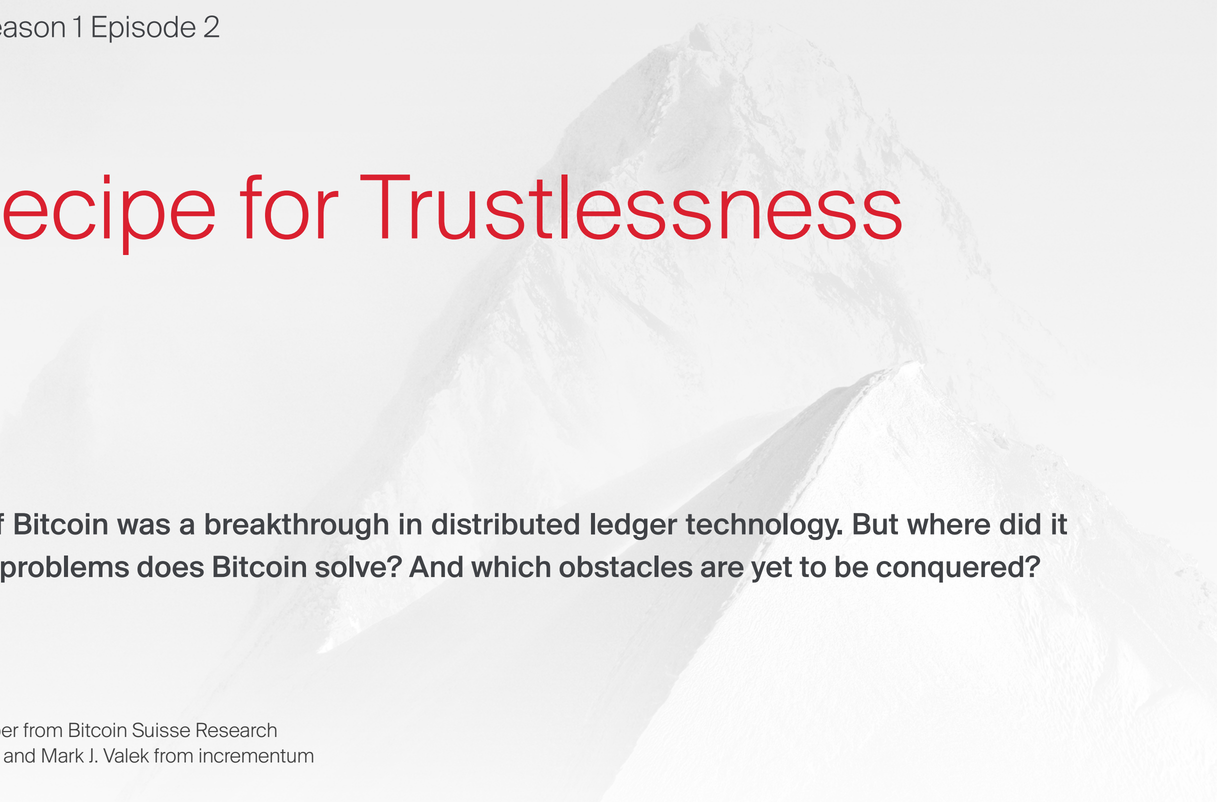
Bitcoin Suisse | Decrypt

July 30, 2019 | Season 1 Episode 2



The Recipe for Trustlessness

The invention of Bitcoin was a breakthrough in distributed ledger technology. But where did it all begin? What problems does Bitcoin solve? And which obstacles are yet to be conquered?

Written by Dr. Raffael Huber from Bitcoin Suisse Research
and Demelza Kelso Hays and Mark J. Valek from incrementum

October 31, 2008. The financial crisis was weighing heavily on the global economy, and the American investment bank Lehman Brothers had just collapsed. Out of the blue, a person or group under the pseudonym of "Satoshi Nakamoto" sent out a link to a paper via a cryptography mailing list. The title of the seminal paper was: "Bitcoin: A Peer-to-Peer Electronic Cash System," and it would mark the beginning of cryptocurrencies as we know them today.

