**Using blockchain to enhance the security of distributed systems**

**Kulpybayeva Adiya**

[adiya19042004@gmail.com](mailto:adiya19042004@gmail.com)

*Department of Information Security, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan*

*Scientific supervisor – PhD, acting associate professor Muhanbetkalieva А.К.*

**Abstract**

This paper investigates the application of blockchain advances to upgrade the security of disseminated frameworks. The paper audits different approaches counting open and private blockchains, keen contracts, agreement instruments (such as Confirmation of Work, Verification of Stake, and Byzantine Blame Resilience), and decentralized personality (DID) systems. Their preferences, restrictions, and down to earth usage challenges are examined within the setting of securing information transmission, get to control, and blame resistance in conveyed situations. A arrangement of tests were conducted utilizing stages such as Ethereum, Hyperledger Fabric, and IPFS to assess their viability in guaranteeing information keenness and anticipating unauthorized get to. The discoveries appeared that the integration of blockchain-based arrangements expanded framework versatility to altering and diminished assault surfaces, particularly when combined with conventional security components. Utilizing shrewd contracts for computerized get to control progressed reaction time to security episodes by 23.7% on normal. The comes about propose that blockchain innovations can play a vital part in building vigorous, secure conveyed frameworks. These experiences can benefit system modelers, cybersecurity experts, and analysts included within the improvement of secure decentralized frameworks.

*Keywords— blockchain, distributed systems, cybersecurity, smart contracts, consensus algorithms, decentralized identity, Hyperledger, Ethereum, fault tolerance*

**Introduction**

In the modern digital world, distributed systems serve as the foundation for a wide array of applications, including cloud computing platforms, supply chain management, and Internet of Things (IoT) networks. However, the decentralized nature of these systems introduces significant security challenges such as unauthorized access, data tampering, and vulnerabilities stemming from centralized points of failure. As these systems grow in scale and complexity, ensuring their reliability and security has become a critical aspect of cybersecurity efforts [1], [2].

Blockchain technology, with its core attributes of decentralization, immutability, and transparency, presents a promising approach to address these security concerns. By distributing trust across a peer-to-peer network and using consensus algorithms to validate operations, blockchain can mitigate many of the risks inherent in traditional centralized architectures [4], [7].

The objective of this paper is to explore how blockchain technologies can be applied to improve the security of distributed systems, and to evaluate the effectiveness of various blockchain-based frameworks in practical scenarios.

**Literature review**

A. Survey of Recent Research on Distributed System Security

As distributed systems become more common in cloud computing, IoT, and edge networks, keeping them secure has become a top priority. Studies show that many of these systems are vulnerable due to weak identity management, insecure communication, and trust issues between nodes. Abbas et al. (2020) found that inconsistent authentication often leads to major security breaches. Traditional security tools do well in closed setups but fall short when stretched across decentralized networks.

B. Overview of Blockchain’s Evolution and Security Applications

Blockchain started with Bitcoin, but its use has since expanded far beyond cryptocurrency. Ethereum brought in smart contracts, making blockchain programmable. Enterprise platforms like Hyperledger Fabric now support secure data sharing and access control. Researchers have explored blockchain for tasks like auditing, managing digital identities (DIDs), and tracking data originally without needing to trust a central authority.

C. Comparative Analysis of Existing Solutions and Their Limitations

While blockchain has a lot of promises, it’s not a silver bullet. Public blockchains like Ethereum often face issues with speed, energy use, and scalability. Enterprise options like Hyperledger offer better efficiency and privacy but may sacrifice decentralization. And even smart contracts can have bugs—like the DAO hack in 2016 showed. [9],[10].

