International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey on Decentralized Privacy for Personal Data and Digital Identity Management using Blockchain

[1]R. Suresh, [2]P. Anupriya, [3]Manyam Sri Hari Priya, [4]A. Priyadharshini

[1]Assistant Professor, Sri Manakula Vinayagar Engineering College, Puducherry, India
[2,3,4] Student, Sri Manakula Vinayagar Engineering College, Puducherry, India.

ABSTRACT—

Ensuring even people, services, and the security of communications between devices entities represent a significant danger in the digital revolution. Pursuing the service provider's targeted solution is unnecessary in terms of duplication, has major security flaws, and is inconvenient for users. The concept of self-sovereign identity, comprising the verified qualities of people and a unified digital identity, enables data users to claim ownership and gain knowledge from the use of their data. To ensure the privacy and security of distributed digital identities, digital identities must first be authenticated and authenticated. The key ideas of self-sovereign identity, and the elements of identity proof and authentication Solutions for various self-sovereign identity systems, are consistently presented in this work.

I. INTRODUCTION

One of the biggest problems in the modern world is identity management. Due to the continuous advancements in technology, especially the development of 5G and the Internet of Things (IoT) , the number of entities in the digital world has increased significantly. Therefore, the need for valid and interoperable (or ideally global) digital identities is not just for individuals, but also for organizations, services, applications, and gadgets. Under International Privacy Rules such as General Data Protection Regulation (GDPR). Data breaches and identity theft, such as stealing credentials or trusting credit card information. New identity management techniques in this context. These vulnerabilities have been identified and published by various organizations such as NIST,

GitHub Advisory, and mitre. These vulnerabilities are accompanied by information to facilitate intensive patching. It is important to look at real needs-based solutions. Blockchain-based identity management solutions have been offered as a potential option to meet these needs. Identity management solutions based on the blockchain are still in their infancy, although they are attracting widespread interest in both academia and industry. A large number of standards already exist (keys, certificates, roles, rights, claims, groups, attributes, etc.) to express information about identity/authentication and authorization/rights of access. These specifications vary widely in complexity and capabilities, and they were created for various purposes. IAM products are diverse and easy to implement. one-time passwords, fingerprint and face scan biometric credentials, and multi-factor authentication have all benefited from the widespread adoption of mobile devices such as smartphones. However, new ideas are still needed, such as sovereign identity and self-service identity in machine-to-machine systems, and additional capabilities, such as issuing and authenticating Vendor Independent Claims. Therefore, we are working on an identity management solution based on blockchain-. The purpose of this article is to summarize the current state of the topic and help readers understand the advantages and disadvantages of applying such solutions Furthermore, as the main contribution of this study, we analyze the ten most popular implementations with a focus on privacy and security issues

II. Related Study and literature review

A survey of Blockchain Technology for IAM and

Authentication is provided in [1] by Lim et al. Despite the fact that they discuss some of the services examined in this survey, they do not examine the support for IAM standards and protocols. The most promising options, like Civic, are not present.

By using a decision model to analyze uPort, Sovrin, and ShoCard, Gruneretal. [2] investing at testis Unlike our work, they limited their analysis to a small number of participants and they did not include application integration and enterprise-level interfaces as important evaluation factors. Jacobovitz [3]. strong competitors like sovrin , and several of the other competitors mentioned, such as BlockAuth and Cryptid, subsequently went out of business. Unlike our work, the integration problem and MFA are not evaluated." A Survey of Blockchain Confidentiality and Privacy-Preserving Technologies" by Yang et al [4] was created at in December 2016. Although the survey does not include R3's 4,444 Corda DLT solutions, the authors have included 4,444 companies. The study also does not mention other well-known products, such as uPort or Sovrin Muhletal. Investigate what they consider to be the key elements of the self-sovereign identity solution in [5]. However, their research doe s no the existing Enterprise-grade systems using defined interfaces and protocols are built.

Using zero-knowledge proofs, Stokkink and Pouwelse develop a "generic provable claim model" in [6]. Their work, which aims to provide the Netherlands a self-sovereign identity, was a part of a government-run trial in 2018 [7]. How the work interfaces with currently used IT applications is not, however, demonstrated.

Augot et al. describe a user-centered approach for verified identities on the Bitcoin blockchain in [8] and [9]. The list a few , the blockchain-based strategy was connected, but the strategy was not analyzed in depth.

Although it lacks DLT or a blockchain, Schanzenbach et al. describe a prototype implementation of a system for selfsovereign IDs in [10]. The authors demonstrate how their approach may participate in an existing standard (in this case, OpenID Connect), unlike most self-sovereign identification alternatives.

