Blockchain Technology and Security

Alexander Hickey and Brandon Crosier

Introduction

- What is a Blockchain?
- Types of Blockchain Networks
- Current Blockchain Uses
- Inherent Blockchain Security Measures
- Current Blockchain Security Measures
- Practical Implications
- Conclusion

What is a Blockchain?

A Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a network.

Simply put, it is a chain of blocks; each digital block contains records of transactions.

Assets can be tangible like a house or a car.

Assets can be intangible like a patent or a copyright.

You can track and trade virtually anything with a blockchain network.

Reducing Risk and lowering Cost

Types of Blockchain Networks

Public Blockchain Networks

Can be joined by anyone

Examples: Bitcoin, Ethereum

Private Blockchain Networks

Similar to a public network but one party controls the network

- Decides who can join the network

Could be used by a Corporation

Types of Blockchain Networks (continued)

Permissioned Blockchain Networks

Can be a private or public network

Places restrictions on who can participate and in what transactions

Need to receive an invitation or permission to join

Consortium Blockchain Networks

These networks are shared by multiple organizations

Pre-selected organizations determine who can access data and participate in transactions

Ideal for businesses in which all organizations need permission and all have shared responsibility for the blockchain

Current Blockchain Uses

Banking & Finance

- Santander One Pay FX
  - first blockchain-based money transfer service
  - Allows customers to make same-day international money transfers

Capital Markets

- With the use of Blockchain technologies in Capital markets you could have
  - Faster clearing and settlement
  - Consolidated audit trail
  - Operational improvements

Current Blockchain Uses (continued)

Supply Chain management

- Blockchain ledger is well suited to supply chain management tasks such as
  - Queuing events
  - Sending newly acquired goods to multiple locations

Healthcare

- Could be used to store health information such as
  - Age
  - Gender
  - Basic medical history
- None of this information can be used on its own, so it is safe to store it in a blockchain.

Inherent Blockchain Security Measures

A blockchain is a chain of digital blocks that represent records of transactions.

Each digital block is connected to all the blocks that precede it and come after it.

Makes it hard to manipulate a singular record *and* remain undetected

Would need to change both the target block and any connected blocks *simultaneously*

Transaction records are secured with cryptography.

Private keys named digital signatures.

Any alteration will render the digital signature and all relevant addresses invalid.

Blockchains are decentralized.

No central location to attack

Would require massive amounts of computing power to make a dent

- Or at least a 51% majority…

Current Blockchain Security Measures

Building a Business Network

- Public blockchains connect via public internet.
  - Therefore, private blockchains are inherently more secure.
  - Favor anonymity
- Private blockchains only permit known parties or organizations.
  - Business network is formed with a members-only private blockchain.
    - Members are organizations
    - Favor identity confirmation
- Consortium Blockchain Networks

Consensus

- Agreement on a transaction being authentic
- In private blockchain, consensus is reached by agreement between members.
- In Bitcoin, a public blockchain, consensus is achieved through *mining*.

Current Blockchain Security Measures (continued)

Mining

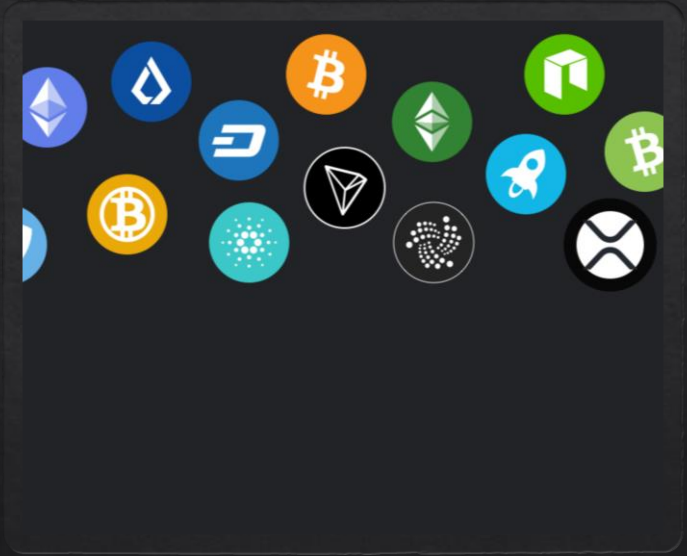
- Used in most cryptocurrencies
- How tokens are added to the market
- “Miners” act as auditors who reach consensus on the legitimacy of transactions.
  - Ensure there is no double-spending
    - Using the same tokens for two or more purchases.
  - Miners must produce a hash that is less than or equal to the target hash.

