Poznan University of Technology

Blockchain Technology And Quantum Computation Security

Jakub Piotr Hamerliński

Blockchain Technology And Quantum Computation Security - Agenda

01. Security aspects of blockchain technology
02. 51% Attack
03. Sybil Attack
04. Eclipse Attack
05. Routing Attack
06. Selfish Mining Attack
07. Replay Attack
08. Timejacking Attack
09. Cryptocurrency fundamentals: Bitcoin, Ethereum, Litecoin
10. Economic, legal, and energy aspects of cryptocurrencies

Security aspects of blockchain technology

Security

Security aspects of blockchain technology

Blockchain technology is often heralded for its security features, which stem from its decentralized and distributed nature, cryptographic elements, and consensus mechanisms. However, while blockchains are designed to be secure, they are not immune to attacks or vulnerabilities. Understanding these potential security threats is vital for the continued development and application of blockchain technology.

Overall, while blockchain has built-in features that enhance its security, it's not invincible. Ensuring the security of a blockchain requires continuous monitoring, regular updates, robust coding practices for smart contracts, and a deep understanding of potential threats and how to mitigate them.

51% Attack

Security

51% Attack

A 51% attack refers to a potential attack on a blockchain network where a single entity or organization manages to control more than 50% of the network's mining power or hashrate. This scenario would allow the attacker to intentionally modify or exclude the ordering of transactions.

Here's a simplified step-by-step breakdown of how a 51% attack could work:

01. Acquiring Majority Control: The attacker, often a mining pool, manages to control more than 50% of the network's computational power. This can be done by owning a large number of mining rigs or by getting other miners to join their pool, unknowingly or otherwise.
02. Starting a Private Chain: Once the attacker gains the majority control, they stop broadcasting their solved blocks to the public network. Instead, they start building their own private chain. This is also known as mining in secret.

Security

51% attack

03. Double Spending: Meanwhile, the attacker makes a transaction on the public chain. For example, they could send a certain amount of cryptocurrency to a merchant in exchange for goods or services. This transaction is recorded on the public blockchain.
04. Outpacing the Public Chain: Since the attacker has more computational power, their private chain grows faster than the public chain. They continue to mine in secret until their chain is longer than the public chain.
05. Broadcasting the Private Chain: Once their private chain is longer, the attacker broadcasts it to the network. According to the rules of most blockchain protocols, the longest chain is considered the valid one. The network then switches to the attacker's chain.

Security

51% Attack

06. Invalidating the Original Transaction: The attacker's chain does not include the original transaction they made on the public chain (the one where they sent cryptocurrency to the merchant). This effectively erases that transaction, making it as if it never happened. This is the "double spend" - the attacker has effectively spent the same amount of cryptocurrency twice. First to buy goods or services, and then they get it back to spend again.

A successful 51% attack undermines the integrity and trust in a blockchain network. However, pulling off a 51% attack is extremely difficult, especially on large, established networks like Bitcoin due to the sheer amount of computational power required. It's more feasible on smaller, less established networks, but even then, it's a significant undertaking.

Sybil Attack

Security

Sybil Attack

A Sybil attack refers to a security threat where a single entity creates multiple identities, or nodes, in a peer-to-peer network. The goal of this attack is to gain a disproportionately large influence over the network. Named after the subject of the book "Sybil" who had a dissociative identity disorder, the term was coined by Microsoft researcher John Douceur in 2002.

Security

Sybil Attack

Here's a simplified step-by-step breakdown of how a Sybil attack could work:

01. Creating Multiple Identities: The attacker creates a large number of pseudonymous identities or directly compromises a large number of nodes on the network. In the context of a blockchain network, this could mean setting up multiple nodes.
02. Gaining Influence: With a high number of nodes under their control, the attacker can manipulate consensus mechanisms, disrupt network operations, or spy on specific transactions.
03. Disrupting the Network: With this influence, the attacker can interrupt the network's functioning in various ways. For example, they could reject or ignore transactions, monopolize mining (in a Proof of Work system), or even modify the blockchain if they control enough nodes.

