KENNESAW STATE UNIVERSITY

COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

CS 4850-01 | FALL 2023 | SP-24 RED | SECURITY IN BLOCKCHAIN

BLOCKCHAIN OVERVIEW DOCUMENT

INSTRUCTOR: SHARON PERRY

BLOCKCHAIN

Introduction

Blockchain is a series of sequential lists, also known as blocks, that are linked together in a decentralized distributed database. The reason blockchain would be used is it requires verification from multiple computers for a new block to be introduced. This allows for the system to be more secure than a system that is just creating a single file on a single system. This makes it impossible for an attacker to get in and change information in the blockchain. That is one of the big reasons it is used in crypto and crypto wallets because it keeps the information safe and allows people peace of mind that their money is going to be safe. Through this blockchain overview one will see the types of blockchain, the various parts included in the structure of most blockchains as well as the mining process for bitcoin in blockchain.

Benefits of Blockchain

Blockchain is a game-changing technology that has swept through the digital landscape, providing unique advantages that permeate multiple sectors. One of its most notable features is its capacity to embody transparency, decentralization, and security in a single solution that can be applied in a wide range of settings. Nakamoto (2008) outlined several key benefits of blockchain in the original Bitcoin whitepaper, highlighting immutability, trust, and heightened security. By chaining blocks, the technology achieves immutability, preventing changes to previous transaction records. The blockchain network's ability to serve as a foundation for diverse use cases is due to the trust fostered by its combination of immutability and security, which are products of cryptographic algorithms that prevent unauthorized access to data.

Types of Blockchain

There are 4 types of blockchain Public blockchain, Private blockchain, Hybrid blockchain, and Consortium blockchain:

- Public blockchain is where cryptocurrency was born. The decentralized nature promotes security and transparency. Also, the chain being public creates trust amongst its users as many people can see the ledger and notice if something has changed or is wrong in any way. However, it is not as secure as a private blockchain as will be discussed later because it is susceptible to 51% attacks which is when an attacker gets control of over 50 percent of the blockchain allowing for certain blocks to be negated. This happens when the attacker publishes a longer chain as blockchain always goes with the longest chain. The most common uses for public blockchain are cryptocurrency and document validation.

- Private blockchain is more secure than public blockchain as any normal attacker cannot get in and perform a 51% attack, they must access it. Private blockchains include access control, which is who has access to the blockchain, and better performance as there are less people contributing to the chain. They are also on a smaller scale than a public blockchain and are usually on one network within a company. This is also known as a permissioned blockchain. This is not a true blockchain in a sense as there is a sort of centralized nature to it being on a single network.
- Hybrid blockchain is the next type of blockchain combining both previous types of private and public blockchains. This allows for two systems to be set up in tandem, part of the chain that the company allows the public to view and part that is only viewable to a select group of people. Typically, the transactions made within a hybrid blockchain are not public but can be verified using smart contracts. This way confidential information is kept within the system and private but can still be verified to be accurate. Advantages to Hybrid include does not allow for a 51% attack to occur and has better scalability than a public blockchain while still retaining the security that private blockchains offer. Hybrid blockchains are used in things such as medical records and real estate.
- Consortium blockchains are like hybrid blockchains in that they contain both private and public features, but they are more decentralized as they are used between multiple organizations. Consortium block chains contain validator nodes which can validate, receive, and transmit information, then member nodes which can only receive and transmit information. Consortium blockchains are more secure than public blockchains as they also offer access control like private and public blockchains. With security comes less transparency consortium blockchain is used in payments and banking.

Blockchain Structure

Blockchain structure contains various parts including block height, block size, block reward, transaction counter, header, and the body. The block height determines the block number in the chain, so this is an incrementing counter with each block by one whole number. Next is a 32-bit field containing the size of the block in bytes. Followed by block reward which tells the amount awarded to a miner for adding the block to a chain. Then the transaction counter containing the number of transactions within a block. The next major section is the block header which contains several sections.

