Poznan University of Technology

Blockchain Technology And Quantum Computation
Blockchain introduction

Jakub Piotr Hamerliński

Blockchain Technology And Quantum Computation

Agenda

01. Blockchain introduction
02. Cryptography fundamentals
03. Types of blockchains
04. Examples of blockchain-based applications
05. Task

Blockchain introduction

Blockchain introduction

Blockchain technology is a decentralized, distributed ledger system that allows for secure, transparent, and tamper-proof storage of digital information. It was first introduced by the pseudonymous individual or group known as *Satoshi Nakamoto* in 2008 with the release of the Bitcoin whitepaper. Since then, it has evolved and been applied to various industries, including finance, supply chain management, and healthcare.

Blockchain introduction

Here are some key characteristics of blockchain technology:

Decentralization: Unlike traditional centralized systems, where data is stored and managed by a single authority, blockchain technology distributes data across a network of computers (nodes), reducing the risk of a single point of failure and increasing system resilience.

Immutability: Once a block of data is added to the blockchain, it is nearly impossible to alter or delete it without the consensus of the network. This feature ensures the integrity and authenticity of the data stored on the blockchain.

Blockchain introduction

Security: Blockchain technology uses cryptographic techniques to secure the data. Each block contains a unique code called a cryptographic hash, which is generated based on the contents of the block and the hash of the previous block. This chain of hashes makes it extremely difficult for an attacker to manipulate the data without being detected.

Consensus mechanism: For a new block to be added to the blockchain, the majority of the nodes in the network must reach consensus on its validity. This process ensures that only legitimate transactions are added to the blockchain and prevents double-spending or other fraudulent activities.

Blockchain introduction

Transparency: All transactions on a public blockchain are visible to everyone in the network, ensuring transparency and making it easier to audit and verify the data. This feature also allows participants to track the provenance and history of assets or information on the blockchain.

Peer-to-peer (P2P) network: Blockchain technology operates on a P2P basis, eliminating the need for intermediaries such as banks or other central authorities. This can result in faster, more efficient transactions and reduce associated costs.

Smart contracts: Some blockchains, like Ethereum, support the use of smart contracts - self-executing agreements with the terms of the contract directly written into code. These contracts automatically execute when predetermined conditions are met, increasing efficiency, trust, and security in various processes.

Cryptography fundamentals

Cryptography fundamentals

Cryptography is the practice of securing communication and data by applying mathematical techniques and algorithms to transform information in ways that ensure its confidentiality, integrity, and authenticity.

Encryption: Encryption is the process of converting plaintext (readable data) into cipher text (unreadable data) using a specific algorithm and a secret key. The purpose of encryption is to protect sensitive information from unauthorized access by making it unreadable to anyone who does not possess the correct key.

Decryption: Decryption is the reverse process of encryption. It involves converting cipher text back into plaintext using the same algorithm and the appropriate decryption key. Only authorized recipients with the correct key can decrypt and access the original information.

Cryptography fundamentals

Hash functions: A hash function is a one-way cryptographic function that takes an input (data) and produces a fixed-size output, usually a string of characters called a hash. The output is unique to the input data, meaning even a small change in the input will result in a completely different hash. Hash functions are used for various purposes in cryptography, such as verifying the integrity of data, creating digital signatures, and proof-of-work mechanisms in blockchain technology. Commonly used hash functions include SHA-256 and SHA-3.

Digital signatures: A digital signature is a cryptographic technique used to verify the authenticity and integrity of a message or document. It involves the use of a pair of keys: a private key, known only to the signer, and a public key, which can be shared openly. The signer generates a digital signature by applying a cryptographic algorithm (e.g., RSA or ECDSA) to the hash of the message or document using their private key. The recipient can then verify the signature by comparing the hash of the received message with the one generated using the signer’s public key. If the hashes match, it confirms the message’s authenticity and that it has not been tampered with.

Types of blockchains

Types of blockchains

There are several types of blockchains, each with its own set of features and use cases.

Public Blockchains: These blockchains are open to everyone, allowing anyone to participate in the network as a node, miner, or user. Public blockchains are decentralized and transparent, meaning that all transactions are visible to everyone on the network. Bitcoin and Ethereum are well-known examples of public blockchains. Public blockchains often use consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) to secure the network and validate transactions.

