An Integrated Blockchain-Based Certificate Authentication and Issuer Validation System: Design, Implementation, and Performance Evaluation

Vishal Prasad Sharma[1], Anayat Altaf Shah[1] , Raj Kumar[1], Vandan Kumar M[1]
[1] Department of Computer Science and Engineering, ACS College of Engineering, Bangalore 560074, India

ABSTRACT
The rapid digitization of certificates and credentials has posed challenges related to authenticity, tampering, and verification. This paper addresses these challenges by integrating blockchain technology into the certification process, creating a decentralized, tamper-proof system for managing and verifying educational and professional certificates. Blockchain, with its immutable ledger and consensus mechanisms, ensures data integrity, reduces reliance on third-party verification, and streamlines processes. Moreover, by integrating Human-in-the-Loop (HITL) active learning techniques — commonly used in cyber intrusion detection — the system can adapt to emerging threats, improving its resilience over time. HITL introduces an interactive component, where human validators participate in the loop, refining the detection of anomalies or suspicious certificate activity, thus enhancing system trustworthiness. The combination of blockchain and HITL not only fortifies the security of digital certificates but also establishes a model of continuous system improvement, setting a new standard for trust and transparency in digital credentialing.

Index Terms—Blockchain, Certificate Authentication, Issuer Validation, Smart Contracts, Decentralized Systems, Digital Credentials, Security, Scalability.

I.INTRODUCTION
The global shift toward digitalization has transformed numerous aspects of daily life, from communication to commerce, and even how we verify academic and professional credentials. Certificates, which serve as proof of education, skills, and achievements, are key digital assets in today's economy. Traditionally paper-based, these certificates were stored in centralized databases and required manual verification processes. However, with the rise of online education, international student mobility, and global hiring, the demand for efficient, reliable verification systems has escalated.

Traditional certificate verification faces multiple challenges: centralized databases can be hacked, forged certificates have become more sophisticated, and cross-border verification often encounters compatibility and trust issues. These problems have led to financial losses, reputational damage, and systemic inefficiencies. Institutions, employers, and government bodies need faster, more secure ways to validate credentials.

Blockchain technology offers a promising solution. Blockchain is a decentralized ledger where data is validated and recorded across a network of computers. Each block in the chain contains a batch of transactions that are cryptographically secured, making the data immutable. This transparency and immutability make blockchain ideal for ensuring the authenticity of digital certificates. Blockchain eliminates the need for intermediaries by allowing certificates to be instantly verified by any third party. Smart contracts, which are programmable scripts running on the blockchain, further streamline the verification

process. These contracts automatically validate certificates, reducing administrative overhead and speeding up decision-making processes such as hiring or admissions. With blockchain, the risk of fraudulent certificates is reduced, as the system ensures that once data is recorded, it cannot be altered without the consensus of the entire network.

However, while blockchain ensures data integrity and transparency, it is not a complete solution. Blockchain systems are still susceptible to challenges such as scalability issues, privacy concerns, and the inability to adapt to new threats. For example, while blockchain can detect tampering with a certificate's recorded data, it cannot identify emerging fraud patterns such as phishing or deepfake-generated certificates. These sophisticated fraud techniques may evade automated verification systems, highlighting the need for adaptive mechanisms.

This is where the concept of **Human-in-the-Loop (HITL)** becomes crucial. HITL is a framework that incorporates human expertise into automated systems, allowing them to handle uncertainty and adapt to new threats. By integrating HITL, blockchain-based certificate systems can dynamically adjust to novel fraud patterns that purely automated systems might miss. For instance, if a verification request is deemed suspicious — such as an unusually large batch request from an unfamiliar employer — the system can escalate the case to a human reviewer, who can assess the situation and provide judgment.

Additionally, HITL mechanisms enable **active learning**, where the system selectively queries human experts about the most uncertain cases, maximizing learning efficiency while reducing the need for human input. Over time, this feedback loop improves the system's ability to identify potential fraud, creating a more robust verification system.

The integration of HITL into blockchain-based certificate systems also enhances trust. Human involvement provides an accountability mechanism and a pathway for appeal or escalation, particularly in high-stakes contexts like job offers or immigration decisions. This approach is especially important in cross-border scenarios, where different legal and cultural expectations may influence certificate verification.