The block header contains time, version, previous block hash, bits, nonce, and the Merkle root. First the header contains the time field indicating the time of when the block was mined. This information is used in transaction data as well. The version in the header is a 4-byte field representing the version number of the protocol used to do the mining. The next section is a 32-bit field containing a SHA-256 hash of the previous blocks address helping to connect the current block to the previous block. Then there is a bit field which tells the level of difficulty based on Proof of Work in blockchain. The nonce is a randomly generated number used in cryptography to prevent replay attacks and add uniqueness to each block. The final item in the header is the Merkle root which is a structure used to combine all the transactions in a hash. Finally, there is the body of the block which contains all transaction in total each block contains an average of 2000 transactions.

SHA-256 in Blockchain

SHA-256 is a hashing algorithm that is used in blockchain. This is used in hashing the previous address of each block. This hashing algorithm also enables Proof of Work consensus algorithm in blockchain. This hashing algorithm is also part of the verification methods in blockchain. The hash is formed by using a randomly generated number, the nonce added to the data from the previous block and hashed to create the previous blocks hash. The reason SHA-256 is the most common hashing algorithm is its difficulty to de hash and crack. However, the weak number added creates a sort of exploitation that attackers can take advantage of. This number is generated every time there is a hash, however sometimes a number could be generated 2 times, or it could be a weak number like one that is generated and added.

ECDSA (Elliptic Curve Digital Signature Algorithm) Verification with Random Numbers

The elliptical curve digital signature algorithm is used in blockchain for verification of digital signatures or private keys as they are called in the tech world. The random numbers are used within this algorithm along with SHA-256 in verification of the private keys. Within this random number generation is where weak randomness is going to be exploited. This is the most common algorithm for verification in the blockchain and bitcoin space.

Why Does Blockchain Typically Use P2P Networks?

Intrinsically to blockchain, P2P networks are employed due to the autonomous and decentralized characteristics of this technology. Communications and data sharing are achieved through direct interaction between nodes without the involvement of a central authority, which is an integral feature of blockchain. This eliminates the possibility of any entity monopolizing the network and boosts security measures and confidence in the technology. Additionally, P2P networks are robust under challenging circumstances, as there is no focal weakness; if an individual node stops functioning, the overall network can continue to operate as normal.

How P2P Networks Work

In a dispersed system, individual nodes within a peer-to-peer network interact with one another in a mesh-like pattern, and all nodes are considered equal. Direct conversation occurs between nodes as they send data or transactions, moving from node to node and arriving at their end point. By allowing for the distribution of the blockchain ledger across several nodes, P2P networks play a crucial role in the functioning of blockchain technology. This communication guarantees that transactions are verified and documented by various nodes, thereby increasing security, and decreasing the likelihood of fraud. Such a system is specifically designed to prevent a single point of failure from compromising the entire system.

Mining and its Purpose

Using computational power, miners compete to solve complex mathematical puzzles to add new blocks to the blockchain, a process that plays a vital role in securing the network. When a miner successfully solves the puzzle, they are rewarded with cryptocurrency and the right to add the new block. Through this process, mining serves two essential functions by validating and confirming transactions to ensure their legitimacy and preventing fraudulent activities like double spending to maintain the integrity and security of the blockchain.

Mining Process

In the mining process, miners race to decode a puzzle that demands computational power use. The puzzle itself derives its structure from a combination of the pending transactions present within the network and a hash from a preceding block. It is only through the selection of an appropriately random number, known as a nonce, that a miner could unravel the puzzle. This endeavor requires persistent attempts to figure out the correct nonce, which, once added to the present data, generates a hash that consistently satisfies specific requirements- often needs to start with a certain number of leading zeros. Upon the successful discovery of the nonce, a miner delivers the solution to the network for broadcast. Every 10 minutes, after other nodes verify the solution, a new block is added to the blockchain by the miner if it is deemed correct in the Bitcoin network. This recurring process is elaborated upon by (Antonopoulos & Mougayar 2019).