The specification and implementation of a decentralised storage option for biometric credentials, carried out using blockchains and DIDs within the IEEE 2410-2017 BOPS, are described by Othman and Callahan in [11]. (Biometric Open Protocol Standard).

ISAEN is a standard for human self-sovereign identities that Der et al. describe in [12], although ISAEN is Not used at the moment. Guggenmos et al. discuss in [13], the "platformization" of digital identities based on blockchain, but never evaluate a product or a solution, and never make a setting establishing standards for evaluation. Al-Bassam offers a suggestion in [14]. PKI based on smart contracts (to address issues with conventional CAs), but there is no further action beyond a CA PoC implementation or final user product.

Different types of Identity Management Resultants

Self-Sovereign Identity (SSI) No need for third parties, or users to own, control, and manage their own Self-Sovereign Identity (SSI) [16]. The general functionality of any SSI solution is as follows. Users create their personas online. In standard blockchain processes, users add these identities to the blockchain, linked to encrypted public keys. anyone to challenge and confirm the validity of the user.

Decentralized Trusted Identity (DTI) uses services to authenticate users and register their digital identities on the blockchain [16]. The presence of an external authority is required to authenticate the user's identity, relying on generally trusted mechanisms or national (international) identifiers such as passports. Similar to SSI, additional identifying features can be further tied to digital identities.

Namecoin The launch of Namecoin marks the beginning of 's use of the blockchain in identity management systems. The oldest Bitcoin fork, Namecoin, connects IP addresses and human-readable names in the manner of the Domain Name System (DNS) [16]. Because of this, Namecoin is actually a naming system rather than an identity management system, although we still use terminology. Namecoin has been shown to be vulnerable to a 51% attack on the blockchain and has recently been shown to allow competitors to take over any. Bit domain

Blockstack The Blockstack Namecoin extension is Blockstack[16], an open-source solution. Blockstack provides a new addition as is potentially subject to a Namecoin 51% attack, allowing to be migrated to another blockchain in the event of a major attack. This can be achieved by creating levels, the first of which is the actual blockchain. Unlike Namecoin, it uses public cryptography to protect user data with encryption, giving them more control.

uPort An open-source identity management system called uPort [16] claims that it can provide users with self-sovereign identities registered on the Ethereum blockchain via a mobile app. In addition, uPorts are illiquid, as only internal identities are able to vouch for claims made by other uPort identities.

Sovrin17 recommends that users use unique identifiers for each relationship. So even if the relationship is compromised and the identifier is leaked, users can still communicate normally in other connections.

DAML20 Participating nodes in the DAML registry [16] can identify themselves using the human-readable string as their identifier. In the real world, an entity can have different identities, represented by different identifiers in the same ledger network.

S.NO	TITLE	AUTHOR	YEAR	TECHNIQUE
1.	Interoperable Blockchain Solution For Digital Identity Management	Sudeep Choudhari, Suman Kumar Das, Shubham Parashe	2021	The dApps was created where the identity management was carried out in Hyperledger Indy and its combined with logical smart contracts based blockchain platforms like Quorum[1].
2.	On the relevance of blockchain in identity management	Andreas Gruner, Alexander Muhle, Christoph Meinel	2018	They examine uPort, Sovrin and ShoCard,[2] as representatives for distinct implementation strategies of identity projects.

3.	Blockchain for Identity Management	Jacobovitz	2020	Sovereign and decentralized identities have been created to counter the perceived limitations of centralized, conventional I AM systems.[3]
4.	Deployment of a blockchain-based self sovereign identity	Stokkink and Pouwelse	2018	Self Sovereign Identity model leans on the properties of personalized blockchain structures like Trust Chain or The Tangle. [4]
5.	Self-Sovereign Identities using Name Systems and Attribute-Based Encryption	Schanzenbach et al	2018	By a practical implementation of reclaim ID based on the name system GNS, we have shown that the approach is valid and achieves the functional requirements of an identity mana gement System [5].
6.	Challenges and Opportunities of Block chainbased Platformization of Digital Identities in the Public Sector	F. Guggenmos, J. Lockl, A. Rieger, and G. Fridgen	2018	Introduction of blockchain, digital identities, and platformization of digital identities.[6]
7.	SCPKI: A smart contract based PKI and identity system	M. Al-Bassam	2017	The system process consists of four phases: request, clearing, auditing and appeal, and verification[7]
8.	A First Look at Identity Management Schemes on the Blockchain	P. DUNPHY	2018	We focus on three particular DLT-based IdM schemes: uPort, ShoCard, and Sovrin[8]
9.	Self sovereign Identity - Opportunities and challenges for the Digital Revolution	Uwe Der, Stefan Jähnichen2, Jan Sürmeli	2017	The "platformization" of digital identities based on blockchain[9], but never evaluate a product or a solution, and never make a setting establishing standards for evaluation.
10.	Identity Management on Blockchain– Privacy and Security Aspects	Andreea-Elena PANAIT, Ruxandra F. OLIMID, Alin STEFANESCU	2019	Discusses identity [10] management on blockchain