Security

Sybil Attack

For a concrete example, consider a decentralized file storage system that works on a peer-to-peer network. If an attacker manages to perform a Sybil attack, they could claim to store many copies of a file by creating many identities. However, they might only store one copy or none at all. The system, thinking the file is well-replicated and safe, might stop other nodes from replicating the file. If the attacker then leaves the network or decides to delete the file, the file could be lost.

It's important to note that while a Sybil attack can be a significant threat, there are mechanisms designed to prevent such attacks. For instance, Proof of Work and Proof of Stake consensus mechanisms in blockchains make it computationally or financially costly to control a significant portion of the network, thus providing some level of protection against Sybil attacks.

Eclipse Attack

Security

Eclipse attack

An Eclipse Attack is a security threat where an attacker isolates a node, making it believe that it's interacting with the entire network when it's actually only interacting with the attacking nodes. This attack can prevent the victim from receiving valid transactions or blocks, and trick them into accepting fraudulent ones.

Here's a simplified step-by-step breakdown of how an Eclipse attack could work:

01. Network Mapping: The attacker begins by mapping the network to identify the target node's peers. This could involve creating multiple connections to different nodes in the network to understand the network's topology.

02. Isolating the Node: The attacker then monopolizes all of the victim node's connections, effectively isolating it from the rest of the network. This is done by forcing the victim node to disconnect from its peers and instead connect with the attacker's nodes. In the context of a blockchain, this can be achieved by manipulating network protocols or exploiting network vulnerabilities.

Security

Eclipse Attack

03. Feeding False Information: Once the node is isolated, the attacker feeds it false information. For a blockchain, this could mean providing the victim node with fraudulent transactions or blocks. Since the victim node is cut off from the rest of the network, it has no way of verifying this information.
04. Exploiting the Situation: With the victim node under its control, the attacker can exploit the situation in various ways. They could launch a double-spend attack, censor transactions, or carry out a variety of other malicious activities.

Security

Eclipse Attack

To illustrate this with an example, let's consider a blockchain network. Suppose an attacker successfully isolates a mining node in the network. The attacker then feeds the miner fraudulent transactions or an alternate version of the blockchain. The miner, not having access to the correct blockchain information, could end up wasting computational resources on mining invalid blocks, or it could unintentionally help the attacker conduct a double-spending attack.

Preventing Eclipse attacks is a significant aspect of the design of P2P networking protocols. Solutions can include limiting the number of connections that can be created from a single IP, randomly selecting peers, periodically refreshing connections, and more.

Routing Attack

Security

Routing Attack

In a Routing Attack, an attacker gains control over the network routes in a node-to-node communication to prevent or modify the exchange of information. In blockchain networks that rely on underlying Internet infrastructure, this could lead to serious issues, like network partitioning, balance discrepancies, and double-spending.

Security

Routing Attack

Here's a simplified step-by-step breakdown of how a Routing Attack could work:

01. Gaining Control Over Network Routes: The attacker takes control of an Internet Service Provider (ISP) or compromises a router to intercept network traffic. This could be done through various methods, such as hacking, BGP hijacking, or exploiting vulnerabilities in the routing protocols.
02. Intercepting and Modifying Traffic: Once the attacker has control over the network routes, they can choose to drop, delay, or modify the packets passing through them. This can disrupt the normal functioning of the network or lead to incorrect information being propagated.

Security

Routing Attack

03. Exploiting the Situation: With the ability to control or manipulate the information flow, the attacker can exploit the situation in various ways. They could selectively censor or delay transactions, isolate certain nodes, carry out double-spending attacks, or create conflicting versions of the blockchain.

For a concrete example, consider a blockchain network where an attacker has gained control over a significant part of the network routing. The attacker could delay the propagation of new blocks from a specific miner, causing the rest of the network to mine on an outdated version of the blockchain. This could result in the miner's blocks being orphaned, causing them to lose out on mining rewards. Alternatively, the attacker could partition the network and facilitate double-spending by creating different versions of the blockchain in different partitions.