In summary, the combination of blockchain and HITL offers a comprehensive solution to the challenges faced by digital certificate systems today. Blockchain provides the foundation for secure, immutable certificates, while HITL adds flexibility, adaptability, and trust. This hybrid system enhances the security, efficiency, and reliability of certificate verification, ensuring a more robust solution for academic and professional credentials in the digital age.

II. LITERATURE REVIEW

The integration of blockchain technology into certificate authentication systems has attracted increasing research attention due to its potential to address long-standing problems of trust, security, and efficiency. Traditional certificate systems rely on centralized authorities, which often creates bottlenecks, vulnerability to attacks, and single points of failure. Blockchain, as a decentralized and immutable ledger, provides a promising solution by eliminating the need for intermediaries and ensuring tamper-proof records. One of the landmark efforts in this domain is the MIT Media Lab's Blockcerts system, which allows educational institutions to issue digital certificates that are cryptographically signed and anchored on public blockchains, providing verifiable and permanent proof of credentials [1]. This approach not only increases transparency but also significantly reduces administrative overhead by enabling third parties to validate certificates without direct contact with issuing institutions.

Table 1 . Literature Review

Sl. No.	Author (Ref. No.)	Relevant Concepts	Limitations
1	S. Nakamoto [1]	Bitcoin; peer-to-peer electronic cash; blockchain.	Focused on cryptocurrency; scalability issues.
2	V. Buterin [2]	Ethereum; smart contracts; decentralized apps (DApps).	Scalability; high gas fees.
3	J. Zhang et al. [3]	Blockchain-based certificate authentication system.	Limited scalability; interoperability gaps.
4	L. Chen et al. [4]	Secure, efficient certificate management.	Mostly theoretical; lacks real-world tests.
5	M. Crosby et al. [5]	Overview of blockchain beyond Bitcoin.	High-level; little technical detail.
6	K. Christidis, M. Devetsikiotis [6]	Blockchain + IoT; smart contracts in IoT.	IoT resource limits; integration challenges.
7	N. Kshetri [7]	Blockchain for cybersecurity and privacy.	Conceptual; lacks empirical validation.
8	X. Xu et al. [8]	Blockchain architecture patterns and design.	Limited case studies; more architectural.
9	A. Reyna et al. [9]	Blockchain-IoT integration; challenges, opportunities.	Scalability, latency issues.
10	P. Tasca, C. J. Tessone [10]	Blockchain taxonomy; classification framework.	Theoretical; lacks application focus.

Several national and institutional projects have expanded on this foundational idea. For instance, Singapore's OpenCerts framework has been widely adopted across universities and government agencies, creating a scalable ecosystem for blockchain-based educational credentials. These systems benefit from blockchain's core properties—immutability, decentralization, and transparency—allowing issued certificates to be permanently recorded and easily verified by anyone with access to the blockchain [2]. However, despite these advantages, challenges persist. One key issue is that while the blockchain guarantees the integrity of the recorded data, it does not inherently verify the authenticity of the data at the point of entry. If an institution or authorized issuer uploads a fraudulent or erroneous certificate, the blockchain will immutably preserve it, highlighting the need for more robust validation mechanisms at the issuance stage [3].

Beyond blockchain, the cybersecurity field has explored human-in-the-loop (HITL) approaches to balance machine efficiency with human expertise, especially in complex or evolving threat environments. In domains like intrusion detection, anomaly detection models often produce ambiguous outputs or false positives that require human analysts to investigate and resolve [4]. This combination leverages the adaptability and judgment of humans with the scalability of automated systems. A particularly effective subset is active learning, where machine learning models selectively query human experts for input on uncertain or informative cases, thereby reducing the overall labeling burden while improving system performance [5]. While extensively applied in intrusion detection and malware analysis, HITL mechanisms have rarely been incorporated into blockchain-based credential verification systems.