Conclusion

Blockchain technology offers a variety of benefits, including immutability, security, and trust. Diverse types of blockchain networks, from public to private to hybrid to consortium, cover a variety of use cases. Next there was a discussion on the overall structure of blockchain. Following up with the used part of blockchain. SHA- 256 is the most common hash algorithm in the blockchain community. ECDSA is the most common verification method in blockchain, but it creates an exploit that attackers can use. Peer-to-peer networks are the foundation for maintaining the decentralization and security of blockchain technology. Mining is a key process in a blockchain network, serving the dual purpose of verifying transactions and ensuring the integrity of the blockchain.

CRYPTOCURRENCY FUNDAMENTALS

Introduction

In the previous section, we explored the fundamental principles of blockchain technology and its underlying mechanisms. Building upon this foundational knowledge, Section 2 delves into the cryptocurrencies ecosystem, where we will unravel the intricate workings of smart contracts, the Ethereum Virtual Machine (EVM), and the critical concept of gas fees.

What is Bitcoin & Ethereum?

Bitcoin (abbreviation: BTC) is the first and most widely known cryptocurrency, a digital currency that operates without any central authority or intermediary. Bitcoin transactions are secured by cryptography and can be sent and received by anyone who has a bitcoin address and a private key. Bitcoin addresses are alphanumeric strings that identify the owners of bitcoins, while private keys are secret codes that allow spending bitcoins from the corresponding addresses.

Ethereum is a decentralized global software platform that enables running decentralized applications. Ethereum's native cryptocurrency is called ether (abbreviation: ETH). Ether can be used to pay for transactions and computational services on the Ethereum network. Ether can also be traded for other currencies or assets or used as a fuel for dApps. Ethereum uses its own blockchain network, similar to Bitcoin's, but with some key differences.

What is Smart Contract?

What makes Ethereum differ from Bitcoin is the ability to create smart contracts. A smart contract is essentially a set of computerized instructions that exist on a blockchain. These instructions outline the terms for how the parties involved will interact. The contract automatically executes once the specified conditions are fulfilled. This code not only simplifies but also authenticates and carries out the terms of an agreement or transaction. It represents the most basic form of decentralized automation.

User accounts are capable of engaging with a smart contract by initiating transactions that carry out a function specified within the smart contract. Similar to conventional contracts, smart contracts have the ability to establish and autonomously enforce rules through their code. It's important to note that smart contracts are inherently immune to deletion by default, and any actions involving them are irreversible.

Automatic Execution

The code in smart contracts cannot be invoked automatically from within the blockchain, it has to be called externally. Consequently, the development of a script or service is required to facilitate interaction with the smart contract.

For instance, consider a scenario where two parties engage in a bet pertaining to the following day's weather. The smart contract retrieves the relevant weather data on the following day and automatically pays the winner. However, complications may arise if the losing party's wallet lacks the necessary funds. In this case, both parties pre-commit their bets to the contract, which securely holds these assets until a clear winner has been decided. Subsequently, the winning party can initiate a withdrawal of their winnings from the contract.

The execution for a smart contract transaction occurs when the mining node includes the transaction in a block it generates. The transaction and smart contract code is re-run by every validating node upon receipt of the block. While Ethereum smart contracts offer automatic execution, they require external triggers and hold funds in escrow until conditions are met. This ensures fairness and trustless operation.

EVM

Smart contracts are run on the Ethereum Virtual Machine (EVM), a key component of the Ethereum network, as it enables the execution of smart contracts and the update of the blockchain state. The EVM is a Turing-complete virtual machine that can run any code that is written in a specific language called Solidity. Solidity is a high-level programming language that is designed for creating smart contracts, which are self-executing agreements that can encode any kind of logic and rules. The EVM is isolated and sandboxed from the rest of the network, meaning that it does not have access to the file system, network, or other external resources. It only operates on the data that is stored on the blockchain, such as accounts, balances, and contract code.

The EVM works by taking the bytecode of a smart contract, which is the compiled version of the Solidity code, and executing it step by step according to a set of instructions called opcodes. Each opcode performs a specific operation, such as arithmetic, logic, control flow, or data manipulation. The EVM has a limited amount of memory and storage, as well as a stack and a call stack for managing function calls and returns.

What is a Gas Fee?

