Cryptocurrencies from a Cryptographic Point of View

By Myrna E. Santiago

CS 463_28691

Introduction

Cryptocurrency is nothing new. The idea of cryptocurrency and its technologies has been around since 1983. But how it came to be? Which technologies were used and which ones are in use now. It is cryptocurrencies the path to the future or another scheme about to meet its end. Many have heard about cryptocurrencies but they do not understand how it works, the technologies needed and how future technologies can be use to create a more permanent change. This research will explore and shed light into the cryptographic technologies used to sustain cryptocurrencies.

What is Cryptocurrency?

Cryptocurrency can be considered a digital or virtual asset. It is a type of currency that is protected by cryptography. Cryptocurrency allows conducting a secure transaction online. Its technology is decentralized protecting against single point of failure thanks to being distributed by a large number of computers. Over the last few years many groups have come with different currencies, similar in nature but with different names. The most famous one is Bitcoin. Other ones are Ethereum, Ripple, Cardano, Dogecoin, Polktadot, and Solana.

What are a blockchain and a block?

To understand cryptocurrencies, we need to understand its components. Blockchain acts as a ledger. A ledger is a permanent record where a company writes down its spending and gains. It should be correct and tampered free. Like a ledger the a blockchain is a series of files connected together in a form of a string or net-like structure.

Investopedia [7] describes a blockchain as scripts that enter, access, saves and stores data. Blockchains are distributed, which means that the data is save in multiple machines and all copies must match.

The main component of a blockchain is a block. A block records the most recent transaction data to be validated. Once data is validated, the block is closed and the next one is created. One important aspect of a block is that the data within cannot be alter or removed, once written. Another characteristic of blocks is that the information needs to be verified by the network before a new block can be created. A block contains encrypted information from other blocks as well as new information.

Elements inside a block includes:

- **Magic number** – specific values that shows that the blocks belong to a particular network.
- **Block size** – sets the size of the block and its limits.
- **Block header** – block information.
- **Transaction counter** – how many transactions are in a block.
- **Transactions** – all transactions within the block. It includes version, previous block hash, hash Merkle root (hash of transactions in the Merkle tree of the current block), timestamp, bits (rating of the difficulty of the nonce), and the nonce (encrypted number that the miner must solve to verified and close the block).

One fascinating thing about the heather is the nonce. It is a 32-bit number in the hash that a mining program using random numbers try to "guess". The nonce verification occurs when a number less or equal to the nonce is guess and the block is closed and a new header is created.

The creation of a block is complex. A network of computers needs to be in communication with each other in a peer-to-peer network. To create a block, miners compete with each other in order to solve a mathematical puzzle. The puzzle is called proof-of-work (PoW) algorithm, and to solve it the miners need to complete a series of calculations using the processing power of their machines. The miner that succeed receive a reward in the form of cryptocurrency and the block is added to the blockchain after being closed. A new block is created by the miner by adding the validated transactions, hash of previous blocks and unique nonce. Then the new block is broadcasted and the process restart.

A new consensus mechanism is also being use. It is called Proof-of-Stake (PoS). While PoW requires large computational requirements, PoS uses the machines of coin owners to do the work. Coins owners put their coin as collateral for the opportunity to validate blocks and earn rewards. This new method provides energy efficiency and security through community control. To validate the validators are selected at random and the validator put their own coin as collateral. Once multiple validators verify the block the block is added to the blockchain and the validators received their reward.

Because blocks are added after validation and from different points the system is distributed. Blockchains are maintained by multiple transparent participants of the network. These nodes follow a consensus algorithm protocol that add and validates new transaction blocks.

Scalability Problems

Scalability is the number of computations a network can process per second []. In a decentralized network the speed will be that of the slowest node in the network and the security depend on how many resources are needed to corrupt the network consensus.

To achieve scalability security and/or decentralization need to be sacrifice. For example, to have a faster process the number of nodes need to be reduce, which can also create a security problem because the resources that need to be corrupted are less. There is also the problem of single point of failure, if the network become more centralized.

To have a fast-decentralized network the blockchains have to be of a certain length constantly that is the only way to maintain decentralization and security, a balance needs to be achieved or alternatives need to be found. Cloud-Storage can provide data distribution, security, privacy, accessibility and ownership.

