



Journey of Blockchain Technology leading to Bloccounting

*Amreen Khan

**Prof. Shurveer S. Bhanawat

*Project Fellow, Department of Accountancy and Business Statistics, Mohanlal Sukhadia University, Udaipur, Rajasthan. Email Id: rusa21_amreen@mlsu.ac.in and 1993khanamreen@gmail.com, Contact no. 9119303918

**Head and PI, Department of Accountancy and Business Statistics, Mohanlal Sukhadia University, Udaipur, Rajasthan. Email Id: Shurveer@gmail.com,

Abstract

The article discussed the journey of Blockchain Technology in three phases starting from 1979 in chronological order. Most of the literature available credited W. Scott Stornetta and Stuart Haber as the early contributors and founding fathers of Blockchain Technology and then acknowledged Satoshi Nakamoto for introducing this underlying technology through Bitcoin. However, by thoroughly looking at the major technological developments that took place from 1970s, a lot of prominent work came to the notice, which was required to be highlighted. The objective behind writing this article is to briefly show the evolution of this technology and how eventually it become so dynamic. Lastly the paper discussed the application of Blockchain in triple entry bookkeeping, covering the benefits of using Blockchain in bookkeeping. Also, the paper reviewed few studies which have shown how practically accounting can be merged with Blockchain and the conclusion is drawn based on these studies.

Keyword: Blockchain technology, Smart Contract, Triple entry bookkeeping, Triple entry accounting, Bitcoin, Ethereum, Digital signature, Distributed Ledger

Introduction

The blockchain symbolizes a shift in power from the centers to the edges of the networks - William Mougayar

Blockchain Technology is not the result of a few years but it is a result of a few decades of technological development. The journey of Blockchain technology can be classified in three phases.