Infrastructure Security Implementations

- Preventing parties, including admins and root users, from accessing sensitive information
- Disallow attempts at manipulating data within a network
- Ensuring high-grade security standards are put in place for encryption keys
  - Make sure keys are not misused
- Recommended for any blockchain, public or private

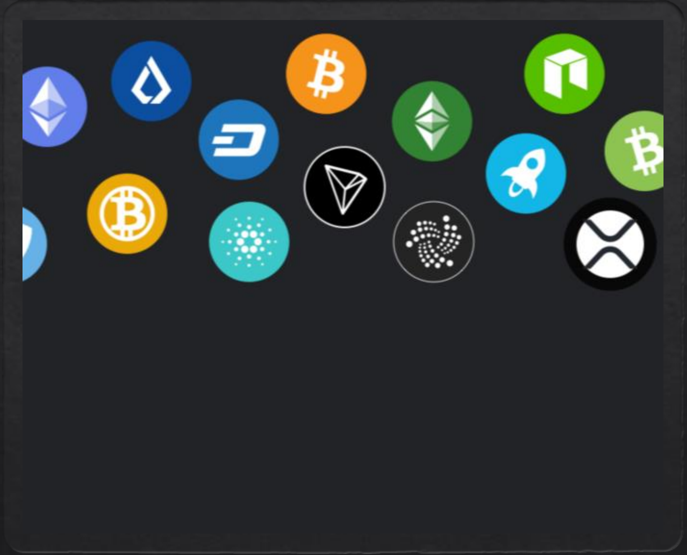
Practical Implications

- Increased access to blockchain technology and increased security in blockchain can result in a multitude of positives.
  - File storage
    - Storing data on decentralized platforms
  - Staking
    - Another form of reaching consensus (like mining) by placing current funds on a hold.
    - Adds even more security due to a greater ability to participate in auditing
  - Use-case specific currencies
    - Greater introduction to currencies that back operations or projects rather than simple ledger technologies like Bitcoin
    - Filecoin, Numeraire, DAOs, APIs



Practical Implications (continued)

- Greater access to blockchain technologies and greater security translates to greater trust.
  - Blockchains as decentralized forms of finance, data storage, and other uses relies on the amount of faith in the system that is given by those involved.
  - The more involved, the more faith
  - The more faith, the greater impact
  - It all starts with trust (security)
- The public network side of blockchain can improve
  - Stands to gain the most from greater security and implementation
    - More mining, staking
    - Greater participation



Conclusion

- A Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a network.
- Types of Blockchain Networks
  - Public
  - Private
  - Permissioned
  - Consortium
- Current Blockchain Uses
  - Banking and Finance
  - Capital Markets
  - Supply Chain Management
  - Healthcare

Conclusion (continued)

- Blockchain Security Measures
  - Inherent
  - Implemented
- Practical Implications
  - Technology and greater access to it
  - Security and greater trust

What is Blockchain?

"What is blockchain?" – this is a question asked by many individuals, tech-savvy or not. Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a network. In other words, blockchain is a specific type of database and is different from a typical database because of the way it stores data. Data that comes into the database is entered in a new block and when the block is filled it is chained into the previous block.

By doing this the data is chained together in chronological order. A block is a group of information that holds a set of instructions. Blockchain databases can store many different types of data. The data can be tangible or intangible. An example of tangible data that could be stored is something like a house or a car. An example of intangible data that could be stored would be something like a patent or copyright. Blockchain as a medium can be used to trade virtually anything like and you can easily trade tangible and intangible objects. This means there are many ways that blockchain technology can be implemented.

Types of Blockchain Networks

There are many ways that a person or a company could implement blockchain technology and many popular ways such technologies can be implemented. There are public blockchain networks, private blockchain networks, permissioned blockchain networks, and consortium blockchain networks. A private blockchain network is a blockchain network that can be joined by anyone that wants to join. An example of a private blockchain network would be Bitcoin or Ethereum. Bitcoin and Ethereum are both well-known examples of blockchain technology and most people do not understand that they use blockchain technology.

However, since they are public networks there is little to no privacy available for transactions, and security is typically weaker than other types of blockchain networks. They also typically require a substantial amount of power to operate. Another popular type of blockchain network is a private blockchain network. A private blockchain network operates and functions the same as a public blockchain network. However, it has the added security benefit of being private. Meaning the owner or operator of the network gets to decide who can join the network. These types of networks are typically used by a corporation.

A third popular type of blockchain network is a permissioned blockchain network. These types of blockchain networks can be as a public or private database managed by a person or corporation. A permissioned blockchain network places a restriction on who can join the network and who can participate in a transaction. They even have the power to choose what specific transaction a user can be a part of. You are required to receive an invitation or permission to join these types of blockchain networks.