The idea of creating a digital version of cash is much older, though. An early attempt was launched in 1989 by David Chaum: *DigiCash*. Chaum, who was a skilled cryptographer, despised the lack of privacy in cyberspace and developed a method – called Blind Signature Technology[1] – which allows signing a message without revealing its contents. Thus, DigiCash enabled private and secure payments over the Internet. Rumor has it that Bill Gates offered $100 million to acquire DigiCash and integrate it in Windows 95, but was turned down by Chaum, who aimed for a higher valuation of his company. DigiCash later went bankrupt in 1998.

Another early attempt at a digital cash equivalent was *e-gold*, which provided users with accounts denominated in grams of precious metals. Founded in 1996, the payment system grew to more than $2 billion in transactions per year in 2006 and had 5 million accounts. However, its centralized nature enabled the US government to force e-gold to suspend its business in 2008 due to regulatory issues following a change in the legal definition of a money transmitter.

> *"A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them."*
> *– Satoshi Nakamoto*

[1] http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF

In both cases, a centralized authority was required to confirm that funds are only spent once. Hence a single point of failure was present, which was attackable by malicious actors or controllable by governments. Bitcoin is different: The decentralization of the network across many participants (nodes) ensures that there are no easy attack vectors to the network.

Without a central authority, a native mechanism to prevent *double-spending* of coins is required. The basic design of how this is done stems in part from B-money and Hashcash, both of which are referenced in the Bitcoin whitepaper. **B-money**, a paper published by Wei Dai in November 1998,[2] was never officially launched – but included many of the ideas now present in modern cryptocurrencies. For example, the creation of money by solving a computational problem or the enforcement of contracts. **Hashcash**, proposed in 1997 by Adam Back,[3] on the other hand was originally intended to be a Denial of Service (DoS) countermeasure and to limit the capability of spammers to send out emails. The system employs *cost-functions*, which rely on brute-force computations to find solutions. Verifying correct solutions then only takes minimal computational effort.

Bitcoin solves the double-spending problem by bundling transactions in blocks and cryptographically chaining these blocks together. Only valid transactions – i.e. transactions that are properly signed and do not double-spend coins – are included in blocks. Each block includes a Hashcash-style *proof of work*, through which the block publisher proves that a certain amount of computational resources was invested to mine the block. Only the longest blockchain, i.e. the one that contains the most work done on it, is then considered valid by all network participants. This algorithm also presented the first solution to the "Byzantine Generals' Problem"[4] and enables consensus on the state of the Bitcoin ledger even in the presence of malicious actors.

January 3, 2009. In the aftermath of the financial crisis, the first Bitcoin block was mined and contained the message: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.*" A new, non-government controlled financial system was created – empowered only by cryptography, code and mathematics.

> *"I think there's no capacity to kill Bitcoin. Even the Chinese with their Firewall and their extreme intervention on their society cannot kill Bitcoin."*
> *– Rep. Patrick McHenry*

Security, Decentralization, Scalability: the Blockchain Trilemma

In cryptography, there is a theory that states that anything that can be done with a central party can also be done without a central party. However, central parties aren't all bad. For example, taking decisions in a firm is faster when there is a vertical hierarchy of owners, managers, and subordinates. Likewise, countries ruled by dictatorships are faster at making decisions than direct democracies. Although centralized entities are faster, they are less inclusive by design because not everyone can participate in taking decisions. Similar parallels can be drawn to how decisions are made in a blockchain. Slow and egalitarian networks such as Bitcoin are criticized by investors that want a fast and global payment network.

Vitalik Buterin, creator of the second largest cryptocurrency Ethereum, refined these thoughts and referred to the problem as the *blockchain trilemma*. The blockchain trilemma describes the trade-offs between security, decentralization, and scalability. Security refers to the network's ability to keep working while fending off attacks like a double spend. Decentralization refers to the number of users or computers that are involved in taking decisions regarding incoming transactions. Finally, scalability refers to how many transactions per second the network can handle. Vitalik argues you can only have two out of three.

Although more than 2,000 cryptocurrencies exist, most of them can be divided into **three** categories based on how they reach an agreement without a leader or central party. **The first is proof of work** and is how Bitcoin solves the double-spending problem as explained above. Other coins such as Bitcoin Cash and Litecoin also fall into this category.