In the Ethereum blockchain, the term “gas” is used to denote the computational effort required to execute transactions or smart contracts. Gas fees are an integral part of Ethereum’s design, serving multiple functions in ensuring the efficient operation and robust security of the network. The cost associated with this computational effort is known as the “gas fee” and is paid in Ethereum’s native cryptocurrency, Ether (ETH), specifically in a denomination known as Gwei. One Gwei is equivalent to one-billionth of an ETH (0.000000001 ETH or 10^{-9} ETH).

The gas fee for a transaction is composed of two parts: the base fee and the priority fee. The base fee, determined by the Ethereum protocol (also known as consensus mechanisms), is the minimum amount required for a transaction to be deemed valid. The priority fee, also known as a “tip,” is an additional amount that users can choose to pay to incentivize validators (also known as miners) to prioritize their transaction for inclusion in the next block. This incentivizes them to perform honest work, thereby maintaining the integrity and security of the blockchain.

To illustrate, consider a scenario where a person named Alice wishes to transfer 1 ETH to another person named Bob. A standard ETH transfer requires 21,000 units of gas and let’s assume that the base fee at this time is 10 Gwei. If Jordan decides to add a tip of 2 Gwei, the total gas fee for this transaction would be calculated as units of gas used multiply with base fee and priority fee, where the base fee is set by the protocol and the priority fee is determined by the user.

Conclusion

Cryptocurrencies have revolutionized the fields of finance, technology, and society by providing new ways of exchanging value. They have also inspired countless other projects and initiatives that aim to leverage the power of blockchain for various purposes. However, they are not without challenges and limitations, such as security, and vulnerabilities. As they continue to evolve and improve, they will likely face new opportunities and threats in the future. In the next section, we will explore security and vulnerabilities of blockchain.

SECURITY

Blockchain technology has transformed various industries, promising secure and decentralized transactions. One of the key reasons behind the robustness of blockchain systems is their focus on cryptography principles, consensus protocols, and security practices. This paper explores these elements, shedding light on the fundamental security aspects of blockchain technology.

Cryptography Principles in Blockchain

Blockchain relies heavily on cryptographic techniques to ensure data integrity, confidentiality, and authenticity. Public-key cryptography, where each participant has a pair of public and private keys, is commonly used. Hash functions, like SHA-256, create unique identifiers for blocks and transactions, ensuring data integrity. Digital signatures authenticate transactions, verifying the sender's identity without revealing their private key.

Consensus protocols are the heart of blockchain security, ensuring all participants agree on the state of the blockchain. Some prominent ones include:

Proof of Work (PoW): PoW requires miners to solve complex mathematical puzzles, making the creation of new blocks resource intensive. This computational effort validates transactions and secures the network against attacks.

- Proof of Stake (PoS): PoS assigns the right to validate transactions and create new blocks based on the participants' stake in the network (number of coins). It is energy-efficient compared to PoW.
- Proof of Authority (PoA): PoA relies on trusted validators, making it highly secure for private blockchains. Validators are reputable entities authenticated by the network.
- Proof of Burn (PoBr): PoBr involves sending coins to a verifiably unspendable address, proving commitment to the network. The sacrifice of coins demonstrates the user's intention to maintain network integrity.
- Proof of Elapsed Time (PoET): PoET relies on a trusted execution environment where participants wait for a random time. The first to finish gets the right to create a block. This protocol ensures fairness without extensive energy use.

Best Security Practices

Ensuring blockchain security involves implementing several best practices:

Regular Code Audits: Periodic audits of smart contracts and blockchain codebases identify vulnerabilities, ensuring robustness against attacks.

Encrypted Communication: Secure channels using encryption protocols like SSL/TLS protect data transmission between nodes, preventing eavesdropping.

Permissioned Blockchains: Limiting access to known participants enhances security. Permissioned blockchains like Hyperledger Fabric restrict network entry to approved entities.

Immutable Data: Once data is added to a blockchain, it becomes immutable. Utilizing this feature for critical data ensures historical records remain unaltered.

Multi-Signature Wallets: Multi-signature wallets require multiple private keys to authorize a transaction, enhancing security against unauthorized access.

VULNERABILITY

Why is Crypto Used for Criminal Activity?