Security

Routing Attack

Preventing Routing attacks is a complex task because blockchain networks often rely on the existing Internet infrastructure, which they do not control. However, solutions can include using encrypted connections, implementing secure routing protocols, and ensuring that the blockchain network is sufficiently decentralized to reduce the impact of an attack on any single route.

Selfish Mining Attack

Security

Selfish Mining Attack

Selfish Mining is a strategy that allows a miner to gain a higher share of rewards compared to their fair share under the protocol rules. This is done by selectively revealing the blocks they mined to keep other miners working on an old block, while the selfish miner gets a head start on the next block.

Security

Selfish Mining Attack

Here's a simplified step-by-step breakdown of how a Selfish Mining attack could work:

01. Mining in Private: The selfish miner mines blocks on the blockchain but, instead of broadcasting their new block to the network, they keep it secret. This means they start working on the next block ahead of the other miners.
02. Keeping the Lead: If the honest miners find a block and broadcast it to the network, the selfish miner immediately broadcasts their secret block. As per blockchain protocols, the network adopts the block that it received first, and the honest miners' block becomes an orphan block, wasting their computational resources.

Security

Selfish Mining Attack

03. Building a Lead: If the selfish miner manages to mine another block before the honest miners solve their block, they now have a lead of two blocks. The selfish miner can then publish their first block. Even if the honest miners solve the block at this stage, the network will discard it in favor of the selfish miner's chain because it's longer.
04. Repeating the Process: The selfish miner continues this process, keeping their lead and wasting the computational resources of the honest miners, thereby earning more than their fair share of the rewards.

Security

Selfish Mining Attack

To illustrate this, consider a blockchain network where a miner, let's say Alice, has enough computational power to control a considerable percentage of the network's hash rate. Alice decides to keep the blocks she mines a secret from the network.

When Bob, an honest miner, successfully mines a block, Alice immediately broadcasts her block, which she had kept hidden. The rest of the network receives Alice's block first and discards Bob's block, even though Bob's work was honest and valid.

Alice gets the block reward, and Bob gets nothing. Alice then continues this process, gaining more than her fair share of the rewards.

Security

Selfish Mining Attack

In real-world scenarios, selfish mining is mitigated by mechanisms like the difficulty adjustment in Bitcoin, which aims to ensure that no single miner can gain a significant advantage. Moreover, if selfish mining becomes widespread and obvious, it could undermine trust in the network, causing the value of the cryptocurrency to drop. Thus, miners have an incentive to act honestly.

Replay Attack

Security

Replay Attack

A Replay Attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated, delayed, or retransmitted. In the context of blockchain, this typically occurs when a network is forked into two, and transactions from one chain are broadcast to the other chain.

Security

Replay Attack

Here's a simplified step-by-step breakdown of how a Replay Attack could work:

01. Network Fork: The blockchain network undergoes a fork, splitting it into two separate chains, Chain A and Chain B. Each chain has its own unique transactions after the fork, but share a common transaction history before the fork.
02. Capturing a Transaction: The attacker captures a valid transaction from Chain A. This could be done by simply monitoring the network, as transactions are typically broadcast publicly.

Security

Replay Attack

03. Replaying the Transaction: The attacker then broadcasts the captured transaction on Chain B. Since Chain B shares a common history with Chain A, and if proper protection measures aren't in place, it may consider the transaction valid and include it in its own transaction history.
04. Unintended Effects: This can lead to unintended effects. For example, if Alice sent Bob 10 coins on Chain A, Bob could replay this transaction on Chain B to receive an additional 10 coins on that chain, even though Alice only intended to send coins on Chain A.

Security

Replay Attack

For a real-world example, this was a significant concern during the split of Bitcoin and Bitcoin Cash in 2017. If proper measures weren't taken, a transaction made on the Bitcoin network could potentially have been replayed on the Bitcoin Cash network, leading to unintended transfers of Bitcoin Cash.

To protect against Replay Attacks, one common method is to introduce a slight modification in the transaction format or validation rules in the new fork, ensuring that transactions from one chain are invalid on the other. This is known as replay protection.

