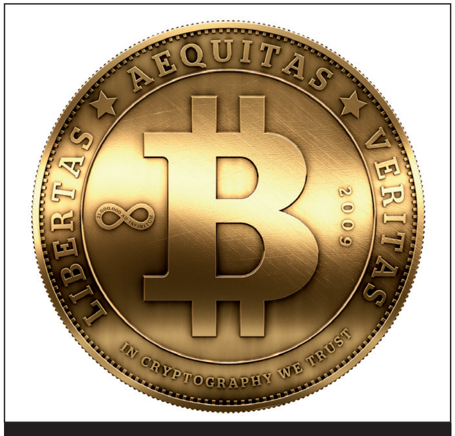
"Mathematics has trust embedded into it – mathematical proofs are irrefutable. Mathematics is also transparent (unlike much of the banking system), making it a good vehicle for the potential storage of value"

After the 2008 financial crisis, the trust inherent in money also began to erode. The actions of the Central European Bank in Cyprus in April 2013, when it moved to appropriate bank deposits to alleviate national debt, bought distrust of conventional currencies to critical levels. Now, those same rules look to be a central tenet of European banking policy.[1]

In contrast, mathematics has trust embedded into it – mathematical proofs are irrefutable. Mathematics is also transparent (unlike much of the banking system), making it a good vehicle for the potential storage of value. And mathematics has ultimate utility: unlike gold, equations and solutions are inherently portable. They don't need careful hoarding or protection. If you stack equations together then, unlike gold bars, they do not compress each other and buckle under their own weight. Nakamoto's paper described a mathematical system that could be used to produce and manage a monetary system, and he called it Bitcoin.[2]

How Bitcoin works

In the Bitcoin network, money isn't printed, it is 'mined', using widely distributed computing power. The 'miners' are operated autonomously by members of the network, using software built to support the initial algorithm. The system's elegance lies in the fact that in producing bitcoins, the mining network also processes the exchange of bitcoins between holders of the currency.



Bitcoin has grown in popularity in the wake of the global financial crisis.

"Because there is no central processing authority for bitcoins, in the same way that there would be for PayPal or a banking transaction, transactions must be confirmed by consensus"

Bitcoins are sent and received via Bitcoin addresses, which are long, alphanumeric strings understood by the network. Any person dealing in bitcoins can use any number of addresses – they are easy to create.

When a bitcoin is sent from one address to another, the transaction is collected by the network. However, that transaction must be verified. Because there is no central processing authority for bitcoins, in the same way that there would be for PayPal or a banking transaction, transactions must be confirmed by consensus. They are collected into logical entities called 'blocks'

The miners must process these blocks by hashing together all of the transactions in the block with a time stamp using a cryptographic function (in Bitcoin's case, it's SHA-256), effectively producing a signature for that block, and 'sealing' it, in the same way that a period of book-keeping records might be locked and sealed.

The hashed block is then added to a serial chain of block hashes, known as the blockchain. This blockchain becomes a record of every transaction that ever took place on the Bitcoin network, preserving Bitcoin's transparency. The blockchain also includes a clever integrity measure: when each block is hashed, the hash from the previous block is also included in the function. This ties each block to the block before it. If someone wanted to go back and create a fraudulent block in the hash chain to obfuscate a transaction that happened in the past, they would have to recreate false versions of every block following the altered block.

This wouldn't be impossible, save for one other important feature of Bitcoin – proof of work. Hashing a set of transactions and another alphanumeric hash is computationally simple, even a smartphone could do it in seconds. But Bitcoin makes it computationally difficult to hash a block, by requiring that the resulting hash have specific numeric properties. This makes the miners work harder.

It isn't possible to choose the hash resulting from a predefined set of numbers (the transactions, the timestamp, and the previous block's hash). The SHA-256 algorithm determines that. So another, unknown string is required to modify that resulting hash, giving it the required properties; but no-one knows which string is needed to ensure that the final hash has the right format. This means that miners have to try many strings until one works. That takes considerable computing power. The strings that are tried are called nonces.

All of the miners on the network compete to find the right nonce and produce a block hash in the required format. This is known as solving the block, and miners must be connected to the network while they do it, so that all participants are in sync. When a miner solves a block, it gets a reward, which at the time of writing is 25 bitcoins. It can be difficult for a single miner to solve a block, so many of them now connect in pools, combining their hashing power to solve a block and then distributing the reward.