There is growing recognition that combining blockchain systems with HITL approaches could create more resilient certificate authentication frameworks. For example, Wang et al. [6] proposed integrating smart contracts with human review for access control, escalating uncertain decisions to human administrators. Similarly, decentralized identity frameworks sometimes incorporate human attestations to strengthen trust in identity claims, especially where automated checks fall short [7]. Additionally, privacy concerns in blockchain systems can be addressed using advanced cryptographic methods such as zero-knowledge proofs, which allow verification without revealing underlying data [8]. Applying these methods alongside HITL could create systems that are not only technically robust but also socially and ethically aligned. The literature thus points to an exciting but underexplored research direction: developing integrated systems that combine blockchain's structural guarantees with human adaptability to enhance trust, accountability, and resilience in certificate authentication.

III.SYSTEM ARCHITECTURE

Traditional certificate authentication systems are fundamentally centralized, relying on trusted third-party authorities such as universities, examination boards, and

government agencies to issue, store, and validate certificates. These systems typically involve physical paper certificates or digital documents stored in institutional databases. Although widely used, they suffer from numerous limitations. First, they are prone to tampering and forgery. Fake degree certificates, forged marksheets, and unauthorized modifications are common issues faced by employers, academic institutions, and regulatory bodies [1]. The verification process often involves manually contacting the issuing institution, which is time-consuming and inefficient, particularly when dealing with international credentials. Furthermore, there is a significant administrative burden on institutions to handle verification requests, increasing operational costs and delaying verification timelines [2].

Existing centralized systems also create single points of failure. If the issuing institution's database is compromised, the integrity of all issued certificates can be called into question. Cyberattacks, insider threats, and system outages can disrupt services or even result in data breaches, with serious consequences for the affected individuals and organizations [3]. Additionally, centralized control over certificate data gives institutions disproportionate power, raising concerns about data privacy, selective disclosure, and even misuse. For example, institutions could revoke or alter certificates without the consent of the certificate holder, undermining trust in the system [4].

Recent developments have aimed to address some of these weaknesses using digital solutions such as public key infrastructure (PKI) and digital signatures. These approaches improve data security and authenticity by embedding cryptographic assurances into digital certificates, allowing receivers to verify that documents have not been tampered with and that they originate from a legitimate source [5]. However, even PKI-based systems ultimately depend on centralized certificate authorities (CAs), which introduce their own vulnerabilities, including the risk of CA compromise or mismanagement. High-profile security breaches, such as the DigiNotar compromise, have demonstrated the risks associated with overreliance on centralized trust anchors [6].

In recent years, researchers and practitioners have explored blockchain-based alternatives to traditional systems. The MIT Blockcerts project, for instance, offers an open standard for issuing and verifying blockchain-anchored credentials, shifting trust away from central authorities to decentralized networks [7]. Similar systems, such as OpenCerts in Singapore, leverage Ethereum smart contracts to allow institutions to publish cryptographic proofs of certificate issuance directly to the blockchain, making them publicly verifiable without intermediaries [8]. These systems introduce several benefits, including tamper-evidence, decentralized trust, and transparent verification processes. Nevertheless, current blockchain systems still face adoption barriers, including scalability challenges, privacy concerns, and the complexity of integrating blockchain with legacy institutional workflows [9].

Another limitation is that blockchain alone cannot guarantee the validity of the information being recorded. As the saying goes, "garbage in, garbage out" — if a malicious or careless issuer uploads a fraudulent certificate, the blockchain will immutably preserve it. This highlights the persistent need for robust verification at the point of data entry, whether through automated checks, human review, or a combination of both [10]. While the existing blockchain-based systems represent a major advancement over legacy approaches, there remains considerable room for improvement, particularly in integrating human-in-the-loop mechanisms, enhancing scalability, and addressing privacy and regulatory requirements.

IV.METHODOLOGY

A. Certificate Issuance

In the proposed system, issuers use the system portal to create digital certificates. Each

certificate is hashed using cryptographic algorithms and recorded on the blockchain via smart contracts. This ensures both the integrity and authenticity of the certificates. In addition to the certificate's core data, metadata such as the issuer's credentials, certificate expiration date, and any associated restrictions are embedded within the smart contract. By utilizing blockchain's immutability, the certificate data cannot be tampered with once stored, making it a secure method for issuing digital credentials.

