From Paper to Blockchain: Toward Sustainable Decentralized Identity in E-Government

Miloš Jolović
University of Belgrade
Faculty of Organizational Sciences
Belgrade, Republic of Serbia
milos.jolovic@elab.rs 0009-0003-6580-2039

Daniel Bjelica
University Clinical Center for Radiology
Novi Sad, Republic of Serbia
daniel.bjelica@kcv.rs 0009-0004-3486-9780

Natalija Antonić
University of Belgrade
Faculty of Organizational Sciences
Belgrade, Republic of Serbia
natalijantonic@gmail.com 0009-0005-6009-0647

Talib Tahirović
University of Belgrade
Faculty of Organizational Sciences
Belgrade, Republic of Serbia
talibtahirovic@gmail.com 0009-0004-9515-8237

***Abstract* – In the era of rapid digital innovations and transformations, identity management still remains a largely paper-based and centralized process, which can lead to excessive paperwork, inefficient public administration and serious data privacy and security concerns. This paper aims to present GreenChainID – a digital identity management platform prototype, based on blockchain technology and Self-Sovereign Identity (SSI) principle. The proposed platform prototype is designed to offer citizens several key functionalities such as secure personal data sharing, remote document signing, and anonymous digital petitions voting. Beyond offering citizens to selectively and carefully choose which personal data they are sharing with other stakeholders in both public and private sector, GreenChainID highlights sustainability by cutting resource consumption in public administration, paperwork, and citizen's need for physical presence.**

Keywords – blockchain, decentralized identity, e-government, digital identity management

I. Introduction

Some of the most prominent industries such as finance, healthcare, and education are rapidly adopting digital solutions. These sectors handle, distribute and preserve most of their data digitally. In contrast, identity management and confirmation still lie in centralized, paper-based processes. Most public services demand that citizens present their ID cards or other personal documents and data physically. These processes often lead to excessive and slow bureaucratic workloads, inefficiencies and restrictions on remote data access. Moreover, centralized storage of large volumes of personal data often raises significant concerns about data privacy, security and potential misuse.

Blockchain technology offers solid foundations for addressing potential problems and limitations in regards of data security and privacy by offering transparent processes, data immutability, and decentralized data storage. Blockchain also introduces the concept of Self-Sovereign Identity – a concept that is a paradigm shift. SSI enables individuals to generate and control their own digital identity, through standards of Decentralized Identifiers (DID) and Verifiable Credentials (VC) and Zero-Knowledge Proofs (ZKP) individuals can choose to selectively disclose their personal, sensitive data. These standards promote digital transaction trust, data security and privacy, and autonomy of an individual in digital interactions.

The "green" dimension of digital identity and decentralization of e-government is noteworthy – by reducing reliance of paperwork, minimizing the in-person verification, and streamlining bureaucratic procedures, decentralized digital identity platforms lower resource consumption and align digital innovation with environmental responsibility.

This paper introduces GreenChainID – a digital identity management platform, based on blockchain technology. GreenChainID aims to enable its individual user secure disclosing of personal data, remote document signing, and anonymous digital voting. By combining digital innovation, sustainability and social benefit principle, this platform prototype seeks to explore the potential for implementing decentralized, citizen-oriented e-government solutions.

II. Literature Overview

A. Blockchain in digital governance

Blockchain is a technology initially developed as a backbone to cryptocurrencies but has rapidly evolved into a general-purpose digital innovation and infrastructure that has a high potential in public governance. Traditionally, public governance and identity management are a paper-based processes which can lead to extreme volumes of data being clustered in one, centralized data storage, which leads to inefficiencies, data silos, and vulnerabilities to fraud and data tampering. Blockchain offers tamperproof, transparent and interoperable records. Practical implementations across the world demonstrate blockchain's value in digital governance. Estonia's usage of blockchain Keyless Signature Infrastructure (KSI) secures health and several other government records against manipulation, ensuring full traceability of changes. Similarly, Sweden and Georgia pioneered blockchain-based land registries, significantly reducing transaction times and costs in property transfers. However, blockchain-based infrastructure for digital governance is not without its challenges. Scalability and cost-efficiency, along with interoperability have proven to be

challenging as integrating blockchain with existing governmental digital systems and services can be a complex task [1] [2] [3] [4].

B. Digital Identity and Self-Sovereign Identity (SSI)

In traditional digital identity systems, like Facebook or Google centralized models manage user's credentials with an option of federated identity which enables single sign-on across multiple services, but with a heavy reliance on intermediaries. On the contrast, Self-Sovereign Identity (SSI) shifts control to the individual user, enabling them to be a sole owner and manager of their identity data. Key standards to SSI approach involve Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), which facilitate secure, privacy-preserving identity solutions without central authorities. VCs can be defined as cryptographically signed attestations about the user's identity attributes that can be partially shared with other stakeholders (e.g. service providers). DIDs are globally unique identifiers, created and controlled by the user without relying on any central authority. These technologies enable secure, decentralized and interoperable identity solutions, fully aligning with W3C standards which promote user autonomy and data integrity [5] [6] [7].