Danger of attack

On the surface, the decentralised nature of the network protects it. Decentralised systems can better protect themselves against attack, and route around damage. Compare this to problems when banking systems go down. Last year, RBS customers suffered when the bank's systems failed.[3] But there are nevertheless theoretical attacks on crypto-currency networks such as Bitcoin, and many of them have been proven practically. One example is the 51% attack.

"If the attacker sends bitcoins to a recipient in exchange for a product or service, it could then record that it had sent the same bitcoins to another Bitcoin address that it controls"

Bitcoin measures the level of computing activity on the network in terms of the hash rate. Should one miner or pool of miners gain control of 51% of the hash rate, then they would theoretically be able to solve their own block of transactions. The 51% attack also results in a fork, which is where there are two conflicting blocks vying for addition to the blockchain.

Jeff Garzik: "It is trivial for a mining hardware owner to switch mining pools and that helps keep individual mining pools from gaining power."

Because the majority of mining power on the network would support the attacker's block, it would be sent to the blockchain. The attacker's block could include fraudulent transactions, designed for financial benefit. For example, if the attacker sends bitcoins to a recipient in exchange for a product or service, it could then record that it had sent the same bitcoins to another Bitcoin address that it controls, in its own block. Bitcoin transactions are irreversible, so this lets the attacker spend the bitcoin twice, in what is known as a double-spending attack.

Mitigating factors

There are mitigating factors that make it difficult to mount a 51% attack, says Jeff Garzik, one of the core developers of the Bitcoin protocol. "I always tell people that's at the bottom of my list," Garzik says. "The mining pool community is very robust, and mining software, for example, is already programmed to automatically switch between mining pools. It is trivial for a mining hardware owner to switch mining pools and that helps keep individual mining pools from gaining power."

Other things that can help to thwart such attacks are that the network generally needs six confirmations of a transaction (each in a separate block). This can make it less likely for someone to get fake transactions accepted and confirmed permanently in bitcoin.

The ongoing decentralisation of miners, as more people get involved, is helping too, along with the dramatic increase in network hash rate in recent months as Bitcoin has gained traction. Large hash rates make it far more difficult to mount enough processing power to grab control.

Those large hashrates are coming, however. Bitcoin miners began by using home computer CPUs before graduating to graphical processing units (GPUs). GPUS are famously good at mathematical heavy lifting, thanks to their floating point capabilities. Now, however, a new phase is approaching in Bitcoin mining – application-specific integration circuits (ASICs). These offer an order of magnitude greater capability than GPUs, but they are difficult and expensive to fabricate, meaning that supplies only began coming on stream in the summer of 2013. KnCMiner, which is preparing 28nm ASICs, planned to balloon the network hashrate from 155 Terahashes per second to around 600 in two months when it begins shipping its first units during September and November 2013.[4] It's too soon to say if they've succeeded.