Private Blockchains: Private blockchains are restricted to a specific group of participants, usually within an organization or consortium. Access to the network is controlled by a central authority or a group of pre-selected nodes. Private blockchains offer greater control over the network, faster transaction processing, and enhanced privacy compared to public blockchains. However, they sacrifice some decentralization and are more prone to central points of failure. Hyperledger Fabric and R3's Corda are examples of platforms designed for private blockchains.

Types of blockchains

Consortium Blockchains: Also known as federated or permissioned blockchains, consortium blockchains are a hybrid between public and private blockchains. They are managed by a group of organizations or trusted nodes, rather than a single entity. Consortium blockchains maintain some level of decentralization while also providing greater control, privacy, and efficiency. They are particularly useful for industries that require collaboration among multiple entities, such as supply chain management and cross-border payments. Examples of consortium blockchains include Quorum and Ripple.

Hybrid Blockchains: Hybrid blockchains combine elements of both public and private blockchains, offering a customizable solution that can cater to specific use cases. These blockchains allow organizations to maintain a private, permissioned network while also interacting with a public blockchain when necessary. This approach enables businesses to enjoy the benefits of both types of blockchains, including transparency, security, privacy, and efficiency. Dragonchain is an example of a hybrid blockchain platform.

Examples of blockchain-based applications

Examples of blockchain-based applications

Blockchain technology has found applications across various industries, thanks to its unique features like decentralization, transparency, immutability, and security. Here are some examples of blockchain-based applications:

Cryptocurrencies: The most well-known application of blockchain technology is cryptocurrencies like Bitcoin, Ethereum, and Litecoin. These digital currencies leverage blockchain to facilitate secure, transparent, and decentralized peer-to-peer transactions without intermediaries.

Smart Contracts: Blockchain platforms like Ethereum enable the creation of smart contracts, which are self-executing agreements with the terms directly written into code. Smart contracts automate transactions and processes, making them more efficient and secure. They have found applications in areas like finance (e.g., decentralized finance, or DeFi), insurance, and real estate.

Examples of blockchain-based applications

Supply Chain Management: Blockchain can be used to track and trace products throughout the supply chain, ensuring transparency, provenance, and authenticity. This application can help reduce fraud, improve efficiency, and enhance collaboration among stakeholders. Examples include IBM Food Trust, VeChain, and Waltonchain.

Identity Management: Blockchain technology can be applied to create secure digital identities, protecting user data and simplifying processes like authentication and authorization. Platforms like Civic, uPort, and Sovrin provide decentralized identity solutions, which have applications in areas like finance, healthcare, and voting.

Examples of blockchain-based applications

Voting Systems: Blockchain-based voting systems can improve election transparency, security, and efficiency by allowing voters to cast their votes securely and anonymously on a tamper-proof platform. Projects like Follow My Vote, Voatz, and Agora aim to revolutionize voting through blockchain technology.

Intellectual Property and Copyright Management: Blockchain can be used to register and track intellectual property rights, ensuring creators receive fair compensation for their work. Platforms like Po.et and Binded help creators protect their copyrights and streamline licensing processes.

Healthcare: In healthcare, blockchain technology can be used to securely store and share patient records, improving data privacy, accessibility, and interoperability. Projects like Medicalchain, Patientory, and MedRec aim to revolutionize healthcare data management through blockchain.

Examples of blockchain-based applications

Energy: Blockchain can facilitate decentralized energy trading and management, allowing consumers to trade excess energy with others on a peer-to-peer basis. Platforms like Power Ledger, Grid+, and WePower enable decentralized energy markets and promote renewable energy adoption.

Task

Task

Create a Simple Blockchain Ledger

Objective: Design a basic blockchain ledger to record and validate transactions using key concepts such as encryption, hash functions, and digital signatures.