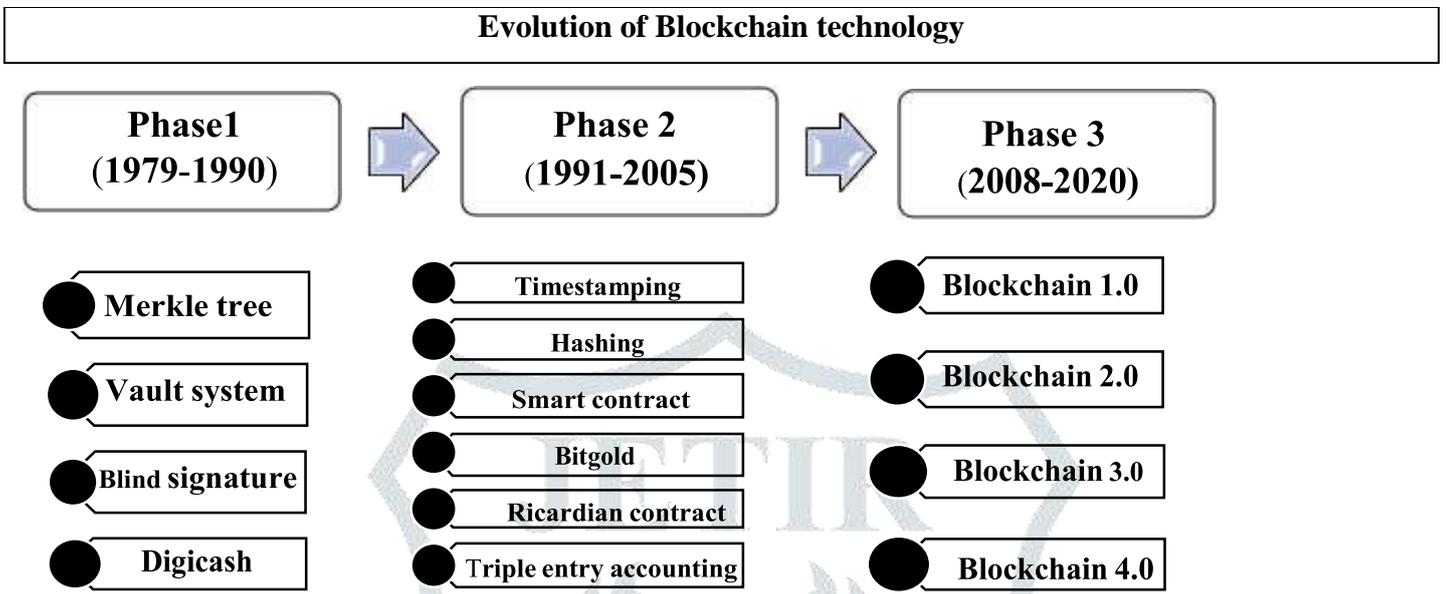


Figure 1: Evolution of Blockchain technology

Own created

Phase 1 (1979 to 1990) Early phase of the evolution

Merkle tree (1979) - Every new technology owes its presence from the previous technologies so is the case of Blockchain technology. The idea of an immutable chain of blocks of information with a cryptographic hash function appeared in the 1979 dissertation “A Certified Digital Signature” by Ralph Merkle. He explained how information can be linked in a tree structure which is now termed as a Merkle hash tree ¹⁵(**Sherman, et al., 2018**). Certified Digital Signature or the Merkle tree allowed the cheap and reliable encryption of data by converting, or hashing, blocks of information into long strands of unique code. This method of hashing blocks of information is the core of both the bitcoin blockchain and the Ethereum blockchain ⁴(**CoinDesk, 2016**).

Vault system (1982) - The next recognizable contribution was given by American computer scientist and Cryptographer “David Chaum”, who first proposed a blockchain-like protocol in his 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups" ¹⁵(**Sherman, et al., 2018**).

In his thesis, he offered a system design that use cryptographic techniques for the groups that do not trust each other ²(**Chaum, 1982**). He also introduced a very new type of cryptography “Blind signature” in 1983 which allowed the realization of untraceable payments which offered improved auditability, control and also increased privacy ³(**Chaum,1983**). He also founded the First electronic cash company named “Digicash” in 1990 that developed the first digital currency e-cash¹(**Abrar, 2015**).

Phase 2 (1991 to 2005) Rapid Developmental phase of the evolution

Timestamping (1991) - The major contribution with regard to blockchain technology was made by Stuart Haber and W. Scott Stornetta. These two scientists are the founding father of Blockchain technology ⁹(Iradale, 2020). In the year 1991, they wrote a paper “How to Time-Stamp a Digital Document,” and proposed a computationally practical procedure for digital time Stamping of documents such that it becomes infeasible to either backdate or forward date any document. Thus, making tampering of data impossible⁸(Haber & stornetta, 1991), and further in 1992, they upgraded their timestamping method by incorporating Merkle tree enabling multiple documents to be stored in one block ⁹(Iradale, 2020) ²¹(Partida, 2021).

Their work had a great significance in the development of blockchain technology as “Timestamping” and “Hashing” are the core feature of blockchain.

Hashcash (1992) - Adam Back, a cryptographer introduced the proof of work in 1992. In his paper “Hashcash: A denial-of-service countermeasure”, he introduced a proof of work system which was used to limit email spam and denial of service attacks. The system checks that a selectable amount of computing time has been taken to generate the stamp and send the email so it is less likely that the email sender is a spammer. This proof of work algorithm was used in Bitcoin in the mining process ¹⁰(Lielacher, 2018).

Smart contract (1997) - Nick Szabo, a computer scientist, cryptographer, and legal professional, proposed the Smart contract. In his research paper, “The idea of smart contracts” (1997) he stated that contractual clauses can be embedded in the hardware and software in such a way that breach of contract becomes expensive for the breacher ¹⁷(Szabo, 1997). This very innovative idea of smart contract was later used as a core feature by Ethereum in its blockchain with some modifications. Presently, the smart contract works like an “if-then” statement condition, which is automatically executed when conditions are met and the contract runs across every node in a blockchain in a decentralized way ¹¹(Meijer, 2020). In 1998, Szabo designed a mechanism for a decentralized digital currency which he called Bit gold. As he considered that money has a major problem of dependency on a trusted third party for its value. Although, Bit gold was a great idea but unfortunately it could never be implemented, but Bitgold is considered a precursor of Bitcoin ¹⁴(Sharma, 2021) ¹²(Moskov, 2018) ²⁰(Medium.com, 2020).

Ricardian Contract (2004) - Nick Szabo’s smart contract was highly appreciated but it has one biggest limitation that it was only machine-readable and this drawback was removed by the Ricardian Contract which was both in text and machine language. It was introduced by Ian Grigg, a financial cryptographer ⁶(Grigg, 2004).