Banks are highly regulated and require identification documents and legal statements. Criminals use cryptocurrency as a tool to conduct illicit activities because they are able to exploit its decentralized nature and pseudonymity. Cryptocurrency enables many illicit activities, such as fraud, money laundering, trafficking, dark marketplace trading, cybercrime, and terror funding. While transaction data is public, the transaction maker is anonymous; another reason criminals use cryptocurrencies is because third parties are not necessary. An additional bonus is that cryptocurrencies require no physical space; they are easy to transfer locally and internationally. Furthermore, trading is easy, it only requires an internet connection and a wallet application; cryptocurrencies are always available and transferred quickly- within minutes (Sadon).

According to the 2023 Crypto Crime Report, illicit transactions reached a record high of $20.1 billion in 2022, increasing the amount of digital assets laundered by 68% from the previous year. Chainalysis categorizes crime by CSAM/human trafficking, ransomware, stolen funds, sanctions, terrorism financing, scam, cybercriminal administrator, fraud shop, and darknet market. Transaction volumes decreased across all but one of the conventional categories of cryptocurrency-related crime. Stolen funds grew 7% year-over-year from 2019 to 2022 (Chainalysis). As of June 2023, crypto-related crime has fallen 65% from the same period last year and inflows to illicit addresses are down across almost all categories. Ransomware, however, is rising, having generated $175.8 million more than last year (Void).

How is Blockchain Technology Attacked?

Blockchain technology has multiple exposure points that make it susceptible to attacks. One weak point is the lack of regulatory intervention, making it so organizations are able to operate in gray areas. A second weak point is the users; fraudsters utilize social engineering to gain access to user accounts and escalate privileges to steal tokens or data. Users, which can include customers, employees, and shareholders, without proper educational training can become victims of phishing attacks and the like. Additionally, ransomware attacks are more likely with the rise of remote work and inadequate cyber awareness. These attacks hinder data availability and cause businesses to suffer long-drawn downtimes. (Chammah).

Code Exploitation and Software Vulnerabilities

A significant benefit of using a blockchain is that it is immutable and allows people who do not necessarily trust each other to share valuable data with one another in a secure way. The data is structured in such a way that it is nearly impossible to tamper with (Orcutt). Tampering is the unauthorized act of modifying a system, parts of a system, a system's behavior, or data (CRSC). However, blockchain systems are still subject to vulnerabilities. When an attacker acting as a blockchain user finds a weak spot in a blockchain's software, they can take advantage of the vulnerability; the act of exploiting weaknesses in software is known as code exploitation. A software vulnerability is a security issue, glitch, or weakness that is found in software code that can be exploited by an attacker (CSRC). If user restrictions are not properly enforced, software vulnerabilities can arise. Cryptographic failures- caused by insufficient protection of sensitive data- and insecure design- caused by lack of threat modeling, secure design principles, or reference architecture- can also cause software vulnerabilities. Another common software vulnerability is outdated components- components consist of frameworks, libraries, and other software modules. A vulnerable component can be exploited, leading to major data loss or server takeover. Software and data integrity failures allow bad agents to perform injection, replay, and privilege escalation attacks, while inadequate logging and monitoring processes can result in data tampering, extraction, or destruction (Foster).

Stolen Keys

Every blockchain user has a unique identifier to enter a blockchain network. These "ID badges" are called private keys; they are used to authorize transactions and to prove ownership of an asset. Private keys can be and are stolen (Frankenfield). Internet connection is the largest threat to private keys. Anything connected to the internet is vulnerable to cyber-attacks, and software wallets store private keys on their host devices. Cyber criminals can also steal keys by getting a user to click on a malicious link or sign a malicious transaction. They can also hack central entities that a user entrusted their private keys to. Furthermore, they can place contract bugs on blockchain platforms; a bug in a smart contact provides them with the means to steal cyber funds (Moreland).

