Blockchain Council™

The Bitcoin Experiment

The 2008 Financial Crisis

- Before COVID - 19, the worst recession faced by the global economy was the period in the year 2008.
- It had the worst impact on the global economy that people considered it as the **Global Financial Crisis (GFC)**. Many economists around the world considered the 2008 crisis as the most serious financial crisis after the **Great Depression.**
- Lax financial regulation along with the excessive risk-taking by banks, and the bursting of the United States housing bubble caused a huge drop in estimations of mortgage-backed house holds which were partnered to American real estate.
- The financial institutions around the globe suffered severe damage and declared the bankruptcy of Lehman Brothers on September 15, 2008 eventually resulting in an international banking crisis.
- Some economists named the post-recession years as the weakest recovery since the Great Depression and World War 2. One commentator even called it ``Zombie Economy '' as it was neither dead nor alive, it was barely surviving.

The Bitcoin Whitepaper

- Bitcoin is a decentralized digital currency without a central governing body such as the Central Bank which can be transferred between peers without any need of the intermediate parties.
- Transactions are verified, validated by the nodes through the cryptography network and recorded in a publicly distributed ledger called a Blockchain developed by an anonymous person or a group of people known as Satoshi Nakamoto.
- On 18 Aug, 2008, a pseudo anonymous user registered the domain bitcoin.org with the email satoshin.gmx thus publishing the bitcoin around the globe. On 31 Oct, 2008, a whitepaper named “Bitcoin: A Peer-to-Peer Electronic Cash System“ was posted to a crypto mailing list. Nakamoto implemented the bitcoin as an open-source software and released its source code in January 2009 on sourceforge.net
- On 3 Jan, 2009, the bitcoin network was created and Nakamoto mined the first block of the chain which is called the Genesis Block.
- A text was embedded into this block that says “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks".

The Bitcoin Whitepaper

Abstract

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Available at https://bitcoin.org/bitcoin.pdf

The Bitcoin Whitepaper

The white paper submitted is 9 pages long with 12 subsections covering all the aspects that are related with the bitcoin network. The sections are:

- Introduction
- Transactions
- Timestamp server
- Proof-of-Work
- Network
- Incentive
- Reclaiming Disk Space
- Simplified payment verification
- Combining and splitting value
- Privacy
- Calculations
- Conclusion

Timestamp Server

- Timestamp servers are a typical form of servers that are used to cryptographically sign, authenticate and validate a digital signature with a signing certificate that took place at a particular moment of time.
- This allows a user to verify at some time in future that a document or program or any other file was digitally verified and signed at a particular instance of time.

History

- The timestamping idea is ancient.
- Robert Hooke, the discoverer of Hooke's law did not publish his writings at the time of his discovery in the year 1660, but wanted to claim the priority.
- Galileo also used the same technique for concealing the details of his discoveries of the Venus phase.
- The same approach is also used by Sir Isaac Newton once the details he wrote about the "Fluxional Technique".
- Haber and Stornetta are the original inventors of the Trusted Digital Timestamping technique. They discussed the technique in their literature.

Types of Timestamping Server

PKI based: In PKI based timestamp server, the timestamp token used is secured using the PKI digital signature.

Linking-based: In this schema, the new timestamp is generated in relation with the existing timestamps.

Distributed: The scheme that uses the cooperation of multiple parties in the process of creating a timestamp.

Transient key scheme: It is a flavor of PKI based schema. It uses signing keys with short life-span for timestamping the objects.

MAC: It is founded in ANSI standard, which is used to timestamp with a simple secret key.

Database: It stores the documented hashes in a trusted location as archives and also provides a lookup service for verification that is available online.

Hybrid scheme: A mixed flavor of the linked scheme with the signed method.

Trusted Digital Timestamping

- By the standards specified by RFC 3161 to be a trusted timestamp, it must be issued by a **Trusted Third Party (TTP)** which is responsible for the role **Time Stamping Authority (TSA)**.
- Higher the number of TSA's, higher the reliability and lower the vulnerability.
- The newer standard ANSI ASC X9.95 amplifies the RFC standard with its data level security prerequisites for ensuring the integrity of the data against any source of time which is proved as a reliable source to any third party.

Timestamp Server

Timestamp creation

- In the first step, a hash value is created with the given data.
- The calculated hash value is further sent to the Trusted Timestamp Authority (TSA).
- The TSA appends the current timestamp with the hashed value and digitally signs the concatenated string with its own private key.
- Then after, the signed hash and the timestamp used are sent to the requester. The requester stores the received information along with the original data available at its end.

Timestamp Verification

- The data which is to be verified is first hashed and appended with the timestamp provided.
- Then we need to decrypt the data received from the TSA which is signed with the TSA's private key. So we use its public key for the decryption process.
- Then, we compare the decrypted data with the computed data which needs to be verified.
- If the data evaluates the same, the submitted timestamp is valid, else it is an invalid timestamp which means either the stamp is modified or it is not issued by the TSA.

Storing Data in Blockchain

To store data, which is almost always the transactions list in a block, the Blockchain technology follows a series of steps to provide safe and secure data storage. They are:

- At the initial stage, the data that needs to be stored in the block is broken into chunks of data that is possible to accommodate into a block.
- After splitting the data in chunks, each chunk will be encrypted to limit the access to only the owner unless it is specified.
- Next, the data chunks or files will be distributed across the network in such a way that all your data will be available, even if a part of the network is unavailable.

In cloud storage such as Amazon or Microsoft, instead of the company handling your data, the files will be distributed across a network of people all over the world. The Blockchain cloud is shared by the community for maintenance and still it restricts others to modify your files. So, we can also use this technology in public services to keep public information safe, secure and decentralized.

Storing Data in Blockchain

Advantages

- The download speeds of the network will be increased exponentially by using peer-to-peer networks similar to torrents.
- The data is globally distributed which means access at any time and anywhere.
- No need for privacy concerns.
- Data storage cost is relatively cheap such as $2 per TB per month.
- The immutability feature of the Blockchain can ensure the files are unaltered which provides the freedom for the users to store sensitive data without worrying about the security and privacy of the files.

Disadvantages

- The security is directly proportional to the size of the network. If the Blockchain network used does not have a big network holding it that means it doesn't have a good number of nodes in the network, the entire system is susceptible to 51% attack which directly disrupts the data.
- More redundancy is needed to secure the data than any other storage model if the network is not big or reliable enough.
- The overhead of the network communication is huge.
- Network bandwidth can be a problem and it can be overcome by selecting an efficient consensus algorithm.

Storing Data in Blockchain

Current Blockchain storages available

- Storj.io and Sia.tech are two famous Blockchain storage platforms that are available right now.
- Filecoin also allows to mine filecoins by sharing storage space and the coins are mined by sharing storage space.