C. Zero-Knowledge Proofs and Privacy

Zerko-Knowledge Proofs (ZKPs) stand for several cryptographic methods that allow one party to prove to another that a certain statement is true without revealing any information beyond the validity of the statement itself. In the context of e-government, ZKPs can enhance data privacy by allowing individuals to prove some aspects of their identity without disclosing sensitive personal information for instance, a person can disclose an age maturity without revealing an exact birth date. More specifically, ZKPs can find usage in anonymous electronic voting by enabling voters to prove that their vote was counted correctly without revealing their specific vote choice [8] [9] [10] [11].

D. Green and Sustainable Aspects of blockchain

The energy demand of blockchain networks has been widely questioned and criticized, with several authors showing that networks such as Bitcoin consume electricity compared to the energy consumption of several small nations. Alternative blockchain solution to this arising carbon footprint problem of traditional (e.g. Proof-of-Work blockchains) is a blockchain based on Proof-of-Stake (PoS) consensus mechanisms that reduce energy consumption significantly. Instead of solving complex cryptographic puzzles through mining, PoS selects validators to create a new block based on the amount of a resource (e.g. some cryptocurrency) they "stage" as collateral. This eliminates the need for energy demanding computations and still ensures network security and fairness.

Quantitative research shows that PoS blockchains are up to three times more energy-efficient than PoW systems. Platforms such as Algorand, Tezos, Ethereum 2.0, Polkadot and Hedera demonstrate reasonable energy consumptions per transaction compared to traditional PoW networks.

When applied in e-government, sustainable PoS blockchain systems not only reduce technical energy costs for their upkeep, but also replace paper-based processes, minimize in-person visits to administrative offices, and cut bureaucratic workloads, thus lowering carbon footprint of public administration even further [12] [13] [14] [15].

III. GreenChainID platform prototype

A. Platform prototype architecture

The proposed GreenChainID platform prototype is formed as a decentralized application (dApp) consisting of three fundamental layers:

- Frontend (Client-side): Built with Next.js and TypeScript, providing a responsive, dynamic interface.
- Smart Contract (Backend-side): Written in Solidity and deployed on Sepolia Ethereum testnet.
- Blockchain Interaction: Uses Wagmi and Viem libraries to bridge the frontend with smart contracts on backend side. All state-changing operations (submit/approve/reject a specific citizen's request on the platform) are blockchain transactions.

B. Examples of platform's architecture depending on different system roles

In the ecosystem of GreenChainID platform, citizens (users) are at the center of the system, managing their digital identity through an SSI (Self-Sovereign Identity) wallet. Users can create, store, and selectively share verifiable digital identity data (Verifiable Credentials), such as an ID card, proof of address, proof of age, or citizenship—without revealing more information than necessary.

Public institutions (e.g., Ministry of Interior, municipalities) act as verifiers and issuers of this data. They guarantee the accuracy of the information but do not store it centrally, each user owns and manages their personal data independently.

Citizens use the application for various processes, including electronic voting in local elections and referendums. By utilizing Zero-Knowledge Proofs (ZKP), they can prove their right to vote (e.g., age, residency in a specific municipality) without revealing additional information, thus preserving privacy.

Legal entities (banks, telecoms, crypto exchanges) use the system for KYC (Know Your Customer) checks. Instead of collecting and storing personal data, they request ZKP proofs demonstrating that a user meets specific criteria (e.g., is of legal age, resides at a certain address, holds a valid document), without disclosing their identity.

C. GreenChainID core functionalities

The dApp provides the following core functionalities:

- User role Assignment: Upon connecting a wallet, users are identified as either Citizens or Issuers based on on-chain role recognition.
- Identity Request Submission: Citizens submit personal details (e.g. full name, date of birth, citizenship) to request a digital ID

- Request Review Workflow: Issuers can view and manage pending ID requests directly from the dApp interface.
- Approval/Rejection Process: Issuers have the authority to approve or reject requests; the results are permanently recorded on blockchain.
- Digital Identity Management: Upon approval, a verified identity entry is created and stored on the blockchain, accessible via the user's wallet.
- Role-Based Interface: The dApp dynamically loads different UI components depending on the user's role, ensuring a tailored experience.

D. Example workflow of a transaction

A key transaction within the GreenChainID dApp is the approval of a digital identity request by an authorized issuer. This action is executed as a blockchain transaction and permanently recorded on the network, ensuring transparency and auditability.