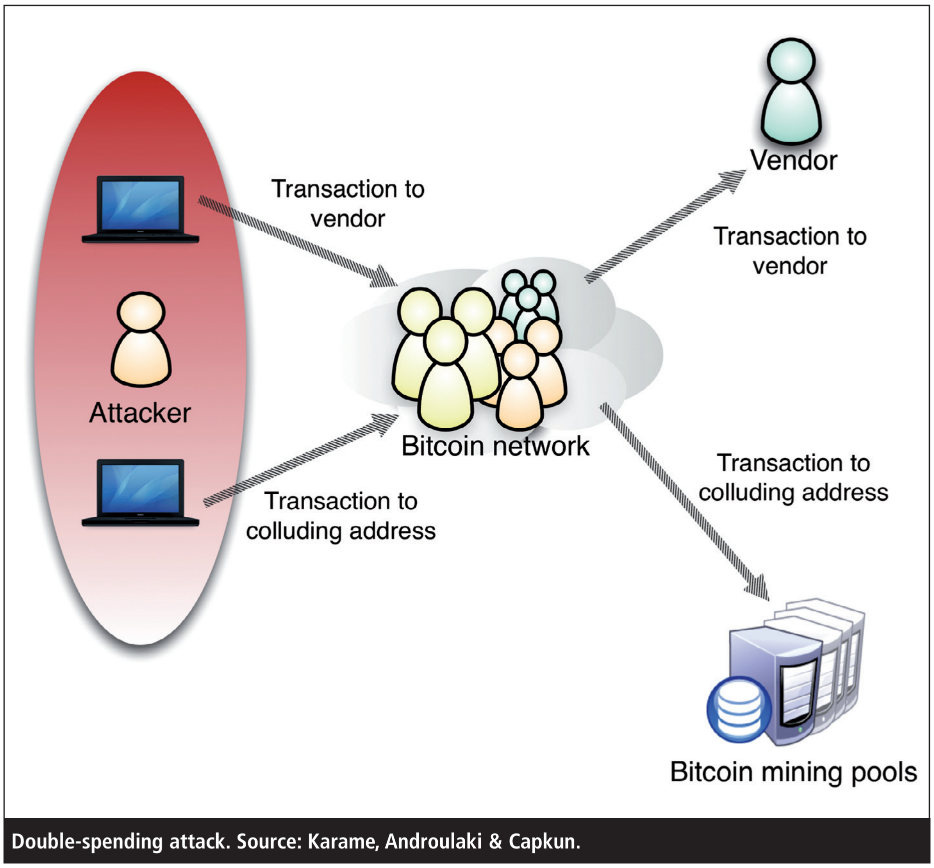
However, 51% attacks can plague other, smaller currencies. In early June 2012, Feathercoin, an alternative currency based on Litecoin, suffered a 51% attack after malicious parties gained control of its chain and 'orphaned' 80 blocks. Its hash rate was only .02 Gigahashes per second, and the attack took it to 1.2 Gigahashes per second in short order.[5]

Double spending

Double-spending attacks are also mountable in other ways. Given that a block takes around 10 minutes to mine, getting even one confirmation of a transaction can take that long. This is why zero-confirmation transactions are encouraged – people simply don't want to wait.

"It is noteworthy that we have performed thousands of double-spending attempts using fixed Bitcoin addresses without having to bear any type of penalty"

This can facilitate a double-spending attack without the significant computing overhead required for a 51% attack.



Double-spending attack. Source: Karame, Androulaki & Capkun.

Researchers from NEC Laboratories and ETH Zurich have shown that it is possible to successfully double spend by broadcasting a fraudulent transaction to a large number of nodes in the network, while also sending the genuine transaction to the service provider in exchange for an immediate service or product. The large number of nodes receiving the broadcast causes the network to assume that the much-publicised fraudulent transaction should be accepted into the block, instead of the little-known genuine one.

"It is noteworthy that we have performed thousands of double-spending attempts using fixed Bitcoin addresses without having to bear any type of penalty," say the researchers.[6]

Dust transactions

These attacks all make it possible to manipulate the network for personal gain, but there are other categories, too. Denial of service attacks can be used to compromise the network. There are several possible attacks. One involves 'dust' transactions – very small transactions that send hardly any bitcoins, but which take up space in the blockchain.

The minimum fraction of a bitcoin is one Satoshi, which is 0.00000001 bitcoins. It was previously possible to send one Satoshi over the network, which is equivalent to $0.00000112 at the time of writing. It was therefore possible to send large numbers of these transactions, which will fill up blocks in the blockchain. Because each block increases the length of the blockchain, it can end up bloating the chain, which is already becoming increasingly unwieldy. In June 2013, the blockchain reached 8GB in size.[7]

The core development team's answer to this was a patch that limited the size of transactions in the network. Thanks to a new version of the client, a minimum of 5,430 Satoshis can now be sent. At current values, that's still around six-tenths of a cent in US Dollar terms, but it still makes it far harder to mount a successful dust spam attack on the blockchain.

Code-based attacks

What's left? The other potential attack lies within the client's code itself. According to core developers that spoke with him via online forums, Nakamoto spent at least a year thinking conceptually about the network before coding it. The source code for the network, Bitcoind, is known as the 'Satoshi client'. It is still in use today, and is maintained by a core group of open source developers via Github.

"The developers are adding features to the Satoshi client, and a bug may slip that could be used to attack the network," says Sergio Lerner, a cryptography expert who searches out vulnerabilities in Bitcoin. "Many people read the source code before a release, but security vulnerabilities are sometimes not easy to spot."