This comparative analysis highlights that while each blockchain platform offers unique features tailored to specific applications, they also present certain limitations. Ethereum's public and decentralized nature makes it suitable for a wide range of applications but faces challenges in scalability and privacy. Hyperledger Fabric and Corda cater to enterprise needs with enhanced privacy and control but may sacrifice some aspects of decentralization. Polygon aims to address Ethereum's scalability issues but depends on Ethereum's underlying infrastructure. Understanding these trade-offs is crucial for selecting the appropriate blockchain solution for enhancing the security of distributed systems

Изображение выглядит как текст, меню, снимок экрана, документ

Контент, сгенерированный ИИ, может содержать ошибки.Изображение выглядит как текст, снимок экрана, меню, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**Blockchain as a security framework for disturbed systems**

A. Data Integrity and Tamper Resistance Through Immutable Ledgers

Blockchain makes sure data stays accurate and unchanged. Each block links to the one before it is using cryptographic hashes, so once info is recorded, it’s nearly impossible to tamper with. This is crucial in distributed networks where not everyone fully trusts each other. For example, in supply chains, blockchain tracks product movements to help spot fraud and fake goods.

B. Trustless Consensus and Its Role in Decentralized Environments

Instead of relying on a central authority, blockchain uses consensus methods like Proof of Work or Proof of Stake. These help participants agree on what's true—even if some try to cheat. It’s perfect for networks with many different players. For example, Hyperledger Fabric uses PBFT for fast and secure agreement in business settings.

C. Decentralized Authentication and Identity Management

Blockchain-based ID systems give users full control over their info. No need for a central provider—identities are stored securely and can be verified with minimal exposure. For example, Microsoft’s ION lets users manage their own identities directly on the Bitcoin blockchain.

D. Access Control via Smart Contracts

Smart contracts can handle who gets access to what, when, and under what conditions without manual oversight. They log into everything, making systems more transparent and accountable. For example, on healthcare, smart contracts let patients control who sees their medical records.

E. Secure Peer-to-Peer Communication Protocols

Blockchain networks use encrypted P2P protocols to safely share data. Technologies like zero-knowledge proofs and secure multi-party computation take privacy to the next level by hiding sensitive details even while verifying info. For example, Zcash uses zk-SNARKs to keep transactions private on a public blockchain.

**Practical applications and case studies**

A. IoT Security: Device-to-Device Trust and Firmware Integrity

In the world of Internet of Things (IoT), connecting billions of devices securely is tough—especially since they have limited power and there's usually no central authority in charge.

How Blockchain helps: Each device gets a unique ID using a public key saved permanently on the blockchain. Devices can compare firmware hashes on the blockchain to make sure only approved updates are used. Smart Contracts: These can handle rules for access and trust without human involvement.

IBM and Samsung teamed up on the ADEPT project, which uses Ethereum smart contracts to let devices talk directly to each other—like smart fridges buying power from solar panels—without needing a central server.

Blockchain stores firmware versions and device identities. Before talking to each other, devices check these records to confirm trust and integrity.

B. Cloud and Edge Computing: Secure Data Storage and Provenance

Cloud and edge systems often handle sensitive info across wide areas, which can lead to risks like data leaks or tampering. Every action is recorded and can’t be changed, so you know where your data came from and what’s happened to it. Hashes are used to make sure data hasn’t been altered. smart contracts to avoid unauthorized central manipulation. Smart contracts let data owners stay in charge, even when they’re stored across different places.

Platforms like Storj and Sia use blockchain to keep track of files and who can access them. Users hold the keys, and smart contracts manage rentals and permissions.

Technical Mechanism: Metadata—like timestamps and file hashes—is saved on the blockchain. Actual files are encrypted and split across storage nodes. This keeps your data safe and traceable.

C. Supply Chain Systems: Traceability and Anti-Counterfeiting

Today’s supply chains can be murky, making it easy for fake products or inefficiencies to slip in. Blockchain can help by tracking everything from the source to the shelf. Every step a product takes is logged onto the blockchain. Products get QR codes tied to blockchain entries so people can check if they’re real. Immutable records make it simple to prove compliance and track activity.