Example Transaction: Approving an ID Request

An issuer approves a citizen's request for a digital identity, triggering a state change in the smart contract and issuing an identity on-chain. The process begins when the issuer connects their MetaMask wallet to the decentralized application (dApp) through RainbowKit. The application verifies that the connected wallet address matches the issuer's address defined in the smart contract. Once connected, the issuer navigates to the request management interface, where the IssuerRequests.tsx component retrieves a list of pending requests by calling the smart contract's getPendingRequests() function using Wagmi's useScaffoldReadContract hook. This list is then displayed for the issuer to review.

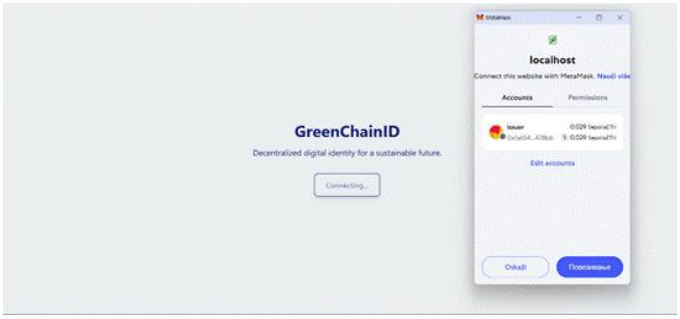

Fig 1. Connecting MetaMask to GreenChainID to gain access to the app's homepage

When the issuer selects a specific request, the application presents the submitted details from the citizen, such as their full name and date of birth. To approve the request, the issuer clicks an "Approve" button in the user interface, which triggers a call to the approveRequest function on the smart contract, passing the request ID and a specified expiry date. This transaction is initiated using Wagmi's useScaffoldWriteContract hook.

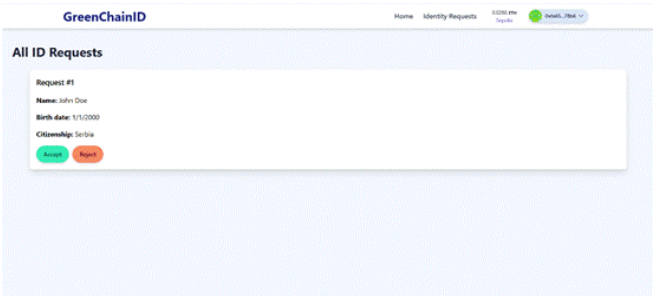

Fig. 2 Issuer's page for approving requests

MetaMask then prompts the issuer to confirm the transaction, displaying the contract address, the function being called (approveRequest), and an estimated gas fee. Upon confirmation, MetaMask signs and submits the transaction to the Sepolia Ethereum testnet. The smart contract processes the transaction by verifying that the caller is the authorized issuer, ensuring the request status is still pending, updating the request to "Approved," and creating a new identity record linked to the citizen's wallet address. Two events are emitted during this process: RequestApproved and IdentityCreated.

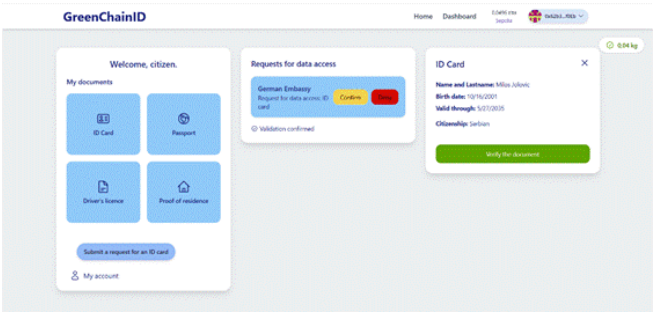

Fig. 3 Citizen's dashboard for document viewing

On the frontend-side, the application listens to these events or periodically polls the contract for updates. Once the transaction is confirmed, the interface reflects the changes: the request is removed from the issuer's pending list, and the citizen can now view their digital identity on their dashboard. This entire process occurs on the Sepolia testnet, with the issuer paying the gas fee in testnet ETH. All interactions and transaction data are publicly visible on the Sepolia block explorer, ensuring transparency and traceability.

IV. Discussion and Conclusion

The analysis of blockchain-based digital identity platforms demonstrates that decentralization can address long-standing challenges regarding the public administration and e-government. Shifting from centralized and paper-based identity verification to SSI model built upon DIDs and ZKPs, individuals gain greater control over their personal information while institutions reduce administrative workloads and risks regarding data privacy and security. GreenChainID platform prototype illustrates how decentralized principle can be operationalized in practice offering digital identity solutions for individual citizens and other stakeholders.

A central discussion point still remains sustainability. Traditional blockchain networks have concerning volumes of

energy consumption, but recent studies confirm that Proof-of-Stake based blockchains have greater efficiency. When PoS based blockchains are combined with reduced reliance on physical documents and fewer in-person visits to administrative offices, digital decentralized identity solutions contribute not only to secure and transparent public services but also to environmentally responsible and sustainable public infrastructure.