Phishing Attacks, Routing Attacks, Sybil Attacks

The four primary blockchain vulnerabilities are phishing attacks, routing attacks, Sybil attacks, and 51% attacks. Phishing attacks entail threat actors targeting wallet key owners by acting as authoritative sources and requesting sensitive information such as login credentials. Attackers often send mass emails or messages from what appears to be a legitimate source (for example, a cryptocurrency exchange). Once the victim has been tricked, the attacker uses their information to steal their crypto funds. These attacks exploit human vulnerabilities more so than blockchain technology itself. Routing attacks allow hackers to extract confidential data or currencies behind the scenes. Blockchain systems rely on large data transfers in real-time. Hackers take advantage of that by intercepting data as it is transferring to internet service providers ("What Is Blockchain"). It is nearly impossible for other nodes to detect tampering because the attacker partitions the network into sections that cannot communicate with each other (BlockchainSentry). In other words, routing attacks involve an attacker partitioning a network into two or more distinct components, blocking the communication between nodes in a chain and nodes outside of it, allowing them to create parallel blockchains and to discard all blocks that were mined within the smaller chain (S). The criminals are able to lurk on weak networks while a permissioned user is on, allowing them to monitor and compromise the blockchain without the user's knowledge (Stouffer). Sybil attacks, seen in peer-to-peer networks, involve hackers creating and using multiple false network identities to flood a network, causing it to crash. Attackers can gain disproportionate control over a network's honest nodes if they are able to create enough fake identities, as that would enable them to refuse to transmit or receive blocks, thus blocking other users from a network. The attack is named after the book Sybil, about a woman with multiple personality disorder. 51% attacks are a type of Sybil attack ("Sybil Attack"). This attack was detailed previously and will be expanded on more throughout the project.

Conclusion

This paper detailed blockchain, cryptocurrency fundamentals, blockchain security, and blockchain vulnerabilities. Next, the *Weak Randomness* case study will be explored, followed by the *Consensus Mechanism Manipulation: 51% Attack* case study, the *Transaction Order Dependence* case study, and the *Underlying Cryptosystem Vulnerabilities* case study. The last case study will cover *Improper Blockchain Magic Validation.* Finally, this paper will include a report on the blockchain system simulation.

REFERENCES

Blockchain

GAREK MILENDER AND JOVANY HERNANDEZ

Afreen, Sana. “Why Is Blockchain Important and Why Does It Matters?” *Simplilearn.Com*, Simplilearn, 21 July 2023, www.simplilearn.com/tutorials/blockchain-tutorial/why-is-blockchain-important#:~:text=Blockchain%20facilitates%20the%20verification%20and,contract%20administration%20and%20product%20auditing.

Antonopoulos, A. M., & Mougayar, W. (2019). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media.

Campbell, Christine. “What Are the 4 Different Types of Blockchain Technology?: TechTarget.” *CIO*, TechTarget, 25 May 2023, www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology#:~:text=There%20are%20four%20main%20types,benefits%2C%20drawbacks%20and%20ideal%20uses.

Discover Colleges, Courses & Exams for Higher Education in India, www.shiksha.com/online-courses/articles/structure-of-a-block-in-blockchain/. Accessed 11 Oct. 2023.

Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.

Nakamoto, Satoshi. “A Peer-to-Peer Electronic Cash System.” *Bitcoin*, bitcoin.org/en/bitcoin-paper. Accessed 19 Oct. 2023.

What Is SHA-256? How It Works in Blockchain & Cryptography - Techopedia, www.techopedia.com/definition/sha-256. Accessed 16 Oct. 2023.

Cryptocurrency Fundamentals

HUY LE

“What Is Ethereum?” *Ethereum.Org*, ethereum.org/en/what-is-ethereum/. Accessed 10 Oct. 2023.

Smith, Corwin. “Introduction to smart contracts” Ethereum.Org, 18 July 2023, ethereum.org/en/developers/docs/smart-contracts/

Smith, Corwin. “Gas and Fees.” Ethereum.Org, 18 July 2023, ethereum.org/en/developers/docs/gas/.

Security

JALON BAILEY

Bitpanda. “What Are Multi-Signature Wallets and How Do They Work?” - Bitpanda Academy, www.bitpanda.com/academy/en/lessons/what-are-multi-signature-wallets-and-how-do-they-work/. Accessed 9 Nov. 2023

Guo, Huaqun, and Xingjie Yu. “A Survey on Blockchain Technology and Its Security.” Blockchain: Research and Applications, Elsevier, 24 Feb. 2022, www.sciencedirect.com/science/article/pii/S2096720922000070.

