3rd Blockchain and Cryptocurrence Conference (B2C' 2024),
16-18 October 2024, Tenerife (Canary Islands), Spain

Oral ☒ / Poster ☐ / The same ☐ Topic: *Enterprise Blockchains*

Virtual: Zoom ☐ / Pre-recorded video ☐

Borderless – Towards a novel approach for a secure and privacy-compliant blockchain

Christian Hammermeister [1], Larissa Krämer [2] and Patrick Stuckmann-Blumenstein [3]
[1] Borderless Technologies GmbH, Dortmund, Germany
[2] Chair of Material Handling and Warehousing, TU Dortmund University, Germany
[3] Chair of Enterprise Logistics, TU Dortmund University, Germany

E-mail: christian.hammermeister@borderless-technologies.com

Summary: Blockchain technology facilitates data sharing in multi-stakeholder processes such as shared manufacturing due to its decentralization and immutable data storage. However, one challenge in blockchain-based data sharing in industrial processes is guaranteeing data privacy while balancing scalability, security, and decentralization. This paper introduces "Borderless," a novel blockchain approach that guarantees decentralization and immutability while ensuring data privacy and legal compliance. Unlike existing solutions, Borderless integrates advanced privacy measures and a robust legal framework, making it a comprehensive, secure option for enterprises with stringent regulatory requirements. Our methodology includes a review of related work, the proposal of the Borderless framework, and simulative benchmarking against other blockchain frameworks. This comparative analysis demonstrates Borderless's suitability in meeting the dual demands of security and privacy for industry without compromising the core benefits of blockchain technology.

Keywords: Blockchain, Smart contract, Borderless, Data privacy, Scalability

1. Introduction

The significance of blockchain technology lies in its ability to revolutionize trust and transparency in multi-stakeholder processes, such as shared manufacturing, by providing a decentralized, standardized, immutable and real-time data exchange [1]. Smart contracting, which automates and enforces agreements using programmable code, further enhances this capability by streamlining industrial interactions [2]. However, in a decentralized blockchain environment for industrial applications, ensuring data privacy is paramount to protect sensitive information and maintain competitive advantage of companies [3]. Additionally, legal compliance is crucial to ensure secure adoption of blockchain technology in industry.

Our aim is to provide a blockchain solution to science and industry that is inherently secure, keeps data privacy and ensures legal compliance while being performant and decentralized at the same time. Consensus mechanisms play a pivotal role in determining the performance and integrity of a blockchain network, making them essential components of blockchain architecture. By bridging the strengths of Proof of Stake (PoS) and Proof of Authority (PoA), we endeavour to create a consensus mechanism that optimizes network scalability, enhances security, and preserves decentralization. Against that backdrop, our research question is: “How can legal compliance, data privacy, decentralization, and network performance and scalability be reconciled in a blockchain network?”

This research introduces a novel approach to blockchain called Borderless, addressing legal compliance and data privacy for industrial applications. Furthermore, the development of an efficient consensus mechanism extends current knowledge in blockchain science, fostering innovation and efficiency in diverse industrial applications while enhancing trust and transparency.

2. Related Work

This section provides foundational insights into blockchain technology and consensus mechanisms for the development of Borderless. Consensus mechanisms are essential in blockchain to achieve agreement among distributed nodes, ensuring the integrity and consistency of the blockchain ledger [4]. Key characteristics of consensus mechanisms such as PoA, PoS, and Proof of Work (PoW) are critical to blockchain performance and define their operational efficiency, security and scalability [4]. PoA is based on reputation and is noted for its efficiency in permissioned networks, whereas the energy-efficient PoS is based on a stake in the network currency. PoW ensures robust data integrity through computational efforts [5].

Besides, the integration of data privacy and legal compliance within blockchain technology is a critical area of ongoing research. Studies have explored privacy-preserving techniques such as zero-knowledge proofs and secure multi-party computation to protect sensitive information on public blockchains [6]. Additionally, researchers examine the alignment of blockchain systems with regulatory frameworks, such

as the european General Data Protection Regulation (GDPR), to ensure legal compliance and address jurisdictional challenges [7].

3. Proposal of a new Secure, Decentralized and Private Blockchain

The Borderless Blockchain introduces a novel private blockchain architecture designed to harmonize blockchain's decentralization and immutability with rigorous data privacy and legal compliance requirements. It employs a certificate authority (CA) to link specific wallets to legal entities, ensuring the legal certainty of smart contracts and guaranteeing data integrity. Unlike traditional blockchains, smart contracts on the Borderless Blockchain execute through a distinct consensus process on participant servers, enhancing flexibility and efficiency. A hybrid consensus mechanism, mixing PoS and PoA, underpins the system, balancing energy efficiency, throughput, and trustworthiness by incentivizing validators to act honestly through staking, while also leveraging the identity-based selection of validators to ensure reliability and integrity.