III. FRAMEWORK

A. The strategy of managing Identities

1. The creation and maintenance of user accounts used by online services for identification and authentication is called Identity Management. The process of setting up users should be simpler to ensure that only authorized users can use the service. A life cycle of an identity management system, called an IdM, or IdM, consists of four stages: registration, verification, issuance and verification. Authentication Provider, Attribute Provider, Service Provider, and Identity Provider are actors that participate in the registration period lifecycle. In our view, we provide three types of 'IDM below, with or without DLT. 1)Silo Model: Using their own authentication system, the central service provider continues to hold onto the credentials and verifies them for access to the web services [5]. Through identification data stored in the DLT layer, central authority and subsequent validation are processed in DLT.

2. Federated model: A central hub for many Web-based service providers serves as an identity provider, which is in charge of establishing, managing, and authenticating all users [6]. The user can sign up for service provider service A and use the same identity to access service b or any other services that are said to be available using the same identity. Examples of federated entities include Facebook and Google's single sign-on systems.

3. Self-Sovereign Identity: To encourage user autonomy and transparency, the self-sovereign Identity gives users ownership of their data. The owner of the data can control the information based on the need-to-know and need-to-retain requirements without relying on third parties which could lead to data loss or misuse of sensitive information.

With rules, privacy-by-design technologies, data portability, and security, the u rights boosted transparency. Due to the current identity crisis, the significance of self-sovereign-based Identity systems has increased dramatically. The comprehensive taxonomy of self-sovereign Identity attributes is shown in Figure 1. We have offered our own analysis of the **taxonomy** found in [7]. The author developed a taxonomy of self-sovereignty that was divided into taxonomies for foundational characteristics, controllability characteristics, sustainability characteristics, security characteristics, and flexibility characteristics.

DIGITAL IDENTITY AND BLOCKCHAIN

Physical entities such as people, gadgets, or organizations are represented by digital identities [3]. Digital world. Since only part of the real identity is composed of digital information, the digital identity is incomplete. It varies according to the specific domains it uses and consists of attributes related to digital identity. A single entity can have multiple digital identities, each used in different contexts and for different purposes. Although, the numbers. Different entities must not have two identical identifiers which indicate that identifiers must be unique. As a result, is not recognized. Examples of characteristics of a digital identity include physical personal characteristics, and contact information (phone, email, and address). The elements of a digital identity [13] include things such as an individual's physical characteristics, addresses, e-mail addresses, and telephone numbers. Some of these s can evolve over time, as can the characteristic of true identity. Technically, other identification methods include credentials (username and password), security tokens, or transaction history. On the other hand, single-use IDs or pseudonyms that were developed expressly for different reasons or certain periods of time can likewise be used to uniquely identify individuals. An end-user (the actual entity with a digital identity who wants to perform an action), an identity provider (the entity that enrolls new users, manages digital entities, and performs authentication), and a service provider (or relying party, the entity that provides services to the end-user and relies on the identity provider to verify the identity of the user.

A peer-to-peer network, the blockchain concept was first announced as Bitcoin [8], and it offers transparency by achieving consensus on transactions. The immutability of blockchain technology and the consensus mechanism remove the need for centralized control and seem to be the perfect solution for dispersed environments. The use of blockchain in data-driven architecture can deliver benefits like decentralization, anonymity, audibility, and persistency because data is currently the most valuable asset [9]. The following definitions of blockchain technology's most popular terms:

1. Node and Block: In a peer-to-peer network, a node is a computer that acts as the owner of transactions carried out by a certain user. In the blockchain, a block is an immutable page of a distributed ledger. After a transaction receives approval, a block is added to the blockchain.
2. Consensus: Transactions are processed and validated through a consensus mechanism, which relies on nodes approving decisions. Proof-of-work, proof-of-play, and practical byzantine fault tolerance are common consensus techniques.
3. Scalability: Depending on the mode of access, the solution currently provided provides performance scalability of either the node or the. Node scalability is provided by public blockchains such as Ethereum [10] and Bitcoin, whereas Hyperledger private blockchain [11] provides the scalability
4. Smart Contracts: The third-generation blockchain revolution extends the use of blockchain beyond the management of assets and cryptocurrencies. smart contracts can control complex applications by specifying arbitrary rules. The "gas" cost of Ethereum smart contract functions varies depending on the amount of processing and storage required. The price of gas is paid in ether (a cryptocurrency)
5. Access: The blockchain is divided into three categories according to the consensus. Public or permission less blockchains Provide anonymity but not privacy. However, at the organizational level, the private string and the consortium string are used.