Timejacking Attack

Security

Timejacking Attack

A Timejacking attack is a sophisticated form of attack on blockchain networks, where the attacker manipulates the timestamp of a node in the network. By doing this, the attacker can potentially influence the blockchain's consensus mechanism, which often relies on accurate timestamps to function correctly.

Security

Timejacking Attack

Here's a simplified step-by-step breakdown of how a Timejacking attack could work:

01. Node Connection: The attacker connects to a node on the network. This can be done relatively easily, as most blockchain networks are designed to be open and accessible.
02. Timestamp Manipulation: The attacker then sends multiple, seemingly legitimate, network connections (peers) with incorrect timestamps to the node. This is intended to manipulate the node's perception of the current network time.

Security

Timejacking Attack

03. Influencing Consensus: Blockchain consensus mechanisms often depend on accurate timekeeping. By manipulating a node's perception of time, an attacker can influence the node's behavior and potentially gain an advantage. For example, the attacker might be able to trick the node into accepting invalid transactions or blocks.
04. Exploiting the Situation: With control over the manipulated node's behavior, the attacker can exploit the situation in various ways. They could launch double-spend attacks, prevent transactions or blocks from being confirmed, or carry out other forms of fraudulent activity.

Security

Timejacking Attack

To illustrate this with an example, consider a Bitcoin network. In Bitcoin, the network time is a median of the timestamps returned by the connected peers. Suppose an attacker connects to a node and provides a large number of peers with incorrect timestamps. If the node's perception of network time is successfully manipulated, the attacker could potentially trick the node into accepting a block with an invalid timestamp, disrupting the normal functioning of the blockchain.

It's important to note that preventing Timejacking attacks can be challenging, as it involves securing a node's network time against manipulation. Solutions can include using secure time synchronization protocols, limiting the influence of individual peers on the network time, and implementing outlier detection algorithms to detect and reject incorrect timestamps.

Cryptocurrency fundamentals

Cryptocurrency fundamentals

Bitcoin

Bitcoin is the first and most well-known cryptocurrency. It was proposed by an anonymous individual or group of individuals under the pseudonym Satoshi Nakamoto in a white paper in 2008, and the network went live in 2009.

Blockchain: Bitcoin's blockchain operates on a proof-of-work consensus mechanism, where miners solve complex mathematical problems to validate transactions and add them to the blockchain.

Usage: Bitcoin was designed as a decentralized digital currency, to be used for peer-to-peer transactions without the need for an intermediary, like a bank or government.

Security: Bitcoin's security comes from its decentralized and distributed nature. Since the blockchain is maintained by numerous nodes all over the world, it's extremely difficult to tamper with.

Cryptocurrency fundamentals

Ethereum

Ethereum was proposed by Vitalik Buterin in late 2013, and the network went live in 2015. While it shares some similarities with Bitcoin, it has a broader goal.

Blockchain: Ethereum's blockchain operates on a a proof-of-stake mechanism (Ethereum 2.0).

Usage: Ethereum was designed to be a platform for creating and executing smart contracts. These are self-executing contracts with the terms of the agreement directly written into code, eliminating the need for a trusted third party.

Security: Ethereum's security is similar to Bitcoin's, but the complexity of its smart contracts can sometimes introduce vulnerabilities.

Cryptocurrency fundamentals

Litecoin

Litecoin was created by Charlie Lee in 2011 as a "lite version of Bitcoin." It shares Bitcoin's goal of being a decentralized digital currency but has several differences intended to allow faster and cheaper transactions.

Blockchain: Litecoin's blockchain operates on a proof-of-work consensus mechanism, like Bitcoin, but it uses a different hashing algorithm (Scrypt) that allows faster block generation.

Usage: Litecoin is intended for use as a digital currency for everyday transactions. Its faster block generation time allows quicker transaction confirmations.

Security: Litecoin's security is similar to Bitcoin's, with its decentralized and distributed nature protecting against most attacks.

