Noah Salafranca
CS 463
Project Paper
4/4/24

Introduction

Cryptocurrencies have emerged as a popular financial investment, leveraging cryptographic techniques and blockchain technology to enable secure transactions without the need for intermediaries. This study thoroughly examines cryptocurrency wallet security, concentrating on cryptographic techniques and weaknesses. It discusses basic cryptographic techniques, including public-private key pairs, digital signatures, and hash functions, showing how they contribute to cryptocurrencies' reliability, consistency, and uniqueness. Emerging technology and recent events like software vulnerabilities and key theft are discussed. By understanding these factors, users can enhance the protection of their digital assets in an evolving threat landscape.

What is Cryptocurrency?

In finance and cryptography, cryptocurrencies have become an innovative trend driven by cryptographic principles that guarantee security, transparency, and decentralization. Three of the best examples of cryptocurrency are Bitcoin, Ethereum, and Dogecoin. To fully comprehend the significance of these digital assets, it's essential to examine their cryptographic origins, procedures, and effects.

Bitcoin, the first cryptocurrency, uses cryptographic techniques to preserve the integrity and security of its transactions. Cryptographic hash algorithms, such as SHA-256, allow for the generation of unique identifiers (hashes) for each block in the blockchain, aiding tamper-resistant data storage. Digital signatures use asymmetric cryptography to validate transaction inputs and outputs, guaranteeing that only the legal owner of a Bitcoin address may begin a transfer. According to [1], Bitcoin's proof-of-work consensus algorithm uses cryptographic puzzles to validate and timestamp transactions, ensuring the blockchain record remains immutable and decentralized.

Ethereum builds on the cryptographic foundations of Bitcoin by adding the concept of smart contracts, which are self-executing agreements stored in cryptographic code. According to [2], these smart contracts allow a diverse set of cryptographic calculations and decentralized apps (dApps) to be implemented on the Ethereum network. Solidity, Ethereum's scripting language, enables the development of complicated cryptographic protocols and decentralized financial instruments such as decentralized exchanges (DEXs), token issuance, and automated market-making algorithms. Ethereum's transaction processing and state transition operations rely heavily on cryptographic hashes and digital signatures to ensure the platform's security and integrity.

While less technically advanced than Bitcoin or Ethereum, Dogecoin reflects a more humorous attitude toward cryptographic innovation. As discussed in [4], Dogecoin, which began as a joke or meme money, now uses cryptographic principles to enable quick, low-cost transactions inside its community-driven economy. Despite its comical roots, Dogecoin uses cryptographic hashes and digital signatures to establish security and immutability for its blockchain ledger. Dogecoin's thriving online community and charity efforts demonstrate the social and cultural influence of cryptocurrencies beyond their cryptographic foundations.

Noah Salafranca
CS 463
Project Paper
4/4/24

Blockchains

A blockchain is a ledger system that records transactions across several computers in a transparent, immutable, and secure fashion. Due to its anatomy, blockchains offer a high degree of openness and confidence because stored data cannot be changed or tampered with. Consensus mechanisms that power blockchains, like Proof of Work and Proof of Stake, allow agreement on the legitimacy of transactions without a central authority. Blockchains run on a peer-to-peer network, with each participant or node owning a copy of the entire ledger.

A blockchain comprises interconnected data blocks, each holding a bundle of transactions. These blocks are cryptographically connected chronologically, resulting in an immutable chain. According to [3], each block generally has the following basic components: a header, a transaction, a nonce, and a hash. The header section contains metadata such as the block's timestamp, a unique identifier, such as a hash, and a reference to the preceding block's hash, ensuring the chain's consistency. Transactions are recordings of digital transactions that include information such as sender, receiver, amount, and any other relevant data. A nonce is a random number created during the mining process essential to the proof-of-work consensus mechanism. The block's hash is a digital fingerprint produced by cryptographic techniques that ensures the block's integrity and immutability.

The link between blocks is maintained by including the preceding block's hash into each following block. This generates a chain-like structure, shown in [3], in which every change to a single block requires the modification of all subsequent blocks, making tampering obvious and practically impossible. The network's consensus mechanism determines how frequently new blocks are added to the blockchain. Users, known as miners or validators, add blocks to blockchain networks. Together, these participants run nodes in a decentralized manner to create a distributed network. Each node checks and validates transactions separately before being included in a new block. After a block is formed, it is added to the current chain and spread around the network using a procedure called consensus, in which most nodes concur that the block is authentic. For example, miners compete to solve complicated mathematical problems in proof-of-work systems such as Bitcoin, with the successful answer entitling them to add a new block to the chain. In contrast, proof-of-stake and other consensus algorithms use different techniques to choose block validators and ensure network integrity.