However, several challenges remain. Regulatory alignment with frameworks such as GDPR and eIDAS, integration with legacy systems, and digital literacy among citizens represent critical barriers. Furthermore, public trust must be achieved through pilot projects, institutional collaboration, and transparent public service mechanisms.

In conclusion, decentralized digital identity platforms hold the potential to transform e-government into a citizen-centered, secure, and sustainable ecosystem. GreenChainID is a pilot project that aims to question readiness for decentralized digital identity platforms, but its broader development and adoption depend on regulatory readiness, technological scalability, and societal acceptance. Future work should focus on empirical evaluations of pilot implementations and cross-national standardization to ensure interoperability and trustworthiness.

REFERENCES

[1] J. Berryhill, T. Bourgery, and A. Hanson, "Blockchains unchained: Blockchain technology and its use in the public sector," 2018.

[2] E. Tan, S. Mahula, and J. Crompvoets, "Blockchain governance in the public sector: A conceptual framework for public management," *Gov Inf Q*, vol. 39, no. 1, p. 101625, Jan. 2022, doi: 10.1016/J.GIQ.2021.101625.

[3] S. Cheng, M. Daub, A. Domeyer, and M. Lundqvist, "Using blockchain to improve data management in the public sector," *URL: https://www. mckinsey. com/business-functions/mckinseydigital/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector(дата обращения: 31.03. 2021)*, 2017.

[4] P. Bustamante *et al.*, "Government by Code? Blockchain Applications to Public Sector Governance," *Frontiers in Blockchain*, vol. 5, p. 869665, Jun. 2022, doi: 10.3389/FBLOC.2022.869665/BIBTEX.

[5] S. Mthethwa, T. Singano, L. Ndlovu, R. Khutlang, D. Shadung, and B. Ngebeni, "Decentralised Digital Identity and Verifiable Credential Tracking and Management System," *International Conference on Electrical, Computer and Energy Technologies, ICECET 2023*, 2023, doi: 10.1109/ICECET58911.2023.10389306.

[6] S. Cucko and M. Turkanovic, "A Novel Model for Authority and Access Delegation Utilizing Self-Sovereign Identity and Verifiable Credentials," *IEEE Access*, vol. 13, pp. 115102–115134, 2025, doi: 10.1109/ACCESS.2025.3582312.

[7] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials," *2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020*, pp. 71–78, Sep. 2020, doi: 10.1109/BRAINS49436.2020.9223292.

[8] A. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, and P. Sharma, "Privacy preserving E-voting cloud system based on ID based encryption," *Peer Peer Netw Appl*, vol. 14, no. 4, pp. 2399–2409, Jul. 2021, doi: 10.1007/S12083-020-00977-4/METRICS.

[9] Z. Xu and S. Cao, "Efficient Privacy-Preserving Electronic Voting Scheme Based on Blockchain," *Proceedings - 2020 IEEE International Conference on Smart Internet of Things, SmartIoT 2020*, pp. 190–196, Aug. 2020, doi: 10.1109/SMARTIOT49966.2020.00036.

[10] A. Alshehri, M. Baza, G. Srivastava, W. Rajeh, M. Alrowaily, and M. Almusali, "Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain," *Applied Sciences 2023, Vol. 13, Page 1096*, vol. 13, no. 2, p. 1096, Jan. 2023, doi: 10.3390/APP13021096.

[11] Y. X. Kho, S. H. Heng, and J. J. Chin, "A Review of Cryptographic Electronic Voting," *Symmetry 2022, Vol. 14, Page 858*, vol. 14, no. 5, p. 858, Apr. 2022, doi: 10.3390/SYM14050858.

[12] D. G. Baur and J. R. Karlsen, "Do crypto investors care about energy use and climate change? Evidence from Ethereum's transition to proof-of-stake," *J Environ Manage*, vol. 369, p. 122299, Oct. 2024, doi: 10.1016/J.JENVMAN.2024.122299.

[13] S. Yan, "Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake," *Proceedings - 2022 International Conference on Data Analytics, Computing and Artificial Intelligence, ICDACAI 2022*, pp. 464–467, 2022, doi: 10.1109/ICDACAI57211.2022.00098.

[14] J. I. Ibañez and F. Rua, "The energy consumption of Proof-of-Stake systems: Replication and expansion," *SSRN Electronic Journal*, Jan. 2023, doi: 10.2139/ssrn.4324137.

[15] M. Platt *et al.*, "The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work," *Proceedings - 2021 21st International Conference on Software Quality, Reliability and Security Companion, QRS-C 2021*, pp. 1135–1144, 2021, doi: 10.1109/QRS-C55045.2021.00168.