Consistency and blockchains

Blockchain technology relies on consistency, where the data in each node is the same and the nodes have a global view of the system state. To achieve consistency the consensus mechanisms ensures the same state for all participants. In distributed systems, coordination schemes are needed. These schemes are cooperative solutions that provide the nodes with the correct information. With all this in mind the consistency of a blockchain relies in the structure of its data.

Applications of blockchain technologies

One application of block chain technologies is money transfer. Block chain save a lot of money to organizations by reducing third-party fees and eliminating red tape. Examples are Cash App and Circle.

Another application is Smart Contracts. These contracts are like regular ones but the rules are enforced in real time, which provides accountability. Examples are Chainlink Labs, DFINITY and Google.

Blockchain-infused IoT prevent data breaches using virtual incorruptibility and transparency. Examples are Xage Security, used by US Air Force, Microsoft and Dell, and Helium.

Blockchain-based enterprises can help in the protection of Social Security numbers, birth certificates and other sensitive information. Civic and Ocular are examples of these enterprises.

Healthcare uses blockchain to reduce cost improve information access and streamline processes. MEDICALCHAIN and Chronicled are blockchain healthcare solutions.

A proposal for transparency in the logistics for the shipping industry is creating a good market for blockchain technology Oracle and Chain.io are some of the solutions created for this proposal.

Other applications can be seen in government, media and NFTs, with companies like Kaleido, MadHive and Candy being providers of the aforementioned.

Properties that Make Cryptocurrencies Secure

Cryptocurrencies has a specific set of properties that make them unique. By combining these properties these technologies and assets are secure and trusted. The following properties are present in cryptocurrencies [8]:

1. Decentralization – By using a network of nodes that represent users and miners, cryptocurrencies are more democratic in nature. The assets are not controlled by a single authority and consensus has to be met in order to proceed with a transaction.
2. Transparency – all transactions are transparent and publicly visible, which helps prevent fraud and provides accountability
3. Immutability - once a transaction is recorded it cannot be change or deleted, which provide a tamper-proof record. This provides trust and security.
4. Pseudonymity – this provide a balance between accountability and privacy. This is done by the use of pseudonymous addresses. The level of privacy is not complete since there are advance techniques that link users and transactions, this provides the accountability.
5. Divisibility – cryptocurrencies can be divided in smaller units that regular money cannot do.
6. Fungibility – no single coin is more valuable than other, which promotes equality.

Puzzle Solving and Cryptography

For centuries cryptography has play a part not only in war to send and receive secure messages but also for entertainment. Puzzles like cryptograms exist. These puzzles use a specific code that substitute one letter for another or a symbol until the message is discover. There are also

hashes, ciphers and mathematical puzzles like sudoku. All these puzzles required deep thinking, problem-solving and math. Since cryptography is the art of solving codes, these puzzles are part of cryptography.

These puzzles help the miners have a healthy competition with a prize at the end of it. Many miners know how complex those puzzles are and they help to keep honesty in the transactions. When multiple people get the satisfaction of solving the problem they are more incline to protect the results from tampering. Which help increase the trust of cryptocurrencies transactions.

Cryptography Technique Use in Class that are Part of Cryptocurrencies

Some of the encryption algorithms use on these technologies are Advanced Encryption Standard (AES), Rivest-Shamir-Adelman (RSA), and Elliptic Curve Cryptography (ECC) []. For example, Bitcoin uses ECC called secp256k1, with the formula $y^2 = x^3 + 7$. This method is use to generate public and private keys. It also uses SHA 256 to encrypt the data in the blocks.

Advanced Encryption Standard (AES) is a symmetric-key algorithm (uses the same key to encrypt and decrypt). It works in a 16-bytes array (4x4). Converting the plain text into a cyphertext by doing multiple rounds depending on the size of the keys.

Rivest-Shamir-Adleman (RSA) is an asymmetric-key algorithm currently mostly use to transport the symmetric keys that are shared. In this algorithm the encryption key is public and the decryption one is private. Combining this algorithm with another one we can create an extra layer of protection for our messages and cryptocurrencies.