Zida, Chek. “Blockchain Consensus Mechanisms: Exploring the Differences between Proof of Work and Proof of Stake.” Medium, Coinmonks, 7 June 2023, medium.com/coinmonks/consensus-mechanisms-exploring-the-differences-between-proof-of-work-and-proof-of-stake-d3042841f9b3. Accessed 9 Nov. 2023

Vulnerability

NIKKI DULANEY

BlockChainSentry. “Security of Blockchain Network Layers.” *BlockChainSentry*, 11 Jan. 2023, blockchainsentry.com/blog/security-of-blockchain-network-layers/.

Chainalysis. “2023 Crypto Crime: Illicit Crypto Volumes Reach All-Time Highs.” *Chainalysis*, 19 Sept. 2023, www.chainalysis.com/blog/2023-crypto-crime-report-introduction/.

Chammah, Ralph. “How Fraudsters Attack Blockchain Technology and How It Can Be Prevented.” *Financial IT*, financialit.net/blog/blockchain/how-fraudsters-attack-blockchain-technology-and-how-it-can-be-prevented. Accessed 8 Nov. 2023.

CRSC. “Tampering - Glossary: CSRC.” *CSRC Content Editor*, csrc.nist.gov/glossary/term/tampering. Accessed 8 Nov. 2023.

CSRC. “Software Vulnerability - Glossary: CSRC.” *CSRC Content Editor*, csrc.nist.gov/glossary/term/software_vulnerability. Accessed 8 Nov. 2023.

Foster, Stuart. “Vulnerabilities Definition: Top 10 Software Vulnerabilities.” *Perforce Software*, www.perforce.com/blog/kw/common-software-vulnerabilities. Accessed 8 Nov. 2023.

Frankenfield, Jake. “Private Key: What It Is, How It Works, Best Ways to Store.” *Investopedia*, Investopedia, www.investopedia.com/terms/p/private-key.asp. Accessed 8 Nov. 2023.

Moreland, Kirsty. “How Crypto Gets Stolen - and How to Avoid It.” *Ledger*, 4 Sept. 2023, www.ledger.com/academy/how-crypto-gets-stolen-and-how-to-avoid-it.

Orcutt, Mike. “How Secure Is Blockchain Really?” – *MIT Technology Review*, MIT Technology Review, 2 Apr. 2020, www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/amp/.

S., Aaron. “What Is Routing Attack? Definition & Meaning: Crypto Wiki.” *BitDegree.Org Learning Hub*, BitDegree.org Learning Hub, 12 Sept. 2023, www.bitdegree.org/crypto/learn/crypto-terms/what-is-routing-attack.

Sadon, Tom. “5 Reasons Why Criminals & Terrorists Turn to Cryptocurrencies.” *Cognyte*, 30 Mar. 2022, www.cognyte.com/blog/5-reasons-why-criminals-are-turning-to-cryptocurrencies/.

Stouffer, Clare. “What Is Blockchain Security? An Overview: Norton.” *United States*, 24 June 2022, us.norton.com/blog/privacy/blockchain-security#:~:text=Code%20exploitation%20is%20when%20a,that%20weakness%20with%20malicious%20intent.

“Sybil Attack.” *GeeksForGeeks*, www.geeksforgeeks.org/sybil-attack/amp/. Accessed 8 Nov. 2023.

Void, Fredrik. “Chainalysis Report: Significant Decline Seen in Crypto Scams in 2023.” *Cryptonews*, 13 July 2023, cryptonews.com/news/chainalysis-report-significant-decline-seen-crypto-scams-2023.htm#:~:text=So%20far%20in%202023%2C%20crypto-related%20crime%2C%20measured%20as,to%20so-called%20%E2%80%9Clegitimate%20services%E2%80%9D%20were%20down%20only%2028%25.

“What Is Blockchain Security?” *IBM*, www.ibm.com/topics/blockchain-security. Accessed 8 Nov. 2023.