* Topic - The Rise of Cryptocurrencies: Exploring the Power of Blockchain
* Introduction and Background – Aaron

**History**

Stuart Haber and W. Scott Stornetta envisioned what many people have come to know as blockchain, in 1991. Their first work involved working on a cryptographically secured chain of blocks whereby no one could tamper with the timestamps of documents.

In 1992, they upgraded their system to incorporate [Merkle trees](https://101blockchains.com/merkle-trees/) that enhanced efficiency thereby enabling the collection of more documents on a single block. However, it is in 2008 that Blockchain History starts to gain relevance, thanks to the work of one person or group by the name of Satoshi Nakamoto. [Satoshi Nakamoto](https://101blockchains.com/who-is-satoshi-nakamoto-bitcoin/) is accredited as the brains behind blockchain technology. Very little is known about Nakamoto as people believe he could be a person or a group of people that worked on [Bitcoin](https://101blockchains.com/bitcoin-guide/), the first application of digital ledger technology.

Nakamoto conceptualized the first blockchain in 2008 from where the technology has evolved and found its way into many applications beyond [cryptocurrencies](https://101blockchains.com/what-is-cryptocurrency/). Satoshi Nakamoto released the first whitepaper about the technology in 2009. In the whitepaper, he provided details of how the technology was well equipped to enhance digital trust given the [decentralization](https://101blockchains.com/decentralization-in-blockchain/) aspect which meant nobody would ever be in control of anything.Ever since Satoshi Nakamoto exited the scene and handed over Bitcoin development to other core developers, the digital ledger technology has evolved resulting in new applications that make up the blockchain History.

**What is Blockchain Technology?**

In the simplest terms, Blockchain can be described as a data structure that holds transactional records and while ensuring security, transparency, and decentralization. You can also think of it as a chain or records stored in the forms of blocks which are controlled by no single authority. A blockchain is a distributed ledger that is completely open to any and everyone on the network. Once an information is stored on a blockchain, it is extremely difficult to change or alter it.

Each transaction on a blockchain is secured with a digital signature that proves its authenticity. Due to the use of encryption and digital signatures, the data stored on the blockchain is tamper-proof and cannot be changed.

Blockchain technology allows all the network participants to reach an agreement, commonly known as consensus. All the data stored on a blockchain is recorded digitally and has a common history which is available for all the network participants. This way, the chances of any fraudulent activity or duplication of transactions is eliminated without the need of a third-party.

To understand blockchain better, consider an example where you are looking for an option to send some money to your friend who lives in a different location. A general option that you can normally use can be a bank or via a payment transfer application like PayPal or Paytm. This option involves third parties to process the transaction due to which an extra amount of your money is deducted as transferring fee. Moreover, in cases like these, you cannot ensure the security of your money as it is highly possible that a hacker might disrupt the network and steal your money. In both the cases, it is the customer who suffers. This is where Blockchain comes in.

Instead of using a bank for transferring money, if we use a blockchain in such cases, the process becomes much easier and secure. There is no extra fee involved as the funds are directly processed by you thus, eliminating the need for a third party. Moreover, the blockchain database is decentralized and is not limited to any single location meaning that all the information and records kept on the blockchain are public and decentralized. Since the information is not stored in a single place, there’s no chance of corruption of the information by any hacker.

**How does Blockchain work?**

A blockchain is a chain of blocks that contain data or information. Despite being discovered earlier, the first successful and popular application of the Blockchain technology came into being in the year 2009 by Satoshi Nakamoto. He created the first digital cryptocurrency called Bitcoin using Blockchain technology. Let’s understand how a blockchain works.

Each block in a blockchain network stores some information along with the hash of its previous block. A hash is a unique mathematical code which belongs to a specific block. If the information inside the block is modified, the hash of the block will be subject to modification too. The connection of blocks through unique hash keys is what makes blockchain secure.

While transactions take place on a blockchain, there are nodes on the network that validate these transactions. In Bitcoin blockchain, these nodes are called as miners and they use the concept of proof-of-work to process and validate transactions on the network. For a transaction to be valid, each block must refer to the hash of its preceding block. The transaction will take place only and only if the hash is correct. If a hacker tries to attack the network and change information of any specific block, the hash attached to the block will also get modified.

