The untold history of Blockchain

Petri Basson

Hash Directors | Lemma DAO Service | Blockchain Association of the Cayman Islands

16 articles Follow

Open Immersive Reader

I have always believed that to really understand something and where it is going, you have to understand where it came from.

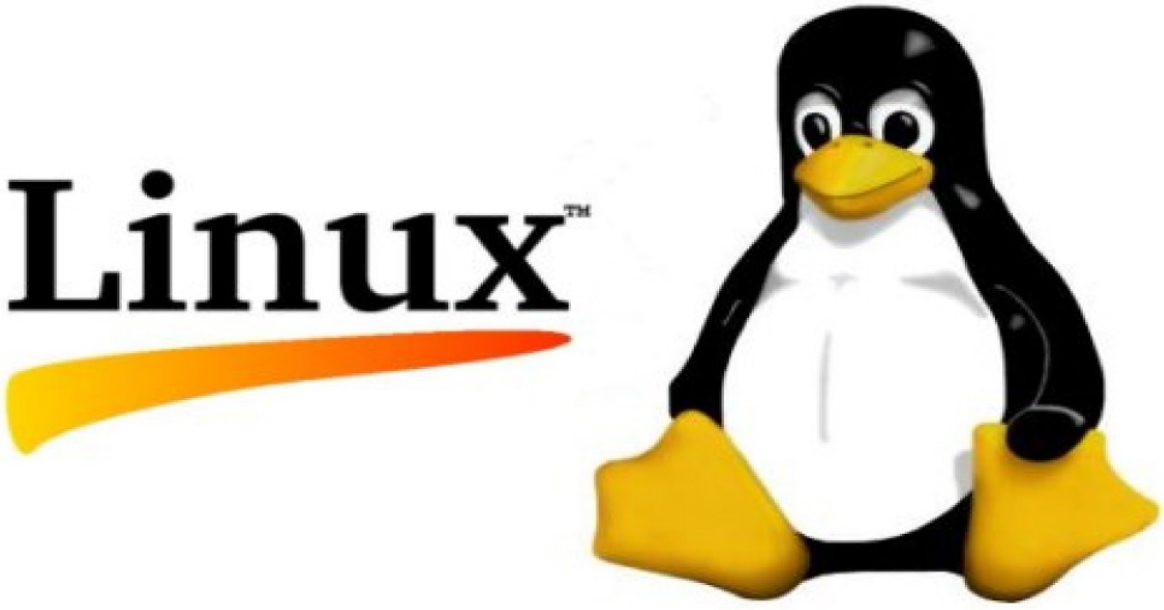
In my own search to better understand Blockchain, I've gone deep down the Blockchain rabbit hole. Asking how did it start and why is this important?
As it turns out Blockchain technology is not something that was created by chance or out of the blue by an anonymous genius called Satoshi Nakamoto. There is a long and fascinating mostly unknown history to this technology.
In this article (and the ones to follow) I will explain a fraction of that history to help you to understand Bitcoin and the Blockchain technology, where it all came from and where it might be going.
In the beginning there was nothing
To get an idea of the building blocks that the blockchain is built on, you have to understand the history of 3 things:

- Encryption;
- Open Source software development; and
- Peer to peer sharing

Encryption
One can start any discussion on encryption in a variety of places. I have chosen to start this particular discussion in 1991, with a little known programmer born in Camden New Jersey, the son of a concrete truck driver, Phil Zimmermann.
Phil had dreamed of creating an encryption system for the masses based on public key encryption that would allow people to communicate freely on the internet, without the risk of surveillance. But, juggling a freelance job and two children, he had never found the time to realize this dream.
In early 1991, he learned about a proposed piece of U.S. Senate legislation that would force electronic communications service providers to hand over individuals' private messages. This was the tipping point for Zimmermann and he decided to develop a tool that would help individuals freely communicate on the internet. In late 1991, after working on the project tirelessly and almost losing his house in the process, he released Pretty Good Privacy (PGP). This was the first ever publicly available encryption tool that allowed people to communicate freely using 128-bit encryption and Diffie-Hellman for key management.
The US government, however didn't share Zimmermann's ideals. After PGP was publicly shared and quickly spread around the world he was charged under the Arms Export Control Act by the United States Customs Service. The government regarded cryptographic software as a munition and only allowed the export of "low-strength" encryption.

