Module 12 Mini Presentation – Communicating Research

Tamsyn Evezard
tae10@hood.edu

Fall 2024
CSIT 555 02
Monday, November 18, 2024

QUESTION 1A: BLOCKCHAIN TECHNOLOGY IN THE CONTEXT OF INFORMATION SECURITY SUMMARY

Blockchain technology is transforming data security through its unique structure and security properties, providing solutions for confidentiality, data integrity, and availability in digital transactions. Blockchains are used in a range of fields, for example, cryptocurrency, healthcare, and logistics, for secure data and transaction storage and management. It is essentially an advanced database mechanism in which data is stored in blocks that are linked together in a chain that cannot be broken, and it is almost impossible to alter data once it is recorded. The primary purpose of blockchain technology is to provide security through transparency and unchangeability for users to instill trust between parties using the network [11]. This is achieved through critical components of blockchains such as blocks, cryptographic hash functions, consensus mechanisms, smart contracts, and decentralized networks. These elements work together to ensure data integrity, prevent unauthorized tampering, and make blockchain technology suitable for real-world applications with a high security demand, like financial transactions, supply chain management, and healthcare data storage.

The core components of blockchain technology – blocks, cryptographic hash functions, consensus mechanisms, smart contracts, and decentralized networks – work in unison to ensure data security and integrity. Each transaction or group of transactions is recorded in a block, which is added to a chain chronologically. Cryptographic hash functions are algorithms that transform input data into a string of characters of fixed size called a digest or hash [5]. Hashes serves as a digital "fingerprint" or unique identifier for data within the blocks. Each block has a hash, a timestamp and reference to the previous block's hash [5]. This ensures that the links between the blocks cannot be broken, because attempting to alter data in one block would require changing the following blocks. This characteristic of unchangeability is called immutability, and makes it computationally infeasible for unauthorized altering of stored data within the chained structure without detection [4]. Hash functions are one-way, meaning they are non-reversible. It is computationally impossible to reverse-engineer the original input from a hashed value or "fingerprint." This ensures data integrity and confidentiality, securing the data in the blocks against unauthorized changes and protecting sensitive information, all essential for cryptocurrency transactions and data blocks [6]. Other essential cryptographic techniques used are public key cryptography and digital signatures. Public key cryptography involves a pair of public and private keys, (think of these as virtual keys used to encrypt and decrypt data). The users share their public keys and keep their own private key secret to secure transactions. Digital signatures allow users to authenticate transactions with their private keys. A challenge to cryptographic key usage is key management – users must protect their private keys from getting lost or stolen [11].

Consensus mechanisms allow peers (adjacent nodes) of a blockchain to reach an agreement about the current state of data in the distributed network [7], just as people reach a consensus or an agreement about decisions in everyday life to ensure that everyone is happy with a particular decision or idea before following through with it. The two most common consensus mechanisms are Proof of Work (PoW) and Proof of Stake (PoS). In PoW, participants called "miners" compete to be the first one to come up with a 64-digit hex number (hash). The winner earns a "block reward" (for example, a specific amount of cryptocurrency) and the right to form the new block and confirm the transactions. PoW is highly reliable and secure; however, it requires a lot of computational energy and resources, so scalability is a concern. In PoS systems, "validators" pledge a stake of digital currency to be randomly chosen to validate a block and get a reward – almost like in the lottery, where the higher one stakes, the higher their chances are to win. PoS is less resource-intensive than PoW; however, both ensure data accuracy and protect against attacks, fraud, and double-spending [7].

Smart contracts are contracts directly written into the code with terms of the agreement that automatically execute. Along with the distributed network or ledger technology, this reduces the necessity for an intermediary, making the process efficient and cost-effective while minimizing fraud risks. Smart contracts are fully transparent and immutable, meaning all parties can view the terms of agreement, eliminating possibilities of disputes between parties, and they cannot be altered once deployed. Some drawbacks of smart contracts include complexity – the writing and auditing of these can come with challenges. Testing, audits, and best practices should be used when developing smart contracts to mitigate vulnerabilities from coding errors [11].

Traditionally, transactions are supervised by a third party or "middleman" to verify information. However, this introduces a single point of potential vulnerability and failure. Blockchain technology eliminates this risk by removing the need for a middleman, using a decentralized network [2]. It is based on a distributed network of computers, or nodes, that maintain copies of the blockchain data. Blockchain's decentralized nature gives it a security advantage by reducing single points of failure and making unauthorized tampering difficult. Instead of relying on a single point in the network, the distributed network ensures every participant can access the same data. Any unauthorized attempt to alter the blockchain data would require the attacker to change data on more than 50% of the network, which is computationally infeasible.

