Het Patel

CS 4301.002

Assignment 2

04/21/2024

# **ScienceDirect: A survey on blockchain technology and its security**

**Abstract**

This paper provides a comprehensive examination of blockchain technology. We delve into its history, exploring the inner workings of various consensus algorithms used to maintain network agreement. We then shed light on the cryptographic foundation of blockchain, including public key cryptography, zero-knowledge proofs, and hash functions. Additionally, we explore the vast potential of blockchain applications across different industries. A core focus of this paper is blockchain security. We employ risk analysis to identify and categorize potential security threats. Real-world attacks and vulnerabilities are then examined to understand their impact. Finally, we explore the latest advancements in securing blockchain systems. The paper concludes by discussing the challenges and future research directions in blockchain technology. Our goal is to pave the way for the development of highly secure and scalable blockchain systems capable of supporting large-scale deployments.

**Table of Contents**

1. **Introduction — 1**
2. **Motivations and Approach for This Survey — 2**

**2.1 Key Contributions of This Survey — 2**

## **Survey for Consensus Algorithms — 2, 3**

1. **Evaluation of Pro & Cons — 3**

**4.1 Pros — 3, 4**

**4.2 Cons — 4**

1. **Conclusion — 4**
2. **References — 4**

**1. Introduction**

Blockchain technology utilizes a distributed ledger system to store data. This approach offers several benefits, including data integrity and availability. Participants within the network can write, read, and verify transactions recorded in this shared ledger. However, modifications and deletions of this information are not permitted, ensuring a permanent and immutable record.

Cryptographic primitives and protocols, such as digital signatures and hash functions, form the security foundation of blockchain systems. These elements guarantee the integrity, authenticity, and non-repudiation of transactions stored on the ledger. Additionally, to maintain agreement on a unified record within a distributed network, blockchain relies on consensus protocols. These protocols essentially define a set of rules that all participants must follow to achieve a consistent global view of the ledger.

In recent years, blockchain has garnered significant interest from academia and industry due to its ability to function in trustless environments. It offers users a compelling set of features, including decentralization, autonomy, immutability, verifiability, fault tolerance, anonymity, auditability, and transparency (as highlighted in references [1, 2, 3]). These characteristics have fueled the rapid adoption of blockchain technology across various fields.

**2. Motivations and Approach for This Survey**

Recognizing the need for a comprehensive understanding of blockchain technology and its security considerations, we embarked on a thorough survey and analysis. This work aims to benefit two primary groups:

* **Blockchain Users:** Equipping users with knowledge about potential security risks empowers them to make informed decisions during transactions.
* **Blockchain Researchers:** By highlighting existing challenges and research trends, we hope to inspire the development of more secure and scalable blockchain systems.

To achieve this goal, we employed a meticulous research methodology. First, we identified a set of relevant keywords: blockchain, survey, consensus algorithm, smart contract, risk, and blockchain security. These keywords formed the foundation for our search through online publications and resources. Furthermore, we focused on scholarly articles related to blockchain published in top security conferences and journals. This included prestigious gatherings like the USENIX Security Symposium, the IEEE Symposium on Security and Privacy, and relevant IEEE Transactions journals. By incorporating research from these esteemed sources, we aimed to overcome potential biases and deliver a comprehensive survey that reflects the current state of knowledge in this field.

**2.1 Key Contributions of This Survey**

This survey offers several key contributions to the field:

1. **Comparative Analysis of Consensus Algorithms:** We provide a detailed comparison of various consensus algorithms, including numerical analysis and figures. Additionally, we explore the fundamental cryptographic principles underpinning blockchain technology.
2. **Smart Contract Deep Dive:** The survey delves into the intricacies of smart contracts and their security considerations.
3. **Blockchain Application Landscape:** We explore the diverse range of applications where blockchain technology is finding practical use, including, but not limited to, various cryptocurrencies.
4. **Security Risks and Solutions:** The survey offers a comprehensive analysis of security risks associated with blockchain, including real-world attacks, vulnerabilities, root causes, and recent advancements in blockchain security measures.
5. **Challenges and Future Directions:** We identify and discuss the key challenges and promising research trends in blockchain technology, paving the way for its development and deployment at scale.