Luckily in early 1996 the government dropped their case against him due to a lack of evidence that he shipped PGP overseas or that he had posted it to Usenet.
This story is significant because, at its core, the code that Zimmermann wrote was nothing other than a form of speech. Therefore, had the US government been successful in their case against Zimmermann, they would have been able to control the distribution of anything written in the United States which would have arguably been a violation of the first amendment of the US constitution:
“Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances”
You would live knowing that every email, every text message, every bank transaction you did and every picture you owned was being monitored and viewed by somebody else. Some may argue that this is the case today, but at least you have the tools to protect yourself if you want to.
Without Zimmermann and many others who tirelessly worked on encryption all our communication would be open for anyone to see and the internet may never have developed as it did.
Open Source software
Surprising to most is that fact that there was once a time when most software was open and free for use. You could buy and edit software as you pleased to suite your own needs. A programmer working at the MIT AI labs Richard Stallman did exactly this.
All of the printers at MIT were on a different floor, so he added an electronic messaging system that would let a user know when their job was printed or if the printer was jammed. Saving everyone a lot of time walking up to the printers to check if jobs had printed or not.
In 1979 he famously called it a “crime against humanity” when Brian Reid placed time bombs in his software to restrict unlicensed access to it
When the university installed a new Xerox 9700 printers and Stallman and the other hackers at the AI labs were refused access to the source code he was convinced that people need to be able to freely modify the software they use. He quit his job at MIT and start the GNU project. The GNU manifesto states that users should be free to run software, share it, study it and modify it.
They also developed the GNU General Public License. Code released under this licensed can be reused in other computer programs as long as it is also released under the same or a compatible license.

One of the most famous programs that runs on this license today is Linux created by Linus Torvalds in 1991 (the same year PGP was released). You may know it better as the operating system that runs your smartphones and tablet computers, or the system that runs 99% of the world's top 500 supercomputers.



What makes Linux different from any other software is the fact that it is completely open source and at any point in time there are up to 10,000 people working on it. With the open nature of Linux, some may argue that it weakens the system because hackers can also see and modify the code. However because of the size of the community, there are various phases in the patch development, review, and merging cycle when Linux is updated. Therefore making the process much more robust and secure.

In 2005 Torvalds created GIT a version control system for tracking changes in computer files and coordinating work on those files among multiple people. This eventually lead to the development of sites such as GitHub, which are used for the development and review of all code changes made to Bitcoin.

You can go to this link right now and see all the changes that have been made to Bitcoin. Every change is reviewed and tested by an entire community making this a technology that doesn't belong to just one company or individual.

It is truly open source and users are free to run it, share it, study it and modify it as they wish. This can be seen with the multiple hard forks and alternative coins based on Bitcoin. Truly open and free as intended by Richard Stallman.

Peer to peer sharing

The last thing you need to understand is the technology that makes Blockchain so resilient that not even governments such as China have been able to stop it.
In July 2001 Bram Cohen released a program called Bittorent. It quickly become the arch nemesis of the entire movie industry as it became the one stop shop to illegally download any movie, series or song. Despite numerous lawsuits and raids against website like The Pirate Bay the multi million dollar entertainment industry has still not been able to stop this technology. Why is that?

Bittorent is a peer-to-peer network. All this really means is that each user becomes part of the network. Instead of a traditional network where all the information is on one central server, with a peer-to-peer network it is spread out among all the users. For Bittorent that means that as soon as you download a movie or a song you can also share it with the rest of the network. Just like the mythological hydra when you cut of one head ten more grows in its place. Whenever one site or one member of the network is shut down ten more pop up to take their place.
This makes the network truly resilient to any form of censorship or manipulation.
This exact same technology is used in the Blockchain and Bitcoin. Anyone can become a node which holds a copy of the blockchain and sharers it with the rest of the network. Currently there is approximately 9,000 nodes running the various versions of Bitcoin in the world. This means that if you ever wanted to stop Bitcoin you would have to find and shut down all 9,000 of these nodes at the same time.
A task which would be nearly impossible.
See you in the next article

I think that’s enough Blockchain knowledge for one article.
In the following article we’ll go into the Cypherpunk movement and how Bitcoin was eventually born from that group.

Special thanks for the review @lizebasson and @kimdennison