Additionally, Borderless utilizes several other mechanisms to secure tokens, assets, and smart contract-related data, maintaining data sovereignty for all participants. To avoid tracing and linking transactions to the same recipient, Borderless uses stealth addresses, which are unique, one-time-use addresses for transactions. Additionally, ring signatures allow a user to sign a message on behalf of a group, making it impossible to determine which group member created the signature, thereby providing anonymity. Borderless further uses Merkle proofs to verify that a specific piece of data is part of a larger dataset without revealing or accessing the entire dataset by leveraging a Merkle tree structure. Besides, Borderless provides a high level of security by using the Advanced Encryption Standard-256 (AES-256), a symmetric encryption algorithm that uses a 256-bit key to encrypt and decrypt data. AES-256 is recognized for its ability to resist brute-force attacks, making it a suitable choice for securing sensitive information.

The Borderless Blockchain does not only uphold the core benefits of blockchain — like immutability and decentralization of data and trust — but also integrates advanced privacy measures and a strong legal framework to offer a comprehensive, secure blockchain solution suitable for enterprises needing to meet strict regulatory standards.

4. Benchmark against Test Networks

To evaluate the performance of Borderless for industrial applications, we comprehensively examine the borderless framework and benchmark it against various test networks within the Ethereum ecosystem. These test networks include those utilizing PoA and PoW consensus mechanisms we have set up. This approach allows us to evaluate the performance and efficiency of the borderless framework in different consensus environments. The test networks are configured to be comparable, considering parameters such as gas limits, gas targets, block time and other relevant metrics across these networks to ensure a standardized benchmarking process. Key performance indicators, including transactions per second, gas units per block, validation time, and network resource utilization (Central Processing Unit (CPU) and Random-Access Memory (RAM) usage), are meticulously evaluated to gauge the efficiency and scalability of each network. By employing this benchmarking approach, we discern the effectiveness of our newly proposed blockchain consensus mechanism, Borderless. Furthermore, we investigate the implications of exceeding scalability limits, shedding light on potential bottlenecks and performance degradation within each network configuration. Through this rigorous assessment, we provide actionable insights into optimizing blockchain scalability and advancing the adoption of innovative consensus mechanisms in decentralized systems.

5. Conclusion

In summary, current research underscores the challenge of achieving secure, legally compliant, scalable, and cost-effective blockchain transactions. Our proposed solution, Borderless, integrates existing consensus mechanisms while emphasizing privacy and security for industry applications. The forthcoming extended paper will detail our methodology, including test network setup and benchmarking, to empirically validate our framework and consensus mechanism, contributing to improved efficiency and trust in blockchain technology.

Acknowledgements

The work presented in this paper was funded by the Deutsche Forschungsgemeinschaft (DFG) – 276879186/ GRK2193.

References

[1] X. Guo, G. Zhang, and Y. Zhang, "A Comprehensive Review of Blockchain Technology-Enabled Smart Manufacturing: A Framework, Challenges and Future Research Directions," *Sensors*, vol. 23, no. 1, Art. no. 1, Jan. 2023, doi: 10.3390/s23010155.

[2] L. Krämer, P. Kaiser, J. Kajewski, and M. Roidl, "Reversing the Digital Twin – Smart-Contracting in Hybrid Production," in *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, Berlin, Germany: IEEE, Jul. 2023, pp. 1–6. doi: 10.1109/COINS57856.2023.10189284.

[3] N. Große, P. Stuckmann-Blumenstein, D. McInnis, and Y. Qiao, "Proposal of the Technical Implementation of 3D Printers in a Blockchain- based Exchange of Capacity," in *Proceedings of the 1st Blockchain and Cryptocurrency Conference*, 2022, pp. 49–51.

[4] B. Lashkari and P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," *IEEE Access*,

pp. 43620–43652, 2021, doi: 10.1109/ACCESS.2021.3065880.

[5] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Banff, AB: IEEE, Oct. 2017, pp. 2567–2572. doi: 10.1109/SMC.2017.8123011.

[6] S. Barj, A. Ouaddah, and A. Mezrioui, "A Review of Privacy-Preserving Cryptographic Techniques Used in Blockchain Platforms," in *Digital Technologies and Applications*, vol. 668, S. Motahhir and B. Bossoufi, Eds., in Lecture Notes in Networks and Systems, vol. 668. , Cham: Springer Nature Switzerland, 2023, pp. 230–240. doi: 10.1007/978-3-031-29857-8_23.

[7] S. Han and S. Park, "A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review," *IEEE Access*, vol. 10, pp. 103888–103905, 2022, doi: 10.1109/ACCESS.2022.3210110.