**3. Consensus Algorithms: Powering Blockchain Decisions**

Consensus algorithms are the hidden machinery that keeps blockchain networks running smoothly. They ensure everyone on the network agrees on the order and validity of transactions, preventing chaos and manipulation. Here's a breakdown of four prominent consensus algorithms:

**1. Proof of Work (PoW): The Brawn Approach**

Imagine a network where creating a new transaction record (block) involves solving a complex computational puzzle. PoW works like this: miners compete to solve the puzzle first, using immense processing power. The winner gets to add the block to the chain and earn a reward – often in cryptocurrency. This approach guarantees security – with more miners, the harder it becomes to tamper with the record. However, PoW comes with a hefty price tag – it consumes a lot of energy due to the heavy computation involved. Bitcoin and Ethereum are popular blockchains that utilize PoW.

**2. Proof of Stake (PoS): A More Energy-Efficient Choice**

PoS seeks a more sustainable solution by ditching the energy-intensive computational battles. Here, nodes (participants in the network) "stake" their own cryptocurrency holdings. The network then selects validators based on the amount staked, like holding voting rights based on ownership. Those chosen earn transaction fees as rewards for validating blocks. This approach incentivizes honest behaviour, as losing your stake is the penalty for trying to add invalid blocks. Ethereum 2.0 is transitioning from PoW to PoS to address scalability and sustainability concerns.

**3. Delegated Proof of Stake (DPoS): A Democratic Take**

DPoS adds a layer of democracy to PoS. Instead of staking for direct validation, token holders elect delegates who act as validators. Users with more tokens have more voting power, influencing who gets to validate transactions. This system can be faster and more efficient than PoS, as the number of validators is smaller. EOS is a blockchain that utilizes DPoS.

**4. Directed Acyclic Graph (DAG): A Different Blockchain Architecture**

Unlike the block-based structure of other algorithms, DAG uses a directed acyclic graph – a network of interconnected transactions. Each transaction links to a few previous ones, creating a web-like structure. There are no blocks to mine, and transactions directly validate each other. A small Proof of Work operation helps prevent spam and ensures the validity of past transactions. IOTA utilizes DAG, aiming for faster transaction processing and scalability.

**4. Evaluation of Pros and Cons**

**4.1 Pros**

* **Detailed comparison of consensus algorithms**

The survey provides a comprehensive analysis of various consensus algorithms, including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Proof of Elapsed Time (PoET). This can be helpful for users who are trying to decide which blockchain platform to use, as each algorithm has its own advantages and disadvantages in terms of security, scalability, and energy consumption.

* **Covers a wide range of applications**

The survey goes beyond just the technical aspects of blockchain and explores the technology's potential applications in various industries. This can be beneficial for users who are interested in learning how blockchain can be used to solve real-world problems. Some of the applications covered in the survey include cryptocurrencies, supply chain management, and government services.

* **Security analysis**

The survey analyzes the security risks of blockchain systems and describes recent security measures. This is important for users to be aware of, as blockchain technology is still relatively new and evolving, and there have been some security breaches in the past.

**4.2 Cons**

* **Limited focus on prior surveys**

The authors acknowledge that other surveys may have partially addressed the security of blockchain. This suggests that the survey might not be entirely novel, and it would be beneficial to compare it with other existing surveys to see how it builds upon or differs from previous work.

Overall, the survey provides a valuable resource for those who want to learn more about blockchain technology, including its technical underpinnings, potential applications, and security considerations. However, it would be even more comprehensive if it explicitly compared itself to other surveys in the field.

**5. Conclusion**

This paper has strived to provide a comprehensive exploration of blockchain technology and its security landscape. Through in-depth analysis, we have delved into various aspects of blockchain, including its history, consensus algorithms, smart contracts, and the cryptographic foundations that ensure integrity, authentication, non-repudiation, and secure payment addressing. We have also explored the diverse applications of blockchain technology, showcasing its potential beyond cryptocurrencies.

Our hope is that this work will serve as a valuable resource for two key audiences:

* **Blockchain Users:** By understanding the potential security risks associated with blockchain systems, users can become more vigilant and make informed decisions when conducting transactions.
* **Blockchain Researchers:** This survey provides a springboard for further research endeavours. By highlighting the existing challenges and emerging research trends, we aim to inspire researchers to develop even more secure and scalable blockchain systems suitable for large-scale deployments.

Ultimately, this paper represents our effort to bridge the knowledge gap surrounding blockchain technology and its security. We believe that by empowering both users and researchers, we can pave the way for a more secure and robust future for blockchain.

**6. References**

* Guo, H., & Yu, X. (2022, June 1). *A survey on blockchain technology and its security*. Blockchain. Research and Applications.<https://doi.org/10.1016/j.bcra.2022.100067>