

What is the Blockchain – part 2 – Public vs Private, Proof of Work vs Proof of Stake & DApps

Published on October 3, 2016



Mark van Rijmenam

Founder Datafloq | Big Data Strategist | International Keynote...



23



1



8

For the tech-savvy people among us, the Blockchain might be nothing new and it may be clear that it will have a big impact on the world. However, for many people, the Blockchain is still a mystery, a puzzle or an unknown unknown. Therefore, in a series of posts, I share with you what the Blockchain is, how it works and how it will completely change the world as we know it, if we get it right.

In my first post about the Blockchain, I explained [the basics of the Blockchain](#) and in this post I will go a bit deeper and talk about the different types of Blockchains, some examples of dApps and talk about the most important part of the Blockchain; the consensus algorithms to validate the data.

Different Types of Blockchains

The most well-known Blockchain is the Bitcoin Blockchain. The Bitcoin Blockchain was envisioned [by Satoshi Nakamoto](#) in 2008 and this is a so-called Permissionless Blockchain, or public Blockchain. This means that anyone interested to join the Blockchain, can do so by simply hooking-up his/her computer to the decentralised Blockchain network, download the Blockchain and contribute to the processing of transactions. It is not required to have a previous relationship with the ledger and you don't need to be approved to join. If you want to start mining Bitcoin and supporting the Bitcoin network, simply [click here](#) and get started. A permissionless Blockchain is not owned by anyone and everyone can contribute.

Next to public, permissionless, Blockchains, there are private, or permissioned, Blockchains. This means that only those that are identified and approved by the Blockchain network, can join the Blockchain and start processing transactions. A private Blockchain is commonly used by a group of companies that want to keep a shared ledger, like for example financial institutions. These Blockchains are owned by an organisation or a group of organisations and you have to be approved if you wish to join. A good example of a private Blockchain is the [Blockchain Settlement System](#) developed by UBS and three other major banks. This Blockchain enables the

four participating banks to drastically improve settlement times among them and no other party has access to the Blockchain or can contribute to it.

Private and public Blockchains are the two flavours that have been around and for both options, the main feature of the Blockchain is that once a transaction is approved and on the Blockchain, it cannot be changed or edited. Since this week, however, a third option has been developed. Accenture has patented an “editable Blockchain”, which means that the data in the Blockchain can be adjusted by a central authority. This is a bit of a contradiction since the power of the Blockchain is that data, once validated, cannot be altered. However, Accenture [claims](#) that this type of Blockchain would only be for private, permissioned, Blockchains used for example by the banks, where a central authority can manage the network under agreed governance rules. It would offer a “safety button” that could, in fact, make the Blockchain more safe to use. If you want to read more about this editable Blockchain, you can read this [article on Forbes](#).

Proof of Work vs Proof of Stake

In order to add data to the Blockchain, it needs to be validated and accepted by the network. Validating the data is done using cryptography and via consensus, meaning that 50% +1 of the network need to agree. There are two ways to achieve this consensus, being Proof of Work and Proof of Stake:

Proof of Work Consensus Algorithm

Proof of Work is used in the Bitcoin Blockchain and it refers to participating users (or nodes) solving difficult mathematical problems to validate the blocks. The node that publishes the solution first, ‘wins’ and receives Bitcoins as a reward. The mathematical problem works like a crossword puzzle; it is difficult to solve, but once it is completed, you instantly know if it is correct. Once accepted by the majority of the network, all the nodes in the network will start working on the next block, thereby repeating the process.

The disadvantage of Proof of Work is its inefficiency in terms of computing power. It requires real-world resources to validate transactions and it requires a lot of it. However, this is also what makes the Blockchain immutable, as it requires a tremendous amount of computing power (a.k.a. as money), meaning 51% of all resources in the Blockchain, to alter transactions.

Proof of Stake Consensus Algorithm

Proof of Stake solves a major problem of the Proof of Work consensus algorithm, which is the computing power that is required to keep the Blockchain working. The most important difference is that with a Proof of Stake consensus algorithm, the amount of computing power is not the requirement for validation, but the amount of cryptocurrency owned. In order to validate, 51% of the digital currency in the network needs to agree on the current state. As a result, the more digital currency you own, the

higher your stake in the success of the Blockchain. The [rationale](#) is quite simple; the higher your stake in the system, the higher your incentive to maintain a secure network, because of the pain felt when the reputation and price of the cryptocurrency is damaged due to attacks.

As a result, Proof of Stake requires significant less energy and can be seen as a greener option. The problem, however, with Proof of Stake is, that it becomes easier for a small group of people owning a majority in the currency, to alter the Blockchain. Especially in new Blockchains, where the digital currency is yet to be owned by many people, this can pose a problem.

DApps on the Blockchain

An application on the Blockchain is called a Decentralised Application, or DApp. DApps offer a lot of benefits for the end-user in terms of increased security, transparency and automation of operations thanks to smart contracts. DApps can be a lot cheaper to run, because of the automation, resulting in reduced overhead costs and faster time-to-market once developed. Basically, any application that's out there, can be turned into a Decentralised Application. When removing a centralised governing body as well as removing as much as governance by management and employees as possible, and instead include governance by code through smart contracts, DApps offer a new way of doing business. In order for a DApp to be a DApp, it needs to have [four characteristics](#):

1. The code needs to be open-source and any changes to the code must be done via consensus;
2. Data has to be stored on a public Blockchain, to avoid a centralised governing body;
3. There must be a cryptocurrency, or App Coin, to access and use the application;
4. A cryptographic algorithm needs to be in place to ensure either Proof of Work or Proof of Stake.

There are already quite a few examples of DApps, of which Bitcoin is of course the most well-known. To view an extensive list of DApps, here is a list of all known DApps at the moment: dapps.ethercasts.com. To have a detailed explanation of DApps, please visit [Bitnation](#).

Changing How the World Works

The Blockchain, and with it the hundreds of DApps that have already been developed, offer a glimpse of what the future beholds. The Blockchain is still in its early development and a lot of development work is still to be done. However, decentralised applications that are run by smart contracts, without the need for a centralised governing


power that generally takes a large commission, offer tremendous advantages. They are cheaper and more efficient to run, more difficult to control by governments or organisations and more secure and transparent than existing applications. Of course, there are still a lot of challenges to be solved, which I will discuss in the next post.

Read part 1 of this series [here](#).

This post originally appeared on [Dataflog](#).



Report this




Mark van Rijmenam
Founder Dataflog | Big Data Strategist | International Keynote Speaker | Author | PhD Candidate
[50 articles](#)

1 comment

Recommended 




Leave your thoughts here...



Udit Bhatnagar ... 3w
MBA | Business Strategy | Consulting | Technology & Innovation in Financial Services

Mark, I read both your posts from this series. Firstly, congratulations on writing two great posts on otherwise a complicated subject. You simplified and presented Blockchain from the ground up. I also appreciate that you incorporated advice from [Winston](#) and explained 'Proof of stake' and 'Proof of work' concepts in your follow-up post. I'd love to read more about applicati... [See more](#)

Like Reply |  2

Don't miss more articles by Mark van Rijmenam



What is the Blockchain – part 4 – Transactions and Smart Contracts

Mark van Rijmenam on LinkedIn



What is the Blockchain – part 3 – Blockchain Startups and Five Challenges to Overcome

Mark van Rijmenam on LinkedIn



What is the Blockchain and Why is it So Important?

Mark van Rijmenam on LinkedIn

Looking for more of the latest headlines on LinkedIn?