Blockchain maintenance is a shared responsibility among network participants, removing the need for centralized management or monitoring. Nodes in the network validate and distribute transactions to ensure consensus on the ledger. While blockchains provide significant security and decentralization benefits, they suffer from scaling issues. Scalability refers to a blockchain's capacity to manage increasing transactions and network participation while maintaining performance. While specific blockchains, such as Bitcoin and Ethereum, have encountered problems with scalability due to their consensus mechanisms and block size limits, others have layer two protocols and enhanced consensus mechanisms to increase scalability, as explained in [13]. As chains lengthen, there will be specific effects on the blockchain's performance, including more significant storage needs, longer validation times, and higher resource demands

on network nodes. Balancing scalability with security and decentralization remains a considerable challenge for blockchain developers.

Cryptocurrency Wallets

Cryptocurrency wallets are crucial tools for anybody exploring the world of cryptocurrencies. These digital tools enable users to safely store, manage, and interact with cryptocurrencies. These wallets take several forms, including software, hardware, and paper wallets, and more. Cryptocurrency wallets enable users to transfer, receive, and monitor their digital assets on the blockchain. Security is critical in the design of digital wallets, which include encryption, two-factor authentication, and backup options to protect money from illegal access or loss.

Software or digital wallets are the most prevalent cryptocurrency wallet type. These wallets are software applications that may be installed on desktops and cellphones or accessed via a web browser. They are convenient and user-friendly, suitable for both beginners and experienced users. According to [5], software wallets are classified as hot or cold depending on their internet connectivity. Hot wallets connect to the internet, providing rapid and straightforward access to money, but they are more vulnerable to hacking. Hot software wallets include Exodus, Robinhood, MetaMask, and Coinbase. Because of their ease of use, these wallets are ideal for daily transactions and regular trading. On the other hand, cold wallets are offline storage that adds additional protection by storing private keys offline, drastically lowering the likelihood of illegal access or hacking. Cold software wallets are often desktop or mobile programs that create and keep private keys on the device. They are perfect for the long-term safekeeping of significant cryptocurrency investments. Cold software wallets include Armory and Electrum.

Hardware wallets provide the most security among cryptocurrency wallets. [5] also, these physical devices, which look like USB flash drives, are designed to keep private keys offline and away from cyber dangers. Since they function independently of the internet, hardware wallets resist malware assaults and hacking attempts. To complete a transaction, users must connect the hardware wallet to a computer or smart device and approve it with a PIN or biometric identification. Popular hardware wallet brands include Ledger Nano S, Ledger Nano X, and Trezor. A drawback for hardware wallets can be the cost, which discourages some users, especially those with little cryptocurrency investments. Additionally, there is the potential for loss or damage. The cash held on the device may be permanently lost if a hardware wallet is misplaced or damaged without sufficient backup mechanisms.

Paper wallets are another type of cold storage for cryptocurrency. They include printing the public and private keys on paper and storing them securely, such as in a safe deposit box. According to [5], paper wallets operate fully offline, impervious to cyber attacks. However, they must be handled with care to avoid losing or damaging the paper that contains the keys. Paper wallets are less accessible to beginners than other wallet kinds since they require a certain amount of technical ability to create and use. A drawback to paper wallets is that they are highly vulnerable to damage. Fire, water, ripping, and deterioration over time might result in a loss of

money. Furthermore, a paper wallet must be recovered, recovered, or recovered with sufficient backups to ensure the stored cryptocurrency can be recovered, resulting in irreversible loss.

Cryptocurrency Incidents

Cryptocurrency's promises of decentralization and security have made it a significant participant in the global financial scene. However, recent occurrences have highlighted the difficulties inherent in digital forms of currency. These incidents, which range from software flaws to key thefts, have brought attention to the necessity of strong security protocols and raised concerns about cryptocurrencies' longevity as a trusted transaction method.

One of the most important concerns confronting the cryptocurrency ecosystem is the emergence of software vulnerabilities. Despite developers' attempts to build safe systems, malicious threats can still exploit software weaknesses. In 2023, numerous attacks took place where software vulnerabilities were exploited in a popular decentralized finance (DeFi) system, resulting in the theft of millions of dollars of cryptocurrencies.

In September 2023, the DeFi space experienced its largest hack of the year, targeting the Mixin Network, leading to an estimated loss of $200 million, as reported by [9]. Mixin Network, a blockchain network that enables peer-to-peer transactions and DeFi services, was the target of a sophisticated attack that exploited a vulnerability in its cloud service provider database. As seen in [6], the exploit enabled hackers to steal significant funds from various decentralized finance protocols and user wallets linked to the Mixin Network. This incident highlighted DeFi platforms' ongoing difficulty in protecting their protocols from increasingly sophisticated cyber attacks.