We have seen some of these attacks surfacing already. An attack on the voluntary Bitcoin nodes on the network – those which relay transaction information around the network but which don't necessarily mine coins – surfaced in late June 2013. The core development team had to issue a patch to solve the problem, and the attack ceased.[9]

> ***"Bitcoin is a mechanism for money, rather the services that are layered on top of money to make it useful. As these begin to emerge, the Bitcoin community will have even more to contend with"***

In this case, the attack exploited an incomplete feature in the source code. The software is filled with these stubs, which are vestiges of Satoshi's original ideas and plans for Bitcoin. These even include an Ebay-like Bitcoin market that was never implemented. Garzik says that such semi-coded features are being 'walled off' within the source code. Nevertheless, they evidently still expand the client's attack surface area.

There are some steps that can be taken to make the code – and therefore the network – more secure, argues Lerner. "They should pay security researchers to review each new patch, or at least clearly document which developers with knowledge in computer security have reviewed each patch."

Bitcoin has already shown lots of promise. However, the core developers face challenges as the size of the network increases. The concept is only just beginning, too. Bitcoin is a mechanism for money, rather the services that are layered on top of money to make it useful. These include credit structures, the issuing of bonds, futures and options trading, and structured financial instruments. As these begin to emerge (and there are already proposals for them), the Bitcoin community will have even more to contend with.

About the author

Danny Bradbury has been a technology journalist since 1989. He writes regularly about Bitcoin for Coindesk magazine, *and is preparing a book on the subject. He also writes regularly for outlets including the* Guardian, *the* National Post *and* Backbone magazine.

Resources

- Rosenfeld, Meni. 'Analysis of hashrate-based double-spending'. 11 Dec 2012. Updated 13 Dec 2012. Accessed Oct 2013. https://bitcoil.co.il/Doublespend.pdf.
- Coindesk.com.
  Garzik, Jeff. 'Random blatherings by Jeff'. Blog. http://garzikrants.blogspot.ca.
- Lerner, Sergio. 'Bitslog' blog. http://bitslog.wordpress.com.
- 'Killing the Dust – the end of all faucets!'. Bitcoin.lift. Accessed Oct 2013. http://Bitcoin.lift-institute.com/killing-the-dust/.
- 'Weaknesses'. Bitcoin wiki. Accessed Oct 2013. https://en.Bitcoin.it/wiki/Weaknesses.

References

1. Waterfield, Bruno. 'EU makes bank creditors bear losses as Cyprus bail-in becomes blue-print for rescues'. Telegraph, 27 Jun 2013. Accessed Oct 2013. www.telegraph.co.uk/finance/financialcrisis/10145355/EU-makes-bank-creditors-bear-losses-as-Cyprus-bail-in-becomes-blue-print-for-rescues.html.
2. Nakamoto, Satoshi. 'Bitcoin: A Peer-to-Peer Electronic Cash System'. Bitcoin.org. Accessed Jun 2013. http://Bitcoin.org/Bitcoin.pdf.
3. 'RBS faces IT failure investigation by FCA', BBC, 9 Apr 2013. Accessed Oct 2013. www.bbc.co.uk/news/business-22083695.
4. Bradbury, Danny. 'A look inside KnCMiner, Bitcoin mining's dark horse'. Coindesk, 27 Jun 2013. Accessed Oct 2013. www.coindesk.com/a-look-inside-kncminer.
5. Bradbury, Danny. 'Feathercoin hit by massive attack'. Coindesk, 10 Jun 2013. Accessed Oct 2013. www.coindesk.com/feathercoin-hit-by-massive-attack.
6. Karame, Ghassan; Androulaki, Ellie; Capkun, Srdjan. 'Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin'. Accessed Jun 2013. http://eprint.iacr.org/2012/248.pdf.
   7. Gilson, David. 'Bitcoin blockchain grows to 8GB'. Coindesk, 20 Jun 2013. Accessed Oct 2013. www.coindesk.com/Bitcoin-blockchain-grows-to-8gb/.
8. Andreesen, Gavin. 'Treat dust outputs as non-standard, un-hardcode TX_FEE constants'. Github. Accessed June 2013. https://github.com/Bitcoin/Bitcoin/pull/2577.
9. Bradbury, Danny. 'Bitcoin network recovering from DDoS attack'. Coindesk, June 2013. Accessed Oct 2013. www.coindesk.com/Bitcoin-network-recovering-from-ddos-attack/.