Blockchain technology aligns with the principles of information security in the CIA triad: Confidentiality, Integrity, and Availability. Blockchain helps maintain data confidentiality through encryption methods. The immutability of blockchain technology is another characteristic that provides inherent security through ensuring data integrity. Once data is added to the blockchain, altering this data without consensus is extremely difficult. The cryptographic hash functions and chained structure explained earlier make the data highly resistant to modification and make it almost impossible for data to be altered by an unauthorized party without being detected. This is especially important in applications of blockchains with financial transactions, medical health records, and contract verification. Because of blockchain technology's distributed, decentralized nature, it is inherently resistant to attacks (specifically, denial-of-service attacks) and outages. Since there are copies of the ledger across many nodes in the network, if a few are compromised, the data is still accessible through the rest of the network. Transparency of blockchain networks contributes to the availability of the transactions and data

within the network (everyone with access to the system should be able to see all the data) and serves as the "bug spray" for fraud. Any attempt to alter data is easily detectable by other participants, ensuring that any malicious changes cannot be made in secret. This is a beneficial quality of blockchains where reliability and availability are demanded.

There are different types of blockchains, namely public, private, hybrid, and consortium, and the security measures vary across them because of their applications and focus. Public blockchains are decentralized and open, meaning that anyone and everyone can use them. In fact, the more people that use them, the better for their security. This openness is an advantage for transparency; however, it could introduce security risks like phishing and 51% attacks, which will be explained later. More downsides of public blockchains include that they are relatively slow and not very scalable. This type of blockchain is used for crypto, such as Bitcoin and Ethereum [8].

Private blockchains are restricted to specific users for privacy and greater control of the network. The restricted access of private blockchains is controlled by a single entity making them rely on centralized management. This contrasts with the decentralized nature of public blockchain. Although private blockchains are faster, have improved privacy, and offer greater control from being centralized, their centralized nature makes them less resistant to risks like internal fraud or manipulation. Thus, security measures must be implemented to prevent unauthorized access within the company. Private blockchains are more common with companies that require data privacy, such as finance (logistics, accounting, and payroll) organizations and other sensitive data recording applications [8].

Hybrid blockchains combine elements from public and private blockchains. They serve as an intermediate option that balances decentralization with control and offers selective data-sharing and privacy for different access levels. The versatility of these blockchains serves as an advantage for companies wanting the advantages of both options, for example, in healthcare, where some information needs to be made public for transparency while protecting patient information to maintain confidentiality. However, managing the combination of public and private aspects introduces complexity with access controls and is resource-intensive [8].

Consortium blockchains are a specific type of blockchain that has specific permissions in which multiple organizations share control of the network. They are useful in environments where collaboration between organizations is required, such as banking and logistics. While this type of blockchain provides a balance between the centralization and decentralization of public and private options, as well as shared cost and risk of manipulation, security depends on the cooperation of consortium members, and vulnerabilities can arise if they do not follow specified security protocols [8].

While blockchain has built-in security strengths, it is still susceptible to cyberattacks. Well-known attacks include phishing, routing, sybil, and 51% attacks [1]. Phishing attacks scam users to obtain their private credentials through a deceptive email, message, or website that seems authentic. To mitigate this risk, user education regarding secure credentials, key management, and two-factor authentication are crucial. Routing attacks are more behind the scenes and involve attackers intercepting or manipulating data as it is being transferred between nodes, hurting the

blockchain's confidentiality, integrity, and availability. They may capture sensitive information or overload routers with excessive traffic, causing actual traffic to be dropped, leading to a DoS (Denial of Service) attack [11]. Encryption and secure routing protocols, as well as monitoring network activity for suspicious activity, reduce the risk of routing attacks. Sybil attacks are when hackers utilize false network identities to gain control over a large proportion of the network. This attack could aim to flood the network, causing it to crash, manipulate the consensus mechanism, leading to double-spending, or increase resource consumption. Enforcing strict identification methods, using PoW or PoS to make it costly for a user to create multiple identities, and designing the network to limit the influence of a single point can prevent sybil attacks. Finally, 51% attacks aim to obtain more than 50% of a blockchain network's mining power, giving them control over the ledger to manipulate it. This requires a significant amount of power in order for miner(s) to rally enough resources to attain that much of the blockchain's mining power. This could lead to double-spending, transaction blocking, and forking the blockchain (where an alternate version of the blockchain is created, causing confusion) [1].