The final popular type of blockchain network is a consortium blockchain network. These are blockchain networks that are shared by multiple people or organizations. Typically, these types of blockchain networks have a pre-selected individual or organization who can determine who and what data can be accessed. They also control who can participate in transactions similar to a permissioned blockchain network. A consortium blockchain network is ideal for businesses where all organizations need permission to the database, and all have shared responsibility within the specified blockchain network.

Current Blockchain Uses

Blockchain technology is being used in many different business sectors. These sectors include banking & finance, capital markets, supply chain management, and even healthcare. Blockchain technology has been used in Banking & Finance and an example of this could be Santander One Pay FX. This was the first blockchain-based money transfer service and was founded by Banco Stander. Banco Stander is a leading retail & commercial bank. This service allows customers to make same-day or next-day international money transfers. This service was made possible with the use of blockchain technology by automating the entire process and reducing the number of intermediaries required.

Capital Markets are also set to benefit from the use of blockchain technology. With the use of blockchain technology companies and organizations in the capital market sector will be able to improve clearing speed and settlement time. Blockchain technology will also allow companies to consolidate the audit trail improving the efficiency of this process. It can also lead to overall operational improvement.

Blockchain Applications in Business

Supply chain management also stands to face large improvements from blockchain technologies because this technology allows a new and dynamic way for companies to track and use their data. Supply chain management should improve because the blockchain ledger is well suited to supply chain management tasks. These tasks could include queuing events to improve supply chain efficiency and sending newly acquired goods to multiple different shipping locations.

Healthcare like supply chain management also stands to face large improvements from blockchain technologies. It stands to face large improvements because blockchain technology is well suited for storing basic health information like age, gender, or basic medical history. Blockchain technology is well suited for this because all this information could be stored on a private or public network and because none of this data would be useful on its own it does not breach a patient's privacy.

Blockchain technologies are already being used by many different companies in the health care industry such as the FDA and Pfizer. The FDA is using blockchain technology by using a Hyperledger to create a platform to secure all kinds of healthcare data. This data could include things such as genomic data, electronic medical records, and various forms of demographic data.

The Hyperledger is an open-source project that was created by a collaboration of over 260 major organizations. Hyperledger projects have been adopted by over ten major organizations including the FDA and T-Mobile, and the London Stock Exchange. Pfizer, along with Biogen, are both large companies leading the blockchain technology charge in the healthcare industry. They both lead the Clinical Supply Blockchain Working Group (CSBWG), and recently they have successfully shown you can track records and manage the digital inventory of pharmaceutical products.

Inherent Blockchain Security Measures

To reiterate, A blockchain is a chain of digital blocks that represent records of transactions. Each of these digital blocks is connected to all the blocks that precede it and come after it, forming a chain of blocks, as the moniker implies. This implementation makes it especially hard for hackers-to-be to both manipulate a singular record and remain undetected during the process. Although this operational policy might seem like a weak deterrent on its own, it is only the tip of the iceberg when it comes to security measures that are inherent to blockchain technology.

Blockchain comes with many more forms of inherent tamper deterrence. Another such form is the use of securing through cryptography. Each participant in a particular network comes equipped with his or her own private key. Each private key is assigned to the individual transactions they make and pose as what is known as the personal "digital signature". In the event that a transaction record of any kind is manipulated or tampered with, the digital signature will be rendered invalid, and all participants within the peer network will be aware of the attempt.

Another important inherent security feature that is included in the blockchain experience is the fact that it is decentralized. This means that blocks within a blockchain are distributed throughout peer-to-peer networks. These blockchains are constantly and consistently updated and kept in a synchronous environment. Blockchains do not have centralized location, hence the "decentralized" adjective – this means that blockchains do not possess a single point of failure and will not be changed simply using a single computer. Accessing virtually every instance of a blockchain in the decentralized, synchronous environment would require a substantial amount of computational power. On top of that, each block would need to be changed simultaneously to avoid detection.

One flaw in this security feature is that, although a huge amount of computing power would be required to access every instance of a blockchain, there are ways to hack into one with only a 51 percent majority – that is, having enough computational power to access and manipulate at least over half of all the digital blocks within a blockchain simultaneously, which is vastly easier than doing all of them at the exact same time. Although gaining a 51 percent majority would still be very difficult, it begs these questions: does this mean that smaller blockchains are inherently vulnerable? Could large blockchains with heavy amounts of stakeholders become increasingly more vulnerable over time as technological strides continue to make large amounts of computational power more accessible? Such questions have raised debates over the past several years, with no definitive answer having been reached in the blockchain community yet.