Triple entry accounting (2005) - Then came the very significant and relevant contribution both in the field of technology and accountancy. Ian Grigg redefined the concept of “triple-entry bookkeeping”, the term which was initially coined by Yuji Ijiri in 1982 in his monograph “Triple entry Bookkeeping and Income Momentum”. In the paper “Triple Entry Accounting” (2005), Grigg explained TEA as a system in which digitally signed receipt was attached with double-entry bookkeeping. He argued that digital signature conferred more probative force to the receipt, thus it is more powerful than double-entry records. The triple-entry system required transaction processing to be authorized by a neutral intermediary, with each party, that is the two parties

involved in the transaction and the intermediary, creating a record for the transaction. Thus, resulting in three entries ⁷(Grigg, 2005). However, it suffered from the drawback that the mechanism required an independent and reliable intermediary to verify each individual transaction. Also, the entries stored by the intermediary were exposed to the risk of loss or unauthorized changes due to cyber-attacks ⁵(Dai & Vasarhelyi, 2017).

Phase 3 (2008 to 2020) Advent of Blockchain Technology

Blockchain 1.0 (2008) – Blockchain 1.0 originated from the concept of Digital Ledger technology. An unidentified person named “Satoshi Nakamoto” conceptualized the first Blockchain. Nakamoto released his white paper “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008). He explained Bitcoin as electronic cash that would allow transfer from one person to another without involving any third party or intermediary. They used digital signature which ensured strong control over ownership and the problem of double-spending was solved by a peer-to-peer network that used proof-of-work¹³(Nakamoto, 2008). The application of Blockchain was limited to only cryptocurrency in this era ¹⁶(Swan, 2015).

Blockchain 2.0 (2015) – Vitalik Buterin extended the concept of Blockchain beyond cryptocurrency by introducing Ethereum which was based on the concept of smart contract along with proof of work consensus mechanism and it also used its own cryptocurrency Ether ¹⁸(Mukherjee & Pradhan, 2021).

The major limitation of first and second generation Blockchain were Poor scalability, based on Proof of Work and take excess of time to confirm transactions.

Blockchain 3.0 (2016) – Third generation of Blockchain was deliberately build to facilitate wider range of applications and activities such as in logistics, finance, banking, construction business, healthcare, recordkeeping etc. The blockchain of third generation introduced linking the IOT devices with the blockchain ⁵(Dai & Vasarhelyi, 2017). It aimed to improve the scalability, interoperability, privacy and sustainability of previous generations, designed on the “FFM” concept which is the acronym for Fast, Feeless and Minerless ¹⁸(Mukherjee & Pradhan, 2021).

Blockchain 4.0 (2018) – The fourth generation of Blockchain is the latest which has made the technology fully mainstream with the possibility of inculcating Artificial Intelligence (AI) with the Blockchain and is ready to deliver blockchain as a business-usable environment for creating and running application¹⁸(Mukherjee & Pradhan, 2021).

Table 1 Chronological development and Contributors in relevance to Blockchain Trechnology

Year	Area Of Development	Major Contributors
1979	Merkle Tree / Certified Digital Signature	Ralph Merkle
1982	Vault system	David Chaum
1983	Blind Signature	David Chaum
1990	Digicash (First electronic cash company that developed the first digital currency ecash)	David Chaum

1991	Time stamping digital records and Merkle tree	Stuart Haber and W. Scott Stornetta
1992	Hashcash	Adam Back
1994	Smart contract	Nick Szabo
1996	Ricardian Contract	Ian Grigg
1998	B Gold	Nick Szabo
1998	B money	Wei Die
2005	Triple entry Accounting	Ian Grigg
2008	Blockchain 1.0 - Transactions	Satoshi Nakamoto (Bitcoin)
2013	Blockchain 2.0 - Contracts	Vitalik Buterin (Ethereum)
2016	Blockchain 3.0 – linking with IOT devices	
2018	Blockchain 4.0	

Blockchain and Triple Entry Bookkeeping (Blockkeeping)

In this article, the integration of Blockchain with Triple entry Bookkeeping is given the new term called as “**Blockkeeping**”. This term is selfmade and is used to give the clarity of Triple entry bookkeeping in reference to Blockchain.

The concept of triple entry system given by Grigg was modified and used in Blockchain to record accounting transaction. Triple entry bookkeeping is a simple idea. When the transaction is carried out, a receipt is signed through digital signature. So, it is assumed that throughout the Blockchain each user had a unique and non-transferable digital signature. Also, it gives an improvement to the current system as the accounting entries made by the companies are visible to the parties involved and are cryptographically sealed by a “third entry”, made by the network itself. The final receipt has the digital signatures of all the parties, and serves as a valuable proof of transaction: that is the “third entry”¹⁹ (Pedreño et al., 2021).

