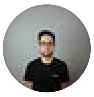
Open in app ↗

Sign up Sign In

Medium

Search

A Brief History on the Origins of Blockchain



Joe Jobes · Follow

3 min read · Feb 26, 2018

Listen Share

The story of Bitcoin has become rather prevalent as of late. With the recent popularity in cryptocurrency running wild, there seems to be a neglect of the underlying technology that helps the entire cryptocurrency world function. This technology, while not making many headlines in the news, is increasingly becoming a hot topic among industry leaders for applications other than cryptocurrency. It could be used in preventing fraud in our voting machines, increase the security and efficiency of online banking, provide a standard for tracking warehouse shipments, and much much more. This technology is blockchain.

Now the purpose of this blog is not to explain blockchain right off the bat. That will be for later installments in this blog. Instead I want to touch upon the history that brought this technology to the forefront of todays tech sector. There are many blogs and publications on the different types of blockchain and it's function, but very few will mention exactly how it came about. Who developed it? Where did it come from? How long has this technology been around? I will try to answer all of these to the best of my abilities.

So. Who came up with the blockchain? Well, many people who have been interested in cryptocurrency, specifically bitcoin, will point to the elusive creator Satoshi Nakamoto. In a 2008 paper, "Bitcoin A Peer-to-Peer Electronic Cash System", Nakamoto describes the concept of bitcoin and the underlying mechanisms by which it works. In this paper Nakamoto never once used the term blockchain. Instead, block and chain were used separately to explain the concept of many blocks, each containing data on transactions, all connected in a chain. Over the years blockchain would become the standard term used for this technology, but as stated above, Nakamoto had never termed it this.

While Nakamoto would ultimately put forth the idea of using a blockchain to record a list of transactions for Bitcoin, this is technically not the beginning the concept of a blockchain. For that we have to go back to 1991, where in a paper written by Stuart Haber & W. Scott Stornetta entitled, “How to Time-Stamp a Digital Document”, the concept of time stamping digital documents was proposed, to ensure transactions were ‘signed’ at a certain time. The following year, Haber & Stornetta, implemented a Merkle Tree, otherwise known as a hash tree, in each ‘block’ to store multiple transactions.

Later, during 1996, another cryptographer from Cambridge University, Ross Anderson, described in a paper, entitled “The Eternity Service”, a decentralized storage system with the inability to delete any updates made to the system. This was considered, at the time, a revolutionary paper on developing more secure peer-to-peer systems, which was directly inspired by the shutdown of the Finland’s penet remailer, by the Scientologists.

Two years later, B. Scheier & J. Kelsey would write a paper detailing another method to secure logs from untrusted machines using cryptography. In this paper, the Scheier & Kelsey describe a method in which computer can prevent attackers from modifying or tampering with any previous logs made, while at the same time making any logs unreadable to the an attacker.

One of the big developments for creating the blockchain occurred in 2002 when another pair of cryptographers named, David Mazières and Dennis Shasha, would propose a network file system with a decentralized trust. This was a proto-blockchain in that the writers to this file system would trust one another, but not the system itself. Instead they would digitally sign, with a SHA256 encryption or similar hashing function, commits and append it to a chain of others housed in a Merkel Tree.

Three years later, 2005, Nick Szabo, a prolific cryptocurrency advocate and developer, would create another version of a simplified blockchain, and introduce it alongside his proto-cryptocurrency bit gold.

All of this leads up to 2008 with Satoshi Nakamoto. Within the first installment of blockchain can be seen the influence of each of these cryptographers and researchers, including others that were not named. To this day blockchain has continued to evolve, in which now, blockchain 2.0 has emerged. With it, the ability to write software on top of the blockchain has been introduced, which can include anything from smart contracts to little apps.

As blockchain continues to evolve and become more robust, prolific, and ubiquitous among industries, there is no telling what new application can be envisioned for it.

In later blogs we will go into what exactly a block chain is and how it can be used in different industries.

Bitcoin

Follow

Written by Joe Jobes

326 Followers

Software Developer with experience in Ruby on Rails, currently attending Turing School for Software and Design

More from Joe Jobes