Current Blockchain Security Measures

Building a business network in the context of blockchain technology brings both security measures and extraneous security needs. Remember that there are two major types of blockchain networks: public and private. Public and private blockchain networks behave differently, and differ in how much security they need, how it is implemented, and where it is chosen to be implemented. Not all blockchains are created equal – blockchains can differ in more ways than just whether they are public or private.

Public blockchains are connected to computers that receive communications via the Internet. Therefore, they are automatically less secure than private networks, since they rely on the communications of these computers to validate transaction data, bundle the records, and place them into individual blocks to be added to a ledger. Essentially, any computer with an internet connect can access a public blockchain. Public blockchains also favor anonymity, meaning the personal identity of all those involved is not a requirement at any given point in time.

Private blockchains, however, are inherently more secure than public blockchains because they favor checking for identity confirmation. In this case, the personal identities of all parties involved is very important, and only permit known parties and organizations to participate. Members of the private blockchain are usually organizations and are let in on a members-only basis. Consortium blockchains typically operate in a similar fashion when it comes to member access.

An important aspect of blockchain security is reaching something called consensus. In the context of blockchains, consensus is defined as an agreement on a transaction as being an authentic transaction. In private blockchains, consensus is reached by an agreement that the transaction is authentic between members. This process may take little to no time, or can take a while, depending on the circumstances. In public blockchains, consensus is reached through a process called mining.

Mining is used in most cryptocurrencies, and many people, tech-savvy or not, have heard the term at least once before. One aspect of mining is that it rewards those who participate with a certain allotted number of tokens for the relevant cryptocurrency. This is, however, only half of the importance of the process of mining. Mining is also used as the primary form of consensus in a public blockchain. “Miners” act as auditors who reach a consensus on the legitimacy of transactions, similarly to how it is reached by members within a private blockchain. Miners must solve complex equations using algorithms to produce a hash that is less than or equal to the target hash, typically using a computer with a high hash rate. The more computational power, the higher hash rate.

Businesses and blockchains also implement a multitude of other infrastructure security processes and policies. One such implementation is the policy that prevents any party, including administrators and root users, from accessing sensitive information. Another policy is to disallow any attempts at manipulating data within a network. Ensuring such high-grade security standards are put in place allows for encryption keys to never be misused and generate a net benefit for all involved parties. These policies and processes are recommended for any blockchain, public or private.

Practical Implications

Increased access to blockchain technology and increased security in blockchain can result in a multitude of positives. File storage can become a norm when it comes to blockchain technology, where users store data on decentralized platforms. Users could also participate in staking, another form of mining that does not require one to have a lot of computational power. In staking, users put their cryptocurrency funds on hold, in the hopes that it grows. This adds even more security due to a greater ability to participate in auditing. Increased access also allows for greater introduction to currencies that back operations or projects rather than simple ledger technologies like Bitcoin, called use-case specific currencies, like Filecoin, Numeraire DAOs, and APIs.

Greater access to blockchain technologies and greater security translates to greater trust. Blockchains as decentralized forms of finance, data storage, and other uses relies on the amount of faith in the system that is given by those involved. The more involved, the more faith; The more faith, the greater impact… it all starts with the trust provided by security implementations within a blockchain network. The public network sides stand to gain the most from greater security implementations because of the possibility of greater participation, and, therefore, more mining and staking, and more efficient consensus. The road to a safer and more robust world of blockchain, and the possibility of fiat currency that does not inflate and a safe data storage system begins with us.

Works Cited

Conway, Luke. “Blockchain Explained.” *Investopedia,* Investopedia, 18 Nov. 2020, www.investopedia.com/terms/b/blockchain.asp.

Hong, Euny. “How Does Bitcoin Mining Work?” *Investopedia,* Investopedia, 19 Apr. 2021, www.investopedia.com/tech/how-does-bitcoin-mining-work/.

Intelligence, Insider. “The Growing List of Applications and Use Cases of Blockchain Technology in Business and Life.” *Business Insider*, Business Insider, 2 Mar. 2020, www.businessinsider.com/blockchain-technology-applications-use-cases.

“List of Top 50 Companies Using Blockchain Technology.” *101 Blockchains*, 28 Dec. 2020, 101blockchains.com/companies-using-blockchain-technology/.

Miles, Curtis. “Blockchain Security: What Keeps Your Transaction Data Safe?” *Blockchain Pulse: IBM Blockchain Blog,* 18 Dec. 2020, www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/.

“Santander Launches the First Blockchain-Based International Money Transfer Service across Four Countries.” Banco Santander.

“What Is Blockchain Technology? - IBM Blockchain.” *IBM,* www.ibm.com/topics/what-is blockchain.