In January 2022, the major cryptocurrency exchange Crypto.com suffered a cyber attack, resulting in unauthorized Bitcoin and Ether withdrawals totaling around $35 million, according to [7]. Crypto.com is a popular cryptocurrency exchange and financial services platform that provides various digital assets. Customers can buy, sell, trade, and store a wide range of cryptocurrencies on it, including Ethereum, Bitcoin, and many more. The attack compromised user accounts, illustrating centralized exchanges' vulnerability to advanced cyber threats. The method of the attack is unknown, with Crypto.com releasing insufficient statements that just a tiny portion of their entire user base was affected. Even though the technique is unknown, it is apparent that there was a vulnerability in Crypto.com security that allowed the attacker to bypass the two-factor authentication.

In May 2021, the Colonial Pipeline, which controls the most significant fuel pipeline in the United States, was hit by a ransomware attack. The cybercriminal group DarkSide was behind the assault, which exploited vulnerabilities in Colonial Pipeline's systems, prompting a halt in operations. The attack interrupted fuel supply along the East Coast, causing panic purchasing and fuel shortages in many states. Colonial Pipeline eventually paid the hackers a ransom of roughly $5 million in Bitcoin to restore control of its systems and restart operations. Following the attack, the U.S. Department of Justice seized a significant portion of the ransom paid to the attackers. According to estimates found on [8], around 63.7 bitcoins out of the 75

bitcoins given to the DarkSide hackers, worth around $2.3 million at the time, were collected. The incident also sparked conversations on how cryptocurrencies help to facilitate cybercrime and the need for more laws and oversight to deal with these issues.

Cryptographic Techniques

Cryptocurrencies such as Bitcoin, Ethereum, and Dogecoin are based on cryptographic algorithms that provide security, anonymity, and integrity in their decentralized networks. These strategies are critical to the functioning and reliability of these digital currencies. Cryptographic techniques these famous cryptocurrencies use include hash functions, digital signatures, and public-private key pairs.

Hash functions are fundamental to cryptocurrencies. As explained in [10], a hash function is a mathematical technique that accepts an input or message and returns a fixed-length string of characters, usually a cryptographic hash value. This hash result is unique to the input data and seems random, making it virtually hard to derive the actual input from the hash. In the context of cryptocurrencies, hash functions are used to generate the cryptographic hash of each block in the blockchain. Blockchains, or distributed ledgers, are used by Bitcoin, Ethereum, and Dogecoin to record all network transactions. Every block has a list of transactions referencing the preceding block's hash, which essentially links the blocks together. Cryptocurrency ensures the blockchain's integrity by hashing the data in each block. Any change to the data within a block would produce a new hash value, making hacking with the blockchain nearly difficult without notice.

Digital signatures are another important cryptographic mechanism used by cryptocurrencies. A digital signature is a mathematical system that confirms the authenticity of digital messages or files. [11] says it ensures that the communication was generated by who it is from and was not altered during transmission. Digital signatures are essential in validating digital asset ownership in cryptocurrency transactions. Users use their private key to sign the transaction data when they start a digital transaction. This signature is then added to the transaction and shared across the network. Other network participants can use the sender's public key to validate the digital signature and confirm that the owner approved the transaction of the private key associated with the public key. This approach protects the integrity and validity of cryptocurrency transactions without needing a central authority.

Public-private key pairs are the foundation of cryptographic security in cryptocurrencies. Two mathematically related keys, the public and private keys, make up a public-private key pair. According to [12], The public key is freely shared with others and may be used to encrypt communications or validate digital signatures. The private key is not being shared and is used to decrypt messages or create digital signatures. In cryptocurrencies, users create a public-private key pair to communicate with the network. Their public key acts as their network address or identification, while their private key allows them to access their digital assets and sign transactions. To ensure that only the correct recipient can decrypt and access the money using their private key, the user sending cryptocurrency to another encrypts the transaction data using the recipient's public key. In addition, users utilize their private keys to sign transactions, providing cryptographic proof of ownership and authority.

Noah Salafranca
CS 463
Project Paper
4/4/24

The Popularity of Cryptocurrencies

The principle of solving puzzles through cryptography is essential to cryptocurrency security. The mining process involves solving challenging mathematical puzzles to validate and add new transactions to the blockchain. These puzzles serve as a network security mechanism, accepting only legal transactions and preventing double-spending. Miners contribute to the blockchain's integrity and immutability by solving cryptographic puzzles, reinforcing its security characteristics.