Cryptocurrency fundamentals

Step-by-step example of a transaction

Here's a simplified step-by-step example of a transaction in these networks:

01. Initiate a Transaction: Alice wants to send 1 BTC/ETH/LTC to Bob. She creates a transaction with Bob's public address and the amount to be sent.

02. Transaction Verification: The transaction is broadcasted to the network, where miners/nodes verify it. In Bitcoin and Litecoin, this involves checking that Alice has the amount she wants to send. In Ethereum, it might also involve executing a smart contract.

03. Block Addition: Once the transaction is verified, it's added to a block. When a miner solves the mathematical problem (proof-of-work), the block is added to the blockchain.

04. Transaction Complete: Bob now has 1 more BTC/ETH/LTC. He can spend it by creating a transaction, just like Alice did, and the cycle continues.

In the real world, all of this happens behind the scenes. Users just see that they have sent or received BTC/ETH/LTC, with the details handled by their wallet software.

Economic aspect of cryptocurrencies

Cryptocurrency fundamentals

Economic aspect of cryptocurrencies

01. **Decentralization and Financial Inclusion**: Cryptocurrencies aim to provide financial inclusion by enabling peer-to-peer transactions without the need for intermediaries such as banks. This can be particularly beneficial for individuals in regions with limited access to traditional banking services.
02. **Monetary Policy and Inflation**: Some cryptocurrencies, like Bitcoin, have a limited supply and follow predetermined rules, making them resistant to inflation. This is in contrast to fiat currencies, which are subject to central bank policies that can impact their value over time.

Cryptocurrency fundamentals

Economic aspect of cryptocurrencies

03. **Volatility and Speculation**: Cryptocurrencies are known for their volatility, with prices experiencing significant fluctuations. This volatility can be attractive to investors seeking potential high returns but also carries increased risk and uncertainty.
04. **Investment Opportunities**: Cryptocurrencies have created new investment opportunities, with individuals and institutions participating in trading, initial coin offerings (ICOs), and decentralized finance (DeFi) projects.
05. **Cryptocurrency Exchanges and Markets**: Cryptocurrency exchanges facilitate the buying, selling, and trading of cryptocurrencies. These exchanges provide liquidity and serve as platforms for price discovery.

Legal aspect of cryptocurrencies

Cryptocurrency fundamentals

Legal aspect of cryptocurrencies

01. **Regulatory Framework**: Governments worldwide are developing regulatory frameworks to address cryptocurrencies. The legal status of cryptocurrencies varies by jurisdiction, with some countries embracing them, others imposing restrictions, and some outright banning their use.
02. **AML and KYC Compliance**: Cryptocurrency exchanges and service providers often need to comply with anti-money laundering (AML) and know your customer (KYC) regulations. This involves verifying the identities of users and monitoring transactions for suspicious activities.

Cryptocurrency fundamentals

Legal aspect of cryptocurrencies

03. **Taxation**: Cryptocurrency taxation varies by jurisdiction. Governments are increasingly imposing tax regulations on cryptocurrency transactions, including capital gains tax, income tax, or specific reporting requirements.
04. **Consumer Protection**: Authorities are concerned about consumer protection in the cryptocurrency space. Regulations may focus on preventing fraud, ensuring transparency of projects, and safeguarding investors from scams and Ponzi schemes.

Cryptocurrency fundamentals

Legal aspect of cryptocurrencies

05. **Security and Fraud**: Cryptocurrencies can be susceptible to hacking, theft, and fraud. Legal frameworks aim to address cybersecurity concerns, establish penalties for fraudulent activities, and protect user assets.
06. **International Transactions**: Cryptocurrencies provide the potential for fast, borderless transactions. However, legal challenges can arise when different jurisdictions have conflicting regulations or restrictions on cross-border cryptocurrency transfers.

Cryptocurrency fundamentals

Legal aspect of cryptocurrencies

It’s important to note that the legal and regulatory landscape surrounding cryptocurrencies is continually evolving. Individuals and businesses should stay informed about the laws and regulations in their respective jurisdictions to ensure compliance and make informed decisions regarding cryptocurrency activities.