It is important that enterprises use measures to enhance the already inherent security of blockchains. Cybersecurity best practices regarding blockchain technology include secure key management, multi-factor authentication, regular security audits, secure coding practices, network segmentation, continuous monitoring and incident response, and blockchain governance and access control [11]. Secure key management is essential for the security of blockchains. Since private keys are the keys used to sign transactions and access assets, they are a vulnerability attackers try to exploit. Hardware wallets for storage of private keys reduce the risk of these attacks by storing private keys offline. Changing keys regularly and multi-signature wallets that require many private keys for transaction authorization also improve security. Multi-factor authentication requires multiple forms of authorization to grant access, for example, combining one-time passwords that are time-sensitive with a regular password to add an extra layer of security. Other biometric authentication, like facial recognition or fingerprints, could also be used. Monitoring the access logs of a blockchain could allow for quick response to suspicious login attempts. Security audits ensure alignment with security policies and identification of any vulnerabilities. These could be internal (by the organization), external (by a third party), or automated audits (software). Secure coding practices ensure that software is developed that is resistant to attacks through error handling, input validation to prevent injection attacks (for instance, inputting malicious code in an online form), and using libraries and frameworks to avoid known vulnerabilities. Network segmentation can be implemented through methods such as firewalls to control traffic between segments. Lastly, monitoring the network continuously and reporting incidents allows for the immediate detection and address of vulnerabilities or potential risks. Access control, like in public and private blockchains, allows companies to lean towards a more decentralized or centralized design based on the company's security needs. Access control allows companies to define who can access and perform what, ensuring that security is a priority. Common models include role-based access control (RBAC) and attribute-based access control (ABAC) to manage permissions [11].

In conclusion, blockchain technology's strength lies in its decentralized, immutable, and transparent nature, which provides security against fraud and tampering, but that does not come without vulnerabilities demonstrated by attacks. As the use of blockchain is becoming more and more popular, implementing cybersecurity best practices and regulatory standards to maintain

the data integrity of these systems is crucial. With these security measures, blockchain technology has potential to reshape data security and trust in transactions in the digital world in the future.

QUESTION 1B: BLOCKCHAIN TECHNOLOGY PRESENTATION

Please see the recording through this link: https://youtu.be/vO5xcJbgaZs

REFERENCES

[1] IBM, "What is Blockchain Security?," *IBM*, 2021. https://www.ibm.com/topics/blockchain-security

[2] Amazon Web Services, "What is Blockchain Technology? - Blockchaining Explained - AWS," *Amazon Web Services, Inc.*, 2023. https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc

[3] Security Quotient, "What is blockchain? | Benefits of blockchain | Cyber security awareness training | Security Quotient," *YouTube*, Mar. 28, 2022. https://www.youtube.com/watch?v=3IVIHUc_LpA (accessed Nov. 11, 2024).

[4] AI Uncovered, "Blockchain Technology Simply Explained," *www.youtube.com*, Aug. 06, 2023. https://www.youtube.com/watch?v=QJn28fFKUR0

[5] Shiksha Online, "Cryptographic Hash Functions in Blockchain - Shiksha Online," *Shiksha.com*, Oct. 19, 2023. https://www.shiksha.com/online-courses/articles/cryptographic-hash-functions-in-blockchain/

[6] C. Crane, "What Is a Hash Function in Cryptography? A Beginner's Guide," *Hashed Out by The SSL Store™*, Jan. 25, 2021. https://www.thesslstore.com/blog/what-is-a-hash-function-in-cryptography-a-beginners-guide/

[7] Crypto.com, "What Is Consensus? A Beginner's Guide," *crypto.com*, May 13, 2022. https://crypto.com/university/consensus-mechanisms-explained

[8] Paxos, "Understanding the Different Blockchain Types," *Paxos*, May 22, 2024. https://paxos.com/2024/05/22/understanding-the-different-blockchain-types/

[9] "Blockchain Security: Common Vulnerabilities and How to Protect Against Them," *Hacken*, Feb. 10, 2023. https://hacken.io/insights/blockchain-security-vulnerabilities/

[10] K. Chin, "The Role of Cybersecurity in Blockchain Technology | UpGuard," *www.upguard.com*, Aug. 03, 2023. https://www.upguard.com/blog/the-role-of-cybersecurity-in-blockchain-technology

[11] J. Anglen, “The Ultimate Guide to Blockchain Security: Threats, Best Practices & Future,” *Rapidinnovation.io*, Sep. 19, 2024. https://www.rapidinnovation.io/post/blockchain-security-best-practices-common-threats

[12] Wikipedia Contributors, “Cryptographic hash function,” *Wikipedia*, Oct. 14, 2019. https://en.wikipedia.org/wiki/Cryptographic_hash_function

[13] S. Team, “Blockchain Technology and Its Layers: The Ultimate Guide | Speed,” *Speed*, May 12, 2023. https://www.tryspeed.com/blog/blockchain-technology-and-its-layers-the-ultimate-guide/ (accessed Nov. 13, 2024).

[14] T. Doan, “Blockchain Technology Applications You Need to Know,” *Eastgate Software*, Jul. 04, 2024. https://eastgate-software.com/blockchain-technology-applications-you-need-to-know/ (accessed Nov. 13, 2024).

[15] A. Takyar, “Ways to Ensure Smart Contract Security,” *LeewayHertz - AI Development Company*, Jan. 09, 2023. https://www.leewayhertz.com/ways-to-ensure-smart-contract-security/

[16] “Blockchain Decentralization: Explained,” *Atomicwallet.io*, 2023. https://atomicwallet.io/academy/articles/what-is-decentralization (accessed Nov. 13, 2024).