Elliptical Curve Cryptography (ECC) is a powerful technique with variation key-length that can be use in mobile devices and regular computers. The smaller keys require less computational power. It is use in cryptocurrencies for signing transactions.

Most cryptocurrencies used combinations of technologies. These hybrid technologies provide layers of security that one cryptographic method cannot provide alone.

Advantages of Cryptocurrencies Over Other Currencies

Cryptocurrencies has some advantages over regular and other types of currencies. Some of them are:

1. Inflation Protection – Because cryptocurrencies have a hard cap their increase demand increases the price protecting against inflation and currency decline.
2. Transactional Speed – transactions are done in minutes instead of days.
3. Cost effective transactions – verification is done fast with minimal or zero cost, there is no need for third parties.
4. Decentralization – help combat monopoly and provide flow of currency.
5. Diversity – help portfolio diversification.
6. Accessibility – can be access from any device with internet access.
7. Safe and secure - because a crypto wallet private key is needed for access transactions are secure
8. Transparent – transactions can be seen in real time.
9. Privacy – through pseudonyms addresses.

Post-Quantum Cryptography and Blockchains

One of the most important aspects of blockchains is it immutability. This means that one the data is recorded it cannot be change or delete. But the data is expose and while we can not read it right know without the private key it cannot be read. The problems arise from the new quantum computers. These computers can break any current cryptography at a high speed. Which means that in the near future all these transactions will be exposed.

In response to these problems new cryptographic schemes are being created. Schemes like hash-based, code-based, lattice-based and multivariate-based that are quantum resistant are being introduce. Another possibility that is being tested are crypto-agility blockchains, which will allow the system to change algorithms without affecting functionality.

There is also the use of hard and soft fork. Forking is when an alternate version of the chain is created. Hard forks make the invalid blocks valid forcing change in the protocol. While the soft one change to a protocol that tighten the rules making some of the previous block invalid.

Conclusion

While the appeal of cryptocurrencies is high the level of risk is also high because of its volatility. Blockchains are an amazing concept and the appeal of taking back the trade is there, the need for more people its high. Banks and governments dislike the idea of this type of trading because it levels the field and takes away the power of the few to give it to the many. There are also the problems with speed and diverse technologies. In some instances, the technologies clashes or the lost of a key means the lost of everything inside the wallet. This have created a great deal of problems in recent years. The technology has a lot of potential and a great future if the currency can be stabilized and the technology problems can be solved before the next set of computers, the quantum computers become available to the public. Like any other technology, cryptocurrencies need more work, but it is running out of time.

References

1. "Blockchain Scalability: Execution, Storage and Consensus". Internet: https://chain.link/education-hub/blockchain-scalability#:~:text=One%20limitation%20of%20traditional%20blockchain,participants%20to%20achieve%20high%20security. [April 13, 2024].
2. G.R. Carrara, L.M. Burle, D.S.V. Medeiros, *et al.* "Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking". *Ann. Telecommun.* vol. **75**, 163–174 (2020). https://doi.org/10.1007/s12243-020-00751-w.
3. "Is Quantum Computing Killing Blockchains". Internet: https://btq.com/blog/is-quantum-computing-killing-blockchains. [April 14, 2024].
4. N. Tambe, A. Jain. "Advantages and Disadvantages of Cryptocurrency in 2024". Internet: https://www.forbes.com/advisor/in/investing/cryptocurrency/advantages-of-cryptocurrency/. [April 14, 2024].
5. Notomoro. "6 Best Alternatives to Blockchain for your Business". Internet: https://webisoft.com/articles/alternatives-to-blockchain/. [April 12, 2024].
6. S. Daley. "36 Blockchain Applications and Real-World Use Cases." Internet: https://builtin.com/blockchain/blockchain-applications. [April 13, 2024].
7. S. Seth. "Explaining the Crypto in Cryptocurrency". Internet:https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/#toc-the-crypto-in-cryptography. [April 14, 2024].
8. "What are Cryptocurrencies? Use Cases and Benefits." Internet: https://www.riverfronttimes.com/gaming/what-are-cryptocurrencies-use-cases-and-benefits-42128344 [April 13, 2024].