The above concept can be explained with the example: In Traditional system of Bookkeeping



However, in Blockchain, both parties will digitally sign a receipt, in which they confirm that the goods have been delivered in exchange for the stipulated price. The issued receipts A and B become an encrypted and unmodifiable proof of the transaction through Blockchain.

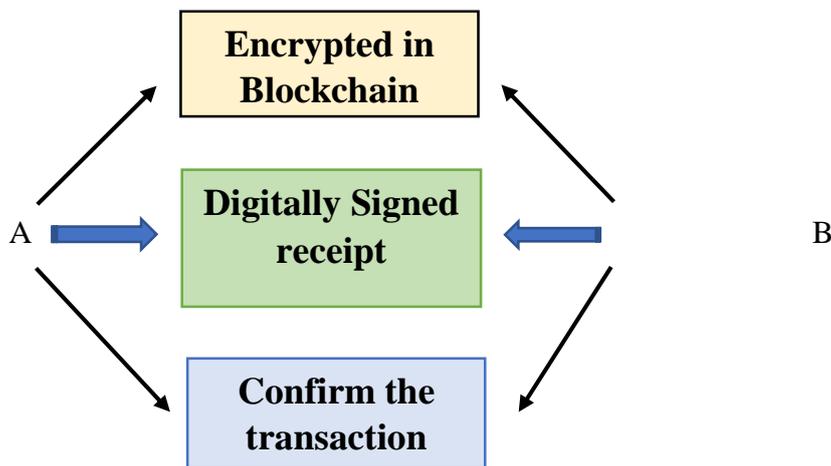


Figure 2: Recording Transaction in Blockchain

Source: Own

Benefits of Blockkeeping

1. It will ensure ease in reconciliation, trust, transparency and ease of auditing by maintaining an unbiased record.
2. There is no need to have an internal company accountant, or an external auditor or expert to issue documentary evidences.
3. The validity of accounting entries is guaranteed by the information contained in the network itself and no longer by mutual control between parties, or their internal or external auditors.
4. Entries are made directly on the blockchain, therefore recorded transactions will be more reliable as they can be easily verified and are identical for each party linked to the transaction ¹⁹(Pedreño et al.,2021).

Blockchain and Triple Entry accounting (Blocounting)

“**Blocounting**” is a self-originated term used to denote Triple entry Accounting in reference with Blockchain. Most of the papers have used triple entry bookkeeping and triple entry accounting interchangeably. But Bookkeeping is just the recording of the accounting entries in the books of accounts. It is the first level or foundation for accounting. Accounting starts where bookkeeping ends. So far it is clear that since Blockchain just works as a database, it is easy to record the transactions in the Blockchain but accounting is a higher process which involves preparation of Final accounts and the accounting software like telly and ERP are already doing this job at its best. So, the question arises why to use Blockchain for accounting. To gain some more insight of this very new and unexplored technology, few papers are reviewed.

Ibanez et al. (2018) proposed an idea: If a delivery order for a purchased product is cryptographically signed, the buyer records the cryptographically received product. A payment by virtual currency is automatically sent to the account of seller, and the transaction is automatically recorded with its payment and delivery phases by the counterpart of its consideration. And the smart contract can ensure not only the recording of the transaction

support like invoice, delivery note, virtual contract etc., but also the accounting record itself (mandatory books of accounts).

Pedreño et al. (2021) in their paper, affirmed that Blockchain is eminently an accounting technology, since data are not only archived, but also dynamically settled and ordered. They argued that Blockchain is a type of DLT with special features, but not all DLTs are Blockchain, A DLT is simply a decentralized database that is managed by various participants, and because of its broad and wide purpose, it would better adapt than Blockchain to accounting.

Jun Dai and Miklos A. Vasarhelyi (2017) attempted to present blockchain-based Realtime verifiable and transparent accounting ecosystem. They provided a potential design of blockchain based triple entry accounting information system with the help of a simple purchase sale business cycle.

Inghirami (n. d.) proposed a framework for integration of Blockchain and ERP systems. They proposed the model with three layers – physical layer, logical layer and control layer. For external transactions (with blockchain) distributed ledger technology serves as the physical layer, blockchain logic along with smart contracts play the role of logical layer and DLT logic works as the control layer.

