How to Read the Bitcoin Whitepaper

Author	josh
Date	2019-10-31 18:00:05

Overview

On October 31st, 2008, Satoshi Nakamoto graced the world with his vision for a peer-to-peer electronic cash system called Bitcoin. The cryptocurrencies we use today started with this abstract and the ideas contained within. I highly recommend anyone interested in Bitcoin or other open blockchain projects read the original whitepaper, but it can be a bit technical and terse for the completely uninitiated.

Let's walk through the whitepaper together, and get an idea of what each section discusses and why it's important for creating the Bitcoin system. The whitepaper can be read here: https://www.bitcoincash.org/bitcoin.pdf and from many other sources.

Understanding The Whitepaper

Abstract and Section 1

The abstract and first section of the whitepaper lay the groundwork for *why* Bitcoin is important and *how* it solves several problems with the existing system used for online transactions. Whitepapers such as this are often oriented around solving a problem, and the Bitcoin whitepaper discusses the particular problem of creating a *trustless* system of internet money, in contrast to traditional systems that require intermediary processors and mints.

Section 2 - Digital Signatures

Section 2 describes what we now know as the system of private/public key pairs (addresses) and how they are used for transactions. In Bitcoin, the user holds their own *private keys* that prove they own their coins. When the user wants to spend these coins, they create a new transaction that sends coins to another address. That transaction contains a mathematical/cryptographic proof that they are the rightful owner of those funds, called a *digital signature*. The user can prove to the rest of the users on the network that they control a *private key* without revealing that key at all! Instead, they *sign* a message and provide a *public key*, allowing other users to verify they own some money without revealing the secret.

This is a powerful and important feature in Bitcoin - transactions are created and chained together without the need for secret information to be revealed. However, this doesn't prevent the problem of *double spending*, where a user could simply do a digital signature twice to re-spend coins.

Sections 3-6 & 11 - Proof of Work Consensus

In order to prevent double spending and ensure *consensus* across the peer-to-peer network of users, Bitcoin uses an interesting system called proof-of-work. This system prevents fraud by requiring that users expend real-world resources in the form of electricity and computing power to solve a mathematical problem. **Sections 3 & 4** describe the proof-of-work timestamp system used to create a consensus on what transactions are valid and when they occurred.

This mathematical problem requires taking a batch of transactions (batched every ten minutes, roughly) and solving a very difficult guessing game, essentially. The answer to this problem, based on data in the block, can *only* be solved by guessing a bunch. But once the answer is found, all the other nodes on the network can verify the answer is correct in an instant! This is based on the properties of the *hashing algorithm* used in the problem.

Now what does that mean for Bitcoin? It means that as a bunch of honest nodes on the network contribute to security through proof-of-work, attackers don't have the resources to outcompete the honest chain. For an attacker to put a fraudulent transaction in a block, they would have to compute faster than the rest of the entire world acting honestly, and with a large network effect this becomes impossible to do at scale!

As well, part of the problem data for a new block is based on older block data (hence, block*chain* as the blocks are cryptographically linked). So, if an attacker wanted to create a fraudulent transaction that is three blocks back in the history, they would have to do outcompute the rest of the world, doing thirty minutes of work in under ten. **Section 11** shows that the probably of a successful attack becomes negligible after only a few blocks of history.

Sections 5 & 6 - Networking and Incentives

Now why act honestly in the first place? Sections 5 & 6 describe how the network interacts and rewards legitimate users.

Section 5 describes how transactions are flooded out across the peer to peer network for batch processing. Any node that wants to mine to help secure the chain can do so using their CPU power. When a solution is found, it is shared with other nodes that can verify it is correct, and the race to solve the next problem begins. Nodes running the Bitcoin software will always follow the *longest chain of solved problems* or the longest chain of "proof-of-work.

Section 6 describes one of the most important aspects of proof-of-work in Bitcoin, and that's the system of economic incentives that rewards miners for acting honestly. The miner that finds solves the problem for a block gets two rewards - first, they get *newly minted Bitcoin*. They also receive all of the *transaction fees* in that block. The system is therefore designed so that it's easier and more profitable to mine legitimately than to try and attack the network.

Sections 7, 8, & 9- Dealing with Block Data

Storing all of the data in blocks takes up a lot of space as time goes on. The Bitcoin blockchain is several hundreds of gigabytes in size as of the time of this writing. However, Satoshi found a way to keep validation secure without storing every bit of data and discusses in **Section 7**.

Transaction data is cryptographically "summarized" in a *Merkle Tree*, so that the amount of data needed for secure validation is reduced through a process called *pruning*.

As well, thanks to Merkle trees, it is not necessary for every user on the network to store the whole blockchain and validate data. **Section 8** describes a process known as *Simplified Payment Verification* that allow Bitcoin clients to create and receive payments securely without needing the entire history stored in the blockchain. This is especially critical for applications such as mobile wallets.

Section 9 describes the model Bitcoin uses to store data about who owns what. This is the *UTXO blockchain* model, where each wallet owns these *Unspent Transaction Outputs* that behave like dollar bills. A user can take multiple UTXOs and combine them to create a transaction, and send the "change" back to their own wallet.

Section 10 - A Privacy Primer

Everything in Bitcoin happens on a completely *public* blockchain. It is pseudonymous, but not anonymous! In order to prevent *blockchain analysis* from linking a bunch of transactions back to an individual user, Satoshi recommends in **Section 10** that users create new addresses for each payment and not reuse old addresses. This makes linking transactions together much harder for observers.

Understanding Bitcoin, Right from the Source!

The Bitcoin whitepaper is a great place to get started in understanding Bitcoin. In only 8 pages of information, this work describes how to create a system of payments that doesn't rely on any central, trusted authorities like our traditional monetary system does.

The paper itself is brief and to the point, which may make it tricky to understand at first. But with this companion, some re-reading, and exploring other works out there, it becomes easier to understand the magic of the ideas described. Happy Birthday to Bitcoin, and happy reading all!