Sathoshi Nakamoto Biography

By Brandon Dooley (#16327446) for CS3012 - Software Engineering

Here is my Bitcoin wallet: 3HnjKB1TnQSiYG3uaTMWD33UF2ZxoSPTP5

Background

'Satoshi Nakamoto' is the person/people/corporation/acronym attributed with being the inventor of the well-known digital currency/cryptocurrency Bitcoin. The original whitepaper for Bitcoin, titled 'Bitcoin: A Peer-to-Peer Electronic Cash System' was written and signed off by Satoshi Nakamoto on October 31st 2008.

To this day it is unconfirmed who Satoshi Nakamoto really is. The first trace of Satoshi Nakamoto appeared on a P2P Foundation profile where he stated to be a man living in Japan, born on 5 April 1975. However, after some detailed research it proved quite unlikely that Satoshi was of Japanese descent due to his perfect English and his activity frequently correlating within times corresponding to daytime within Greenwich Mean Time (GMT), meaning that he was either a Japanese insomniac or that he in fact lived outside of Japan in a different time zone.

Who is Satoshi Nakamoto?

There are quite a number of people who are suspected to be the real Satoshi. One of the main suspects is Hal Finney, a pre-bitcoin cryptographic pioneer who was the first person (other than Satoshi) to test and use the Bitcoin blockchain software and to develop upon the first solution proposed by Satoshi. Finney had a Japanese-American neighbour named Dorian Nakamoto whose birth name was actually Satoshi Nakamoto, this has remained one of the main areas of speculation that has re-enforced peoples beliefs into the theory that Hal Finney was in fact the founder and creator of Bitcoin. Dorian himself is also highly suspected of being the real Satoshi, a trained Physicist who worked as a systems engineer and a computer engineer for financial services companies who was an avid libertarian.

Also tipped to be Satoshi is a cryptography graduate student from Trinity College Dublin, Michael Clear. Clear, now a post-doctoral student at Georgetown University was hired by Allied Irish Banks to improve its currency-trading software and also co-authored an academic paper on peer-to-peer technology. In 2011 Joshua Davis published an article in the New Yorker he narrowed down the search for Satoshi to several candidates, one of these being Michael Clear. However when asked if he was the founder, he stated:

> *"I'm not Satoshi, but even if I was I wouldn't tell you,"*

Digital Currency & Digital Cash

The idea of having digital cash was not invented by Satoshi Nakamoto. In fact, it stems back all the way to 1983 when a research paper published by David Chaum introduced the idea of digital cash. He later went on to found DigiCash in 1990, an electronic cash company in Amsterdam to commercialize the ideas produced in his paper. However, the company filed for bankruptcy in 1998 and Chaum later left the company in 1999.

Following on from DigiCash the likes of PayPal began to emerge in 1998. These provided quite a successful solution for taking physical cash to a digital medium and allowing users to send/move cash in various currencies around the globe. However, the currencies supported by these platforms were state backed currencies such as USD, GDP, EUR which were all controlled by central banks.

This paved the way for Satoshi's new currency - Bitcoin. Bitcoin would develop to be the first fully decentralized digital currency with a fully open-source underlying technology and a public encrypted ledger allowing the world to transparently see the distribution and transfer of the wealth held by the anonymous people who owned some Bitcoin.

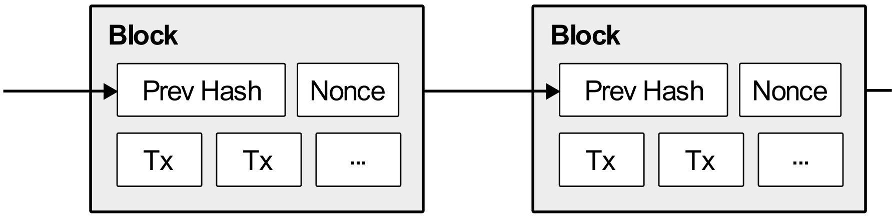
Double Spending

One of the main reasons why digital currencies had not succeeded prior to Bitcoin was due to the double-spending problem. This is an issue where a digital token can be spent more than once, this can be seen in physical currencies in the case of counterfeit money where a person can create a new amount of fraudulent currency that did not previously exists which further leads to inflation.

To prevent this, commerce - both on the internet and in physical form - has relied on financial institutions and third parties to process payments and verify their validity. This third party validator requirement gives birth to an unnecessary demand for trust, merchants must be wary of their customers and hassle them for information in order to prevent fraud.