Cryptocurrencies are popular for various reasons, including their potential for financial innovation, accessibility, and distrust in traditional banking systems. As the first cryptocurrency, Bitcoin pioneered the notion of decentralized digital money, disrupting established financial institutions and providing an alternative source of wealth. Ethereum extended this by offering smart contracts, which allow developers to construct dApps and new use cases for blockchain technology. Dogecoin, which began as a fun meme currency, grew in popularity due to its community-driven approach and minimal transaction costs, attracting a larger audience beyond professional investors. Alongside the potential for substantial financial returns, cryptocurrencies have created a culture of innovation, transparency, and financial freedom. The popularity of cryptocurrencies stems from their ability to bypass intermediaries such as banks, allowing peer-to-peer transactions and financial ownership. This culture resonates with younger generations who are dissatisfied with traditional financial institutions and ready to embrace new forms of money and investment. Furthermore, the development of DeFi platforms has increased access to financial services, allowing people worldwide to lend, borrow, and engage in cryptocurrencies. The cultural shift towards cryptocurrency reflects a broader societal trend towards digitalization and decentralization of finance, supported by confidence in blockchain technology's potential.

Cryptocurrencies have various benefits over physical or digital currency like credit and debit cards. For starters, they eliminate the need for intermediaries such as banks or payment processors, allowing peer-to-peer transactions to occur without a centralized authority's intervention. This decentralization promotes financial inclusion and gives individuals complete control over their money. Additionally, cryptocurrencies are nationless and function worldwide, allowing more transactions. Furthermore, the underlying blockchain technology is transparent, immutable, and secure, assuring transaction integrity.

Conclusion

Cryptocurrencies represent a paradigm shift in financial technology, offering innovative solutions powered by blockchain and cryptographic techniques. Bitcoin, Ethereum, and Dogecoin exemplify digital currencies' diverse applications and potential, offering unique contributions to the evolving cryptocurrency ecosystem. Cryptocurrencies have several benefits over traditional currencies, including security, ease of use, and financial innovation, but they also carry certain concerns, such as regulatory uncertainty and price fluctuation. As cryptographic techniques continue to advance and adapt to emerging challenges, cryptocurrencies will reshape the landscape of finance and cryptography.

Noah Salafranca
CS 463
Project Paper
4/4/24

References

E-book:

[1] A. Santos-Alborna, *Understanding cryptocurrencies: Bitcoin, Ethereum, and Altcoins as an Asset Class*. Business Expert Press, 2021.

[2] M. G. Solomon, *Ethereum for dummies*. John Wiley & Sons, 2019.

Journal Article:

[3] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, Mar. 2017, doi: 10.1007/s12599-017-0467-3.

[4] M. Brichta, "Fanning Money: The Cultural Economy and Participatory Politics of Dogecoin," *International Journal of Communication*, vol. 17, no. 1932–8036, p. 6032, Jan. 2023.

[5] S. Houy, P. C. Schmid, and A. Bartel, "Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review," *ACM Computing Surveys*, vol. 56, no. 1, pp. 1–31, Aug. 2023, doi: 10.1145/3596906.

Blog:

[6] R. Behnke, "Year In Review: The biggest DEFI hacks of 2023," Jan. 08, 2024. https://www.halborn.com/blog/post/year-in-review-the-biggest-defi-hacks-of-2023

[7] R. Behnke, "Explained: The Crypto.com hack (January 2022)," Jan. 24, 2022. https://www.halborn.com/blog/post/explained-the-crypto-com-hack-january-2022

[8] C. Team, "Chainalysis In Action: How FBI Investigators Traced DarkSide's Funds Following the Colonial Pipeline Ransomware Attack," *Chainalysis*, Sep. 20, 2023. https://www.chainalysis.com/blog/darkside-colonial-pipeline-ransomware-seizure-case-study/

Article:

[9] S. Reynolds, "Mixin Network Losses Nearly $200M in Hack," *CoinDesk*, Sep. 25, 2023. [Online]. Available: https://www.coindesk.com/tech/2023/09/25/mixin-network-losses-nearly-200m-in-hack/

[10] I. Team, "Cryptographic Hash Functions: definition and Examples," *Investopedia*, Aug. 19, 2023. https://www.investopedia.com/news/cryptographic-hash-functions/#:~:text=A%20cryptographic%20hash%20function%20is,hash%20functions%20with%20security%20properties.

[11] "Understanding Digital Signatures | CISA," *Cybersecurity and Infrastructure Security Agency CISA*, Feb. 01, 2021. https://www.cisa.gov/news-events/news/understanding-digital-signatures

[12] PreVeil, "Public and private encryption keys | PreVeil," *PreVeil*, Mar. 14, 2024. https://www.preveil.com/blog/public-and-private-key/

[13] Ledger, "What are Ethereum Layer 2 blockchains and how do they work? | Ledger," *Ledger*, Jan. 25, 2024. https://www.ledger.com/academy/topics/blockchain/what-are-ethereum-layer-2-blockchains-and-how-do-they-work