The breach will be detected as the modified hash will not match with the original one. This ensures that the blockchain is unalterable as if any change which is made to the chain of blocks will be reflected throughout the entire network and will be detected easily.

In a nutshell, here’s how blockchain allows transactions to take place:

1. A blockchain network makes use of public and private keys to form a digital signature ensuring security and consent.
2. Once the authentication is ensured through these keys, the need for authorization arises.
3. Blockchain allows participants of the network to perform mathematical verification and reach a consensus to agree on any value.
4. While making a transfer, the sender uses their private key and announces the transaction information over the network. A block is created containing information such as digital signature, timestamp, and the receiver’s public key.
5. This block of information is broadcasted through the network and the validation process starts.
6. Miners all over the network start solving the mathematical puzzle related to the transaction to process it. Solving this puzzle requires the miners to invest their computing power.
7. Upon solving the puzzle first, the miner receives rewards in the form of bitcoins. Such kind of problems is referred to as proof-of-work mathematical problems.
8. Once most nodes in the network come to a consensus and agree to a common solution, the block is time stamped and added to the existing blockchain. This block can contain anything from money to data to messages.
9. After the new block is added to the chain, the existing copies of blockchain are updated for all the nodes on the network.

**Blockchain Characteristics and Components**

1. Ledger: Any file with a constantly growing record related to the transaction.
2. Permanent: transaction means that once the transaction goes inside a Blockchain, it is stored permanently in the record and immutable.
3. Secure: Information is stored securely through this technology as highly advanced cryptographic techniques are used to ensure that your information is locked within the Blockchain.
4. Chronological:  It means every transaction occurs after the previous one.

* Scope of the study

**What is Cryptocurrency?**

Cryptocurrency is made up of two words- crypto and currency. While the meaning of currency is clear that it is money, crypto means encrypted or written in codes. So, the meaning of a cryptocurrency is that it is a digital asset that has a value like money. It is created to foster easy exchange, and that’s where blockchain comes into the picture. All the crypto transactions that take place are recorded using blockchain technology. The first ever cryptocurrency was Bitcoin, which became synonymous with blockchain. Since then, thousands of cryptocurrencies have entered the market.

**Blockchain and Cryptocurrency**

The blockchain of a cryptocurrency is the master ledger that generally records all prior transactions and activities, validating the ownership of all units of the currency at any given point in time. The blockchain contains the entire transaction history of a cryptocurrency as a record. It has a finite length containing a finite number of transactions that eventually surge in due course of time. Identical copies of the blockchain are stored in every node of the cryptocurrency’s software network. This network of decentralized server farms is managed by tech-savvy individuals or groups of individuals known as miners. Miners continually record and authenticate cryptocurrency transactions. A blockchain currency transaction technically isn’t necessarily finalized until it has been added to the blockchain. Once the transaction is finalized, it is usually irreversible. Unlike traditional payment processors, such as PayPal and credit card modes of transactions, most cryptocurrencies have no built-in refund or chargeback functions.

While cryptocurrency transactions depict security, there are certain aspects that question the authenticity of their existence. To mitigate these allegations of authenticity, there was a need to develop a foolproof technology that would not only make online cryptocurrency transactions safe but also construct an impregnable firewall through which hackers can’t penetrate. This is where the blockchain took the center stage. Apart from providing a secure platform, blockchains also ensured that transparency is the key to all cryptocurrency transactions. With blockchains, any person on the Internet can have a sneak of transactions that have happened on a cryptocurrency unit since its inception. This allows users to transparently traverse through transactions. Also, the ledger can be copied onto every computer in the world. This means that there exists no centralized place which a hacker can leverage to tamper with transactional data.

* Literature reviews and supporting information supporting the group position
  + Technology Observations - Aaron
* Conclusion and Recommendation

Blockchain technology has revolutionized the world of cryptocurrencies, offering numerous benefits such as decentralization, transparency, immutability, and security. Cryptocurrencies built on blockchain networks have gained significant attention and adoption in recent years. However, it is important to note that the cryptocurrency market is highly volatile and can be subject to regulatory challenges and security risks.