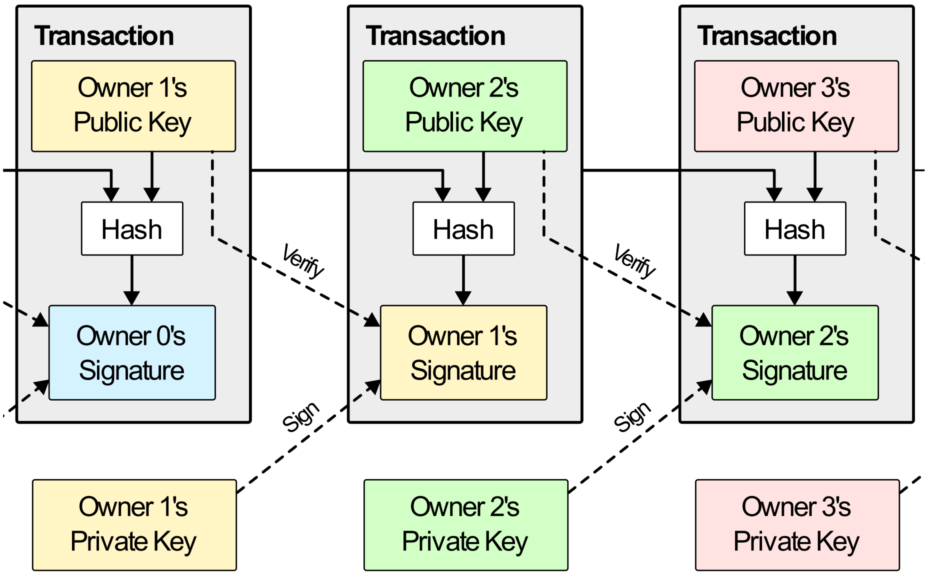
Proof-of-Work & Blockchain

Satoshi proposed the design for an electronic payment system which would use cryptographic proof (hashes) instead of trust. As a result of using these cryptographic hashing functions as a provider of proof it allows the likeliness of the occurrence of fraud to be significantly reduced whilst also removing the necessity of a (expensive) third party such as a financial institution.



The Bitcoin network can be considered as a large chain of blocks representing transactions with each block entirely dependent on the previous blocks validity. This validity is provided in the Bitcoin network by users performing a 'mining' operation to find the correct hash needed to validate a transaction within the network. In order for a transaction to be validated, a Bitcoin miner must perform the necessary proof-of-work to calculate/compute a hash that begins with the number of zero bits required at a given difficulty. Satoshi proposed a proof-of-work method where the average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

Once a block has been validated the next block can then be validated. However, the validity of this block includes the hash of the previous block within it and thus in order to modify a previous block, an attacker would have to redo the proof-of-work of block x and all blocks before it.



Applications of Blockchain Technology

Blockchain is a common word in today's vocabulary. If you read a large newspaper it is quite likely that there will be reference to blockchain in some article. Blockchain has found quite a large spectrum of usage outside of digital currencies.

Satoshi's proof-of-work idea has found use-cases in areas of everyday life such as election fraud. By using a blockchain based voting system within an election it would allow all votes to be anonymously and publicly visible on a blockchain and also allow every person with access to see the results of such an election. This allows for a guarantee of votes within an election to be counted and represented trustfully and as intended.

Blockchain has also spread to industries such as refugee aid. The Ethereum blockchain was recently used to run a United Nation's World Food Programme (WFP) campaign where refugees were given cryptocurrency-based vouchers that could be redeemed in participating markets. This allows for people who may be sceptical of where their donations are going to ensure they are being used in the intended manner as it would be publicly visible on the Ethereum blockchain once this token had been used.

Medical records of patients are required to be consistent at all times. By moving health care records onto a blockchain based systems they would become immutable. This can be seen in the developments of the company TrustedHealth. They provide a direct connection between medical practitioners, patients and other service providers in the health sector.

Why Satoshi Nakamoto?

The reason I chose to do my essay on Satoshi Nakamoto was mainly because of the fact that I have an avid interest in cryptocurrencies and blockchain technologies. I enjoy the idea of a world where one day we may not have to use third parties such as banks and other financial institutions and where all global wealth can rest upon a decentralized open-source ledger.

Satoshi's original idea has spread and been built upon in amazing ways which are being used to benefit all aspects of society in a meaningful (and some otherwise) way. I find it hard to believe that Satoshi could have imagined what his original whitepaper would blossom into and hope that one day we may find the real Satoshi Nakamoto to say thanks to. And if not, so be it, let him be our Mona Lisa.

Sources

- Wikipedia - Satoshi Nakamoto
- Bitcoin Whitepaper
- Trinity's Satoshi Nakamoto - Business Insider
- Trinity's Satoshi Nakamoto - New Yorker
- Double Spending
- Blockchain Elections
- UN World Food Programme Ethereum Campaign
- Blockchain Applications