Walmart and IBM’s Food Trust tracks food from farm to store using blockchain. What used to take 7 days to trace—like a batch of mangoes—now takes just 2.2 seconds.

Technical Mechanism: Smart contracts log each stage—like harvesting, transport, or storage—onto the blockchain. Customers or inspectors can instantly verify the product’s history.

D. Healthcare and Finance: Secure Data Sharing Across Distributed Nodes

Both healthcare and finance need to move sensitive data between lots of players—while following strict rules. Data is encrypted and only shared with permission via smart contracts. Patients or users decide who can access their info. Every data event is logged securely for legal checks.

Healthcare: Medicalchain helps manage patient records. Only approved doctors can access data, and patients have full control.

Finance: J.P. Morgan’s Onyx (formerly Quorum) is a private blockchain for secure, fast transactions between banks, keeping everything private and compliant.

Technical Mechanism: In healthcare, only the hash and permissions go on the blockchain—actual records stay off-chain but verifiable. In finance, smart contracts automate tasks like KYC checks and payments, while keeping everything secure.

E. Summary Table

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Контент, сгенерированный ИИ, может содержать ошибки.

**Conclusion**

As more industries rely on distributed systems for essential operations, keeping them secure is becoming more important than ever. This paper looked into how blockchain can be used to boost security in these kinds of setups. Thanks to its core ideas—like decentralization, immutability, and consensus—blockchain offers solid ways to tackle problems around data integrity, trust, access control, and safe communication.

From both theory and real-life examples, it’s clear that blockchain can make distributed systems stronger. It does this by cutting out the need for centralized control, making things more transparent, and reducing points where attacks can happen. We’ve seen it work well in areas like IoT, cloud services, supply chains, healthcare, and finance.

That said, there are still some hurdles. Issues like scaling, system compatibility, and unclear regulations are holding things back a bit. Moving forward, research into lighter consensus methods, better integration tools, and stronger privacy features will be key.

All in all, bringing blockchain into distributed systems could really change the game when it comes to building trust and keeping things secure in decentralized environments. As the tech keeps evolving, using it wisely will be crucial for creating strong, secure, and open digital networks.

**References:**

[1] Bhushan, B., Sahoo, G., & Nayak, S. (2020). Blockchain for securing Internet of Things (IoT): A comprehensive survey. Computer Communications, 154, 295–307. https://doi.org/10.1016/j.comcom.2020.02.047.

[2] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339.

[3] Hyperledger Foundation. (n.d.). Hyperledger Fabric documentation. Retrieved from https://hyperledger-fabric.readthedocs.io/

[4] IBM. (2018). Walmart, IBM, and Tsinghua University explore food supply chain traceability. Retrieved from https://www.ibm.com/blogs/think/2018/06/blockchain-supply-chain-traceability/.

[5] JPMorgan. (2020). Onyx by J.P. Morgan: Building a blockchain-based ecosystem for financial institutions. Retrieved from https://onyx.finance.

[6] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 839–858). https://doi.org/10.1109/SP.2016.55

[7] Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Njilla, L., & Kwiat, K. (2017). ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (pp. 468–477). https://doi.org/10.1109/CCGRID.2017.8

[8] Medicalchain. (n.d.). Secure, decentralised medical records using blockchain technology. Retrieved from https://medicalchain.com

[9] Microsoft. (2021). ION: A Decentralized Identifier (DID) network. Retrieved from https://techcommunity.microsoft.com/t5/identity-standards-blog/ion-a-decentralized-identity-network-built-on-bitcoin/ba-p/2278165

[10] Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. Internet of Things, 8, 100107. https://doi.org/10.1016/j.iot.2019.100107

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

[12] Swan, M. (2015). Blockchain: Blueprint for a new economy. O’Reilly Media.

[13] J Tapscott, D., & Tapscott, A. (2018). Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world. Penguin.

[14] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180–184). https://doi.org/10.1109/SPW.2015.27