Conclusion

- Blockchain is not the invention of today, the history covered in the paper clarifies that it is the result of technological innovations of decades.
- Blockchain is a database and it is easy to record the accounting entries of a business transaction but would it be possible to do full-fledged accounting, is still a question.
- Accounting is dynamic in nature and covers analytical part like preparation of financial statements which is possible only when it is integrated with some accounting software like ERP or Tally. Also, Blockchain-based smart contracts need to be prepared that triggers the transaction orders, like Smart contract for sale, purchase, income, expenses, payroll, tax etc.
- New Accounting standards have to be framed. How the classification of cryptocurrencies, NFT, Tokens, virtual properties will be done.
- Even if accounting will be possible in Blockchain, a company will adopt it only if its benefit will be more than its cost.
- The current scenario, shows that Blockchain is more beneficial only where bookkeeping is concerned but Accounting is doubtful.

References

¹Abrar, W. (2015). Untraceable Electronic Cash with Digicash. doi:10.13140/RG.2.1.1900.3040

²Chaum, D. (1982). Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups. 96.

³Chaum, D. (1983). Blind signature for untraceable payments. Advances in Cryptology Proceedings of Crypto. 82 (3): 199–203.

⁴Coindesk. (2016). Retrieved from www.coindesk.com:

<https://www.coindesk.com/markets/2016/06/28/the-inventor-of-the-merkle-tree-wants-daosto-rule-the-world/>

- ⁵Dai, J., & Vasarhelyi, M. A. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information systems*.
- ⁶Grigg, I. (2004). The Ricardian Contract. *IEEE Xplore*. doi: 10.1109/WEC.2004.1319505
- ⁷Grigg, I. (2005). Triple entry Accounting.
- ⁸Haber, S., & stornetta, w. S. (1991). How to time stamp a digital document. *Journal of Cryptology*.
- ⁹Iradale, G. (2020). Retrieved from Blockchain Technology History: Ultimate Guide (101blockchains.com)
- Iradale, G. (2020). Retrieved from Blockchain Technology History: Ultimate Guide (101blockchains.com)
- ¹⁰Lielacher, A. (2018, march 23). Retrieved from <https://btcmanager.com/the-history-of-bitcoin-part-1-what-is-hashcash/>
- ¹¹Meijer, C. R. (2020). Finextra. Retrieved from www.finextra.com:
<https://www.finextra.com/blogposting/19383/smart-working-with-blockchain-based-smartcontracts#:~:text=Ethereum%2C%20the%20wellknown%20global%20blockchain%20platform%20was%20the,platform%20for%20coding%20and%20processing%20of%20smart%20contracts.>
- ¹²Moskov, P. (2018). Coincentral. Retrieved from What Is Bit Gold? The Brainchild of Blockchain Pioneer Nick Szabo - CoinCentral
- ¹³Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
- ¹⁴Sharma, R. (2021). Investopedia. Retrieved from www.investopedia.com:
<https://www.investopedia.com/terms/b/bitgold.asp#:~:text=Bit%20gold%20was%20one%20of%20the%20earliest%20attempts,be%20the%20precursor%20to%20Satoshi%20Nakamoto%E2%80%99s%20bitcoin%20protocol.>
- ¹⁵Sherman, A. T., Javani, F., Zhang, H., & Golaszweki, E. (2018). On the Origins and Variations of Blockchain Technologies. *IEEE Security Privacy*.
- ¹⁶Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. United states of America: O'reilly.
- ¹⁷Szabo, N. (1997). The Idea of Smart Contracts. Satoshi Nakamoto Institute. Retrieved from <https://nakamotoinstitute.org/the-idea-of-smart-contracts/>
- ¹⁸Mukherjee, P., & Pradhan, C. (2021). Blockchain 1.0 to Blockchain 4.0—The Evolutionary Transformation of Blockchain Technology. In *Blockchain Technology: Applications and Challenges*. Springer Nature Switzerland AG 2021. doi:DOI: 10.1007/978-3-030-69395-4_3
- ¹⁹Pedreño, E. P., Gelashvili, V., & Nebreda, L. P. (2021). Blockchain and its application to accounting. *Intangible Capital*.
- ²⁰(2020). Retrieved from Medium.com: [https://medium.com/bitcoin-news-today-gambling news/nickszabo-a-living-crypto-legend-b231bc04b72f](https://medium.com/bitcoin-news-today-gambling-news/nickszabo-a-living-crypto-legend-b231bc04b72f)
- ²¹www.bitcoin.org, Partida, D. (2021). Retrieved from the history and evolution of blockchain (swissborg.com)