[2] https://nakamotoinstitute.org/b-money/
[3] http://www.hashcash.org/papers/announce.txt
[4] https://www.metzdowd.com/pipermail/cryptography/2008-November/014849.html

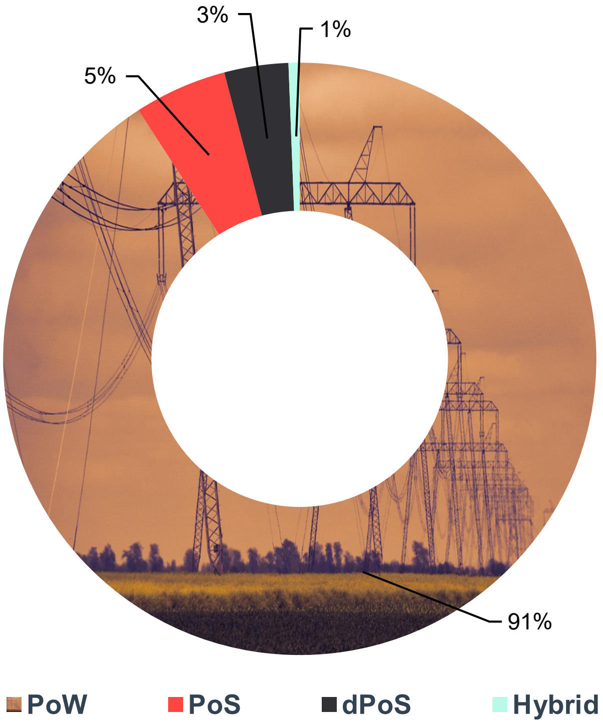
Proof-of-work blockchains are decentralized and secure. According to the blockchain trilemma, that means they must give up scalability. And, sure enough, they must. Proof-of-work blockchains are limited in terms of transaction throughput and speed because each node processes every single transaction on the network. Ethereum manages a maximum of 20 transaction per second, while Bitcoin only achieves seven. Centralized systems such as PayPal can process about 200 transactions per second, and Visa achieves a staggering 56,000.

The second is proof of stake, which requires users to deposit coins into an escrow account before they are allowed to take decisions. If they make a decision that harms the whole network, their deposit in the escrow will be confiscated. This is similar to forming a company with equity capital. If the business does not behave honestly, people can sue their capital. Another way to think of proof of stake is that the decisions makers have "skin in the game." Coins such as NEO, Stellar, and Binance Coin all fall into this category.

Finally, **the third is delegated proof of stake**, which is a variation of proof of stake. Coins such as EOS, Cardano, and Tezos (delegation is optional) are in this category.

So far, no one has solved Vitalik's blockchain trilemma. Many cryptocurrencies claim to solve the problem with first-layer governance or directed acyclic graphs; however, each improvement upon Bitcoin has its own advantages and disadvantages. In the future, these different approaches for solving the double-spend problem will compete on the free market with centralized solutions. And another nice feature of the blockchain technology is that it financially rewards the early investors who can anticipate the market's winners and losers.

Illustration 1: Over 90% of the cryptocurrency market cap uses proof of work.



Source: CryptoSlate.com, Incrementum AG.

Bitcoin
Suisse

Bitcoin Suisse AG
CH-6300 Zug
bitcoinsuisse.com

in collaboration with

incrementum

Disclaimer:

The information provided in this document pertaining to Bitcoin Suisse AG and its Group Companies (together “Bitcoin Suisse”), is for general informational purposes only and should not be considered exhaustive and does not imply any elements of a contractual relationship nor any offering. This document does not take into account nor does it provide any tax, legal or investment advice or opinion regarding the specific investment objectives or financial situation of any person. While the information is believed to be accurate and reliable, Bitcoin Suisse and its agents, advisors, directors, officers, employees and shareholders make no representation or warranties, expressed or implied, as to the accuracy of such information and Bitcoin Suisse expressly disclaims any and all liability that may be based on such information or errors or omissions thereof. Bitcoin Suisse reserves the right to amend or replace the information contained herein, in part or entirely, at any time, and undertakes no obligation to provide the recipient with access to the amended information or to notify the recipient hereof. The information provided is not intended for use by or distribution to any individual or legal entity in any jurisdiction or country where such distribution, publication or use would be contrary to the law or regulatory provisions or in which Bitcoin Suisse does not hold the necessary registration or license. Bitcoin Suisse 2019.