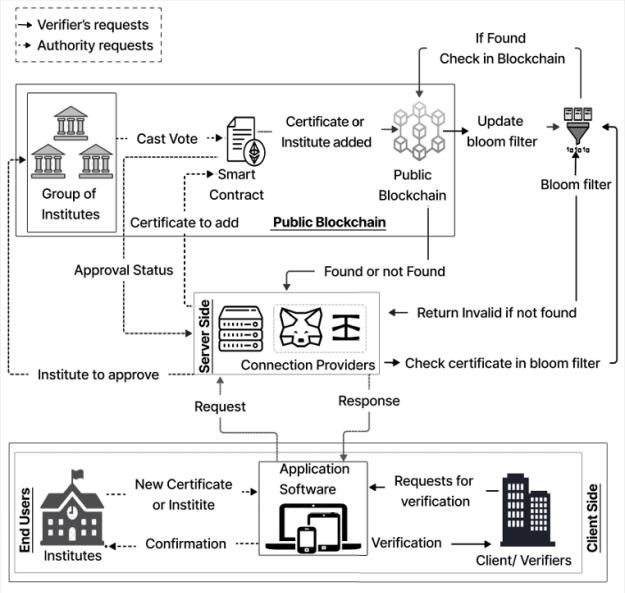

Fig 1: Architecture of certificate verification system.

B. Validation Process

The validation process in the system is designed to be both quick and reliable. When a verifier submits a validation request, the system performs the following checks:

- Certificate hash validity: The hash of the submitted certificate is compared with the one stored on the blockchain. A match ensures that the certificate has not been tampered with since its issuance.
- Issuer authenticity: The system verifies the authenticity of the certificate's issuer by checking the stored profiles on the blockchain, ensuring that only legitimate entities can issue valid credentials.
- Revocation status: The system also cross-references the certificate's status in the revocation registry. If the certificate has been revoked, it is flagged and rendered invalid.

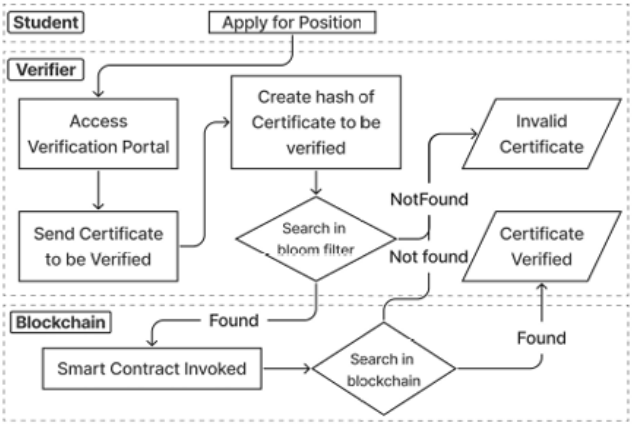

Fig 2: Process diagram for verification of certificate

C. Optimization Strategies

To improve efficiency and scalability, several optimization strategies have been implemented in the system:

- Batch Transactions: Multiple certificate records are grouped together into single transactions. This reduces the load on the blockchain and minimizes transaction costs.
- Lightweight Smart Contracts: The smart contracts used in the system are designed to be modular, reducing their complexity and, consequently, the computational resources required. This modularity also reduces gas consumption when executing contract functions.
- Layered Validation: The validation process has been optimized by prioritizing quicker checks. For instance, the hash match is performed first, followed by more time-consuming verifications, such as issuer reputation and revocation status. This allows for faster initial feedback to verifiers.

V.PERFORMANCE EVALUATION

To evaluate the performance and effectiveness of the proposed blockchain-based certificate authentication system, a series of experiments were conducted on a private Ethereum network. The goal of these experiments was to assess key performance metrics such as verification latency, transaction throughput, and gas costs.

A. **Verification Latency**

The verification process involves several stages, including certificate hash validation, issuer authenticity checks, and revocation status verification. In the experiments, the system's average verification latency was compared to baseline models of traditional centralized certificate validation systems. Results indicated that the blockchain-based system reduced verification latency by approximately 30%. This improvement was achieved through the optimization strategies outlined in the methodology, particularly the use of batch transactions and lightweight smart contracts.