Energy aspect of cryptocurrencies

Cryptocurrency fundamentals

Energy aspect of cryptocurrencies

01. **Proof of Work (PoW) and Energy Consumption**: Bitcoin and some other cryptocurrencies use a consensus mechanism called Proof of Work (PoW), which requires significant computational power and energy consumption. PoW mining involves solving complex mathematical problems to validate transactions and secure the blockchain network. This process requires miners to perform intense computations, which consume substantial amounts of electricity.
02. **Energy Consumption of Mining Operations**: Cryptocurrency mining operations, especially those using PoW, require specialized hardware (ASICs) and consume substantial electricity to power and cool the mining equipment. As the mining difficulty increases and more miners join the network, the energy consumption of the overall network also rises.

Cryptocurrency fundamentals

Energy aspect of cryptocurrencies

03. **Carbon Footprint and Environmental Impact**: The energy consumption of cryptocurrency mining has raised concerns about its carbon footprint and environmental impact. The majority of mining operations rely on fossil fuels, such as coal or natural gas, to generate electricity. This leads to carbon emissions and contributes to global greenhouse gas emissions.
04. **Shift Towards Energy-Efficient Alternatives**: There is an ongoing shift towards alternative consensus mechanisms that aim to reduce energy consumption, such as Proof of Stake (PoS), which requires validators to hold a certain amount of cryptocurrency to participate in block validation. PoS mechanisms consume significantly less energy compared to PoW, as they don't involve resource-intensive computations.

Cryptocurrency fundamentals

Energy aspect of cryptocurrencies

05. **Sustainable Mining Practices and Renewable Energy**: Some initiatives aim to promote sustainable mining practices, such as using renewable energy sources like solar or wind power to run mining operations. Green mining initiatives focus on reducing the carbon footprint associated with cryptocurrency mining and exploring ways to make the process more environmentally friendly.

06. **Energy Efficiency Improvements and Innovation**: Continuous efforts are being made to improve the energy efficiency of mining hardware and optimize mining operations. Additionally, advancements in technology and innovation may lead to more energy-efficient consensus mechanisms and blockchain platforms.

Cryptocurrency fundamentals

Energy aspect of cryptocurrencies

It's worth noting that while energy consumption is a valid concern, some argue that the traditional banking system and other industries also consume substantial energy resources. Moreover, not all cryptocurrencies and blockchain networks have the same level of energy consumption, as it depends on the consensus mechanism and underlying technology.

It is important for researchers, developers, and industry participants to explore and implement sustainable practices to minimize the energy consumption and environmental impact of cryptocurrencies and blockchain technologies.

Sources

01. Truffle

Security aspects of blockchain technology:

01. Investopedia - Blockchain Security: A Comprehensive Guide for Beginners: Link
02. DZone - Understanding Blockchain Security Risks and Challenges: Link
03. ScienceDirect - Blockchain Security: Concepts, Problems, and Solutions: Link

Attacks on blockchain technology:

01. IEEE Xplore - A Comprehensive Study on Blockchain Attacks: Link
02. MDPI - Blockchain Attacks and Security Measures: A Systematic Review: Link

Sources

Cryptocurrency fundamentals:

01. Bitcoin Whitepaper by Satoshi Nakamoto: Link
02. Mastering Bitcoin: Unlocking Digital Cryptocurrencies by Andreas M. Antonopoulos: Link
03. Ethereum Whitepaper by Vitalik Buterin: Link
04. Mastering Ethereum: Building Smart Contracts and DApps by Andreas M. Antonopoulos and Gavin Wood: Link
05. Litecoin Whitepaper by Charlie Lee: Link
06. Litecoin: The Ultimate Beginner's Guide for Understanding Litecoins and What You Need to Know by Elliott Branson: Link

Sources

Economic, legal, and energy aspects of cryptocurrencies:

01. Cryptocurrency: A Comprehensive Introduction by Robert Lennox: Link
02. The Law of Bitcoin by Jerry Brito et al.: Link
03. Energy Consumption of Cryptocurrencies Beyond Bitcoin by Joule: Link

Thank you

Feel free to reach me via LinkedIn

Fin