Input:

```
# Transaction     Sender      Recipient       Amount
1               <s-9>       <n-9>           <x-9>
2               <s-8>       <n-8>           <x-8>
(...)           (...)       (...)           (...)
(...)           (...)       (...)           (...)
8               <s-2>       <n-2>           <x-2>
9               <s-1>       <n-1>           <x-1>
10              <s-0>       <n-0>           <x-0>
```

where `s` is first letter of yours surnames combination (smaller index student first)
where `n` is first letter of yours names combination (smaller index student first)
where `x` is first digit of yours index combination combination (smaller index student first)

Task

Create a Simple Blockchain Ledger

Example input:

```
# Transaction     Sender      Recipient       Amount
1                 K           B               10
2                 S           U               9
3                 N           K               8
4                 I           A               7
5                 L           J               6
6                 R           B               5
7                 E           U               3
8                 M           K               3
9                 A           C               2
10                H           J               1
```

If sender and recipient end up the same increment recipient letter by number of given transaction amount e.g. in row 9 recipient was `A` so I've incremented it by `2` so it became `C`

Task

Create a Simple Blockchain Ledger

Instructions:

01. You are given a set of 10 transactions between different parties. Each transaction includes a sender, recipient, and amount (e.g., Alice sends 5 coins to Bob). Create a table to represent these transactions.

02. In pairs, choose one transaction from the table and encrypt it using a simple encryption method (e.g., Caesar cipher, a basic substitution cipher). Exchange the encrypted transaction with your partner, and attempt to decrypt each other's transactions.

03. Calculate a simple hash for each transaction in the table using a basic hash function, such as adding the ASCII values of the characters and taking the remainder when divided by a prime number. Add a column to the table for the hash values.

Task

Create a Simple Blockchain Ledger

05. Discuss the concept of digital signatures and how they could be applied to the transactions. Choose one transaction and create a simple digital signature for it using a basic method, such as appending a unique identifier known only to the sender (e.g., Alice#123). Share the transaction with its "digital signature" with your partner and discuss how this method helps ensure the authenticity and integrity of the transaction.

06. Now, create a simple blockchain ledger by organizing the transactions into "blocks." Group the transactions into sets of three (leaving one transaction ungrouped). For each group, calculate a combined hash by concatenating the individual transaction hashes and applying the basic hash function again. This combined hash will represent the "block" hash.

Task

Create a Simple Blockchain Ledger

07. Link the blocks together by including the previous block's hash in the current block's hash calculation, creating a "chain" of blocks. For the first block, use a predefined hash value (e.g., "0000").

08. Discuss with your partner how this simple blockchain ledger provides transparency, immutability, and security for the transactions. Consider the steps an attacker would need to take to tamper with a transaction and how the blockchain structure would make it difficult to do so.

Task

Create a Simple Blockchain Ledger

There are several ways this task can be complete, depending on the resources available and the desired level of technical engagement. Here are some options:

Paper and pen: You can complete the task using paper and pen, which is a straightforward and accessible option. This approach allows you to focus on understanding the concepts and calculations without the need for technical tools.

Spreadsheet software: You can use spreadsheet software like Microsoft Excel or Google Sheets to create the table of transactions, perform calculations, and organize the data in a structured manner. Spreadsheet software also makes it easy to share the results with peers and instructors.

Programming languages: More advanced students may choose to write a simple program or script in a programming language like Rust, C, or C++ to automate the process of encryption, decryption, hashing, and creating the simple blockchain ledger. This approach allows you to develop your programming skills and gain a deeper understanding of how the concepts are applied in practice.

Sources

Blockchain technology and its applications:

Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons.
Zohar, A. (2015). Bitcoin: Under the Hood. Communications of the ACM, 58(9), 104-113. DOI: https://doi.org/10.1145/2701411

Cryptography fundamentals:

Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography. CRC Press.
Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. John Wiley & Sons.

Types of blockchains:

Merkle, R. C. (1987). A Digital Signature Based on a Conventional Encryption Function. Advances in Cryptology—CRYPTO' 87, 369-378. DOI: https://doi.org/10.1007/3-540-48184-2_32
Buterin, V. (2015). On Public and Private Blockchains. Ethereum Blog. Retrieved from https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Sources

Blockchain-based applications:

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

Thank you

Feel free to reach me via LinkedIn

Fin