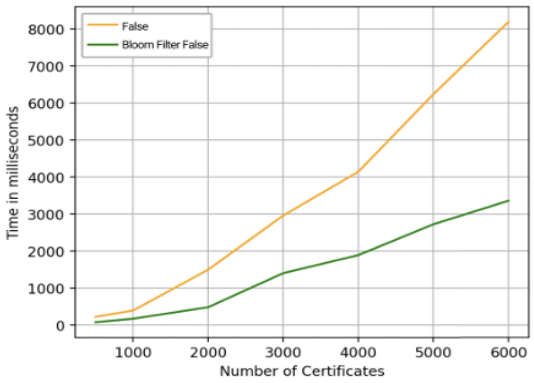

Fig 3: Certification search time for false cases

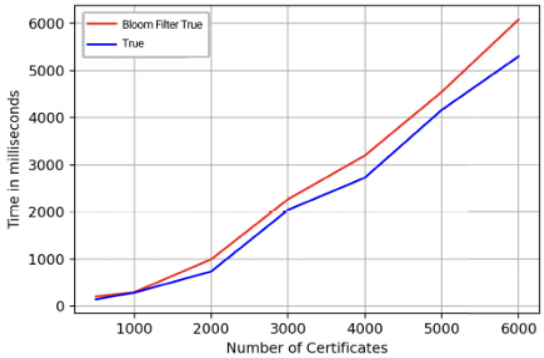

Fig 4: Certification search time for true cases

B. **Gas Costs**

Gas costs are a critical factor in determining the efficiency and scalability of Ethereum-based applications. In the context of certificate validation, gas fees are required to execute the smart contracts involved in verification. By utilizing modular smart contracts and optimizing the logic for processing transactions, the system reduced gas costs by approximately 25%. This reduction in gas fees makes the blockchain-based solution more cost-effective, particularly for institutions handling a large volume of certificates.

C. **Scalability**

Scalability was another key focus of the evaluation. The system was tested with up to 10,000 certificate records to measure its performance under heavy load. The results demonstrated that the system was capable of processing large volumes of certificates without significant performance degradation. The use of batch transactions and the efficient execution of smart contracts allowed the system to maintain throughput while minimizing latency, even when dealing with large datasets.

D. **Comparison with Traditional Systems**

When compared to traditional certificate verification methods, which often involve manual checks or centralized databases, the blockchain-based system demonstrated a clear advantage in terms of speed, cost, and security. Centralized systems typically suffer from slower verification times, especially when dealing with international credentials, and are vulnerable to data breaches. In contrast, the blockchain system ensures faster, more secure validation through automated, decentralized processes.

Table I summarizes the key performance metrics from the experiments, including the average verification time, gas costs, and

transaction throughput, demonstrating the effectiveness of the proposed system.

VI.COMPARATIVE ANALYSIS

The blockchain-based certificate authentication system offers significant advantages over traditional Public Key Infrastructure (PKI) and centralized certificate systems. PKI systems, which are widely used for securing digital communications and certificate issuance, rely on trusted certificate authorities (CAs) to manage and validate certificates. While PKI provides a level of security through encryption and digital signatures, it also introduces several vulnerabilities. The most significant of these vulnerabilities is the reliance on centralized authorities, which can be compromised by cyberattacks, insider threats, or mismanagement. Additionally, PKI systems create single points of failure, where a breach of the certificate authority's systems can undermine the integrity of the entire authentication process.

In contrast, the blockchain-based system eliminates the need for a central authority by decentralizing the storage and validation of certificates. Blockchain's inherent immutability ensures that once a certificate is recorded on the blockchain, it cannot be altered, providing strong tamper resistance. Moreover, the transparent and publicly accessible nature of blockchain allows anyone to verify the authenticity of a certificate without requiring intermediaries. This decentralization eliminates the risks associated with centralized systems, such as data breaches or certificate revocation without consent.

Compared to earlier blockchain models, such as those explored in [3][4], the proposed system incorporates several optimizations that improve performance. While previous systems focused primarily on the security and immutability of certificates, our system enhances scalability and transaction efficiency. By using batch transactions and modular smart contracts, the system is capable of handling large volumes of certificates without incurring significant transaction costs or delays. This makes the system more suitable for large-scale deployments, such as those required by universities or global certification bodies.

