History of Blockchain

The term “Blockchain” originated in a reference to a “chain of blocks” as described by the mysterious creator of Bitcoin, Satoshi Nakamoto (pseudonym) in 2008. [1] Nakamoto was describing the mechanism to solve the double-spending problem without the need of a trusted authority or central server. Three papers referenced by Nakamoto cite papers co-authored by physicists Scott Stornetta and Stuart Haber published in 1991-1997. These papers form some of the conceptual principles of Blockchain and proposed a way to digitally time stamp intellectual property documents in chronological order to provide ownership protection. In 1990, Stornetta got his idea at a Friendly’s restaurant in Morristown, New Jersey. He realized his system could have many dispersed but interconnected copies of a shared ledger. The time stamp would be a hash code with each hash dependent on the ones preceding it in the chain. The block’s data could not be altered without affecting all the other blocks chained to the one in question. As an additional precaution, they advocated publicly publishing the sequence of records, so data could be reviewed and verified by any third party, effectively crowd-sourcing the varication process. Working at Bellcore, Stornetta and Haber let the patent lapse in 2004, before the inception of Bitcoin.

Blockchain is a distributed ledger software technology that forms the underlying platform of Bitcoin. Transactions are clustered into chronologically chained blocks of data using a hashing algorithm that makes the record immutable. Prior to the person or people referred to as Nakamoto, Nick Szabo designed a system in 1998 called “bit gold.” [2] It has been described as a direct precursor to Bitcoin. He said he was trying to mimic in cyberspace the trust and security characteristics of gold. The problem Szabo was trying to solve was that our money currently depends on trust in a third party for its value which is not an ideal state of affairs as evidenced with the 2007-2008 Financial crisis. Szabo has proposed using blockchains for “smart contracts” and Bitcoin provides a Turing-incomplete Script language that allows the creation of smart contracts. Ether

In 2008, Nakamoto published the source code for Bitcoin on SourceForge. (later provide architecture for initial code and other implementations). This proliferated the use of blockchain technology and hyperledger fabric substrate in applications today. Currently there are many open-source blockchain frameworks, we will explore a few such as Bitcoin, Ethereum, RootStock, EOS.

Current use cases for blockchain include public health, financial, customs declarations, payment and digital currency, supply chain, identity, fraud prevention, trade network, insurance, clinical trail management, food safety, dispute resolution, private equity networks, distributed energy source/power grid, asset management, carbon credit management.

Citations (MLA APA Chicago Harvard Vancouver):

Foundation:

[1]

Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).  
<http://bitcoin.org/bitcoin.pdf>

[2]

Szabo, Nick. “Bit gold” (2005)  
<https://unenumerated.blogspot.com/2005/12/bit-gold.html>

Szabo, Nick. “Money, blockchains, and social scalability” (2017)  
<http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html>

Peck, Morgen. IEEE Spectrum Bitcoin: The Cryptoanarchists’ Answer to Cash  
<https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash>

Journal of Cryptology: January 1991, Volume 3, Issue 2, pp 99–111

How to time-stamp a digital document

1. Haber, S. & Stornetta, W.S. J. Cryptology (1991) 3: 99. <https://doi.org/10.1007/BF00196791>

[The Double Spending Problem and Cryptocurrencies](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174). *Banking & Insurance Journal.* Social Science Research Network (SSRN).

<https://www.wsj.com/articles/the-eureka-moment-that-made-bitcoin-possible-1527268025>

Khan Academy. <http://www.youtube.com/user/khanacademy>

Scott Driscoll. How Bitcoin Works Under the Hood.  
<http://www.imponderablethings.com/2013/07/how-bitcoin-worksunder-hood.html>

Adam Back. Hashcash. <http://www.hashcash.org/>

Galvin, David. "IBM and Walmart: Blockchain for Food Safety." *PowerPoint presentation* (2017)  
<https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/6%20Using%20Blockchain%20for%20Food%20Safe%202/$file/6%20Using%20Blockchain%20for%20Food%20Safe%202.pdf>