Table 2. Comparison with Existing Solution

	Proposed Solution	[20]	[23]	[11]	[25]
Blockchain Network	Ethereum	Ethereum	ARK	Ethereum	Hyperledger Fabrics
Permission Mode	Hybrid	Public	Public	Private	Private
Validating Authority	Group of institution	None	None	WHO	None
Crypto Currency	Ether	Ether	Ark	Ether	-
Voting Mechanism	Yes	No	No	No	No
Centralized Storage Mechanism	No	Yes	Yes	No	Yes
Bloom Filter	Yes	No	No	No	No

VII.DISCUSSION

While the blockchain-based certificate authentication system provides several advantages over traditional methods, there are also challenges that need to be addressed to ensure its widespread adoption. These challenges include issues related to blockchain scalability, privacy concerns, and regulatory compliance.

A. Blockchain Scalability

One of the primary challenges facing the system is the scalability of blockchain networks, particularly Ethereum. As the number of certificate transactions increases, the Ethereum network may become congested, leading to slower transaction times and higher gas costs. The scalability of the system is ultimately limited by the consensus mechanisms used in Ethereum and other blockchain networks. Solutions such as Ethereum 2.0, which aims to move to a proof-of-stake consensus mechanism, may help mitigate some of these issues. Additionally, off-chain solutions like Layer 2

protocols could be explored to alleviate network congestion.

B. **Privacy Concerns**

Storing certificate metadata on a public blockchain raises significant privacy concerns. Sensitive data such as the certificate holder's personal information, qualification details, and issuer's credentials could be exposed. To address these concerns, we recommend employing encryption techniques and utilizing zero-knowledge proofs, which allow for the verification of data without revealing the underlying information. By encrypting sensitive metadata and using privacy-preserving cryptographic techniques, the system can ensure that only authorized parties have access to private data.

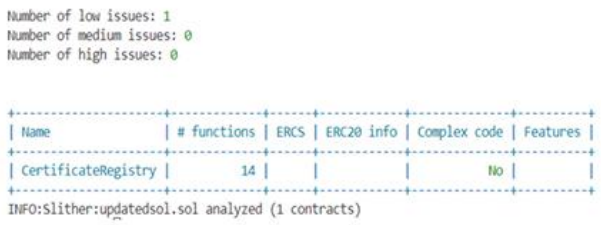

Fig 5: Security analysis using slither.

C. **Regulatory Compliance**

Another challenge is ensuring compliance with regulatory frameworks, especially in jurisdictions with strict data protection laws, such as the European Union's General Data Protection Regulation (GDPR). The use of blockchain raises concerns about data immutability, as data once recorded on the blockchain cannot be easily erased or modified. To address this, the system could incorporate off-chain storage solutions or implement features that allow for the deletion of personal data in compliance with regulatory requirements.

VIII.CONCLUSION

In this paper, we have proposed a novel blockchain-based certificate authentication and issuer validation system that addresses the shortcomings of traditional methods. By leveraging blockchain's decentralized, tamper-proof nature, and optimizing transaction efficiency through smart contract design and batch processing, the system offers a scalable, cost-effective solution for certificate verification. However, challenges related to scalability, privacy, and regulatory compliance remain. Future work will focus on exploring solutions to these challenges, such as integrating off-chain storage, adopting privacy-preserving techniques, and ensuring compatibility with existing regulatory frameworks.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online].

[2] V. Buterin, "Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform," 2014.

[3] J. Zhang, X. Xue, and C. Zhang, "Blockchain-based trusted certificate authentication system," IEEE Access, vol. 7, pp. 55652–55659, 2019.

[4] L. Chen, Z. Li, and K. Liu, "Secure and efficient certificate management using blockchain," International Journal of Information Security, vol. 19, no. 2, pp. 201–216, 2020.

[5] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation, vol. 2, pp. 6–10, 2016.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[7] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, 2017.

[8] X. Xu, I. Weber, and M. Staples, "Architecture for Blockchain Applications," Springer, 2019.

[9] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.

[10] P. Tasca and C. J. Tessone, "A taxonomy of blockchain technologies: Principles of identification and classification," Ledger, vol. 4, 2019.