SMART CONTRACTS

Smart contracts, also known as crypto contracts [14] are computer software that, in some cases, directly and automatically regulates the transfer of digital assets between two parties. Similar to typical contracts, smart contracts work with automated execution of contracts. A smart contract is a computer program that functions exactly as it was coded or programmed by its author. smart contracts are enforceable through code, just like traditional law contracts**.**

IV. Features of Blockchain-based Identity Management

Blockchain-based identity management systems leverage the inherent advantages of technology [12]. They transfer the burden of administration and control from the central authority of the system to the users. Hopefully these benefits (to some extent) will help address issues such as identity fraud and data breaches that occur in centralized systems. However, this is problematic because identity governance methods also fail to achieve full decentralization. Or require great confidence. the design of the blockchain provides transparency for data changes, and the historical data cannot be changed in any other way (unless the majority of the nodes agree to change). On the, on the other hand, it raises questions about the effectiveness and even the safety of the implementation. It should be possible to selectively store identities in a blockchain-based identity management solution. The blockchain authority or another blockchain organization must guarantee the identity. This works normally as follows. The organization applies for a verified identity, which is confirmed after verification. Various user characteristics (such as phone numbers, email addresses or official identification documents) (Biometric, credentials) Identities blockchain There is a clear distinction between digital and physical identities in management. An identifier (a value that specifically identifies an entity) and any associated attributes. Since security and privacy breaches result from uncontrolled or unauthorized exposure of functionality, ownership of the functionality, if any, should be handled accordingly according to clearly defined principles.

V. FUTURE WORK

We intend to expand the evaluation criteria to include Machines and Things ID or Internet of Things as part of our ongoing research. Additionally, we also intend to create a new concept of identity based on the blockchain that combines the best of existing features with original ideas. The concept will be built on top of a GDPR- compliant ledger that supports deletion and modification of consensus-based audit data.

VI. CONCLUSION

In this work, we discuss blockchain-based identity management. The adoption of blockchain technology to solve any type of problem should be avoided by carefully considering the advantages and the disadvantages. We have shown the shortcomings of current solutions and the need for further research to solve various problems. The real benefits of blockchain-based identity management relate to the difficulties of use, implementation, and maintenance, which require careful consideration and further research.

VII. REFERENCES

1. S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, “Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey,” International Journal on Advanced Science, Engineering and Information Technology, vol. 8, no. 4-2, pp. 1735–1745, 2020.
2. A.Gruner, A. M uhle, and C. Meinel, “On the relevance of blockchain ¨ in identity management,” 2021.
3. O. Jacobovitz, “Blockchain for Identity Management,” Ben-Gurion University, Beer Sheva, Israel, Tech. Rep., 2020. [Online]. Available: https://www.cs.bgu.ac.il/frankel/TechnicalReports/2020/16-02.pdf
4. Z. W.-O. Danny Yang, Jack Gavigan, “Survey of confidentiality and privacy preserving technologies for blockchains,” R3 Research, Tech. Rep., 2019. [Online]. Available: https://z.cash/static/R3 Confidentiality and Privacy Report.pdf
5. A.Muhle, A. Gr ¨ uner, T. Gayvoronskaya, and C. Meinel, “A Survey ¨ on Essential Components of a Self-Sovereign Identity,” 2018.
6. Q. Stokkink and J. Pouwelse, “Deployment of a blockchain-based self sovereign identity,” 2018.
7. UNOPS, “The Legal Aspects of Blockchain,” UNOPS, Tech. Rep., 2018. [Online]. Available: https://www.blockchainpilots.nl/booksSulley. Available online: https://github.com/OpenRCE/sulley (accessed on 4 April 2018).
8. D. Augot, H. Chabanne, O. Clemot, and W. George, “Transforming ´ face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain,” CoRR, vol. abs/1710.02951, 2017.
9. D. Augot, H. Chabanne, T. Chenevier, W. George, and L. Lambert, “A User-Centric System for Verified Identities on the Bitcoin Blockchain,” CoRR, vol. abs/1710.02019, 2017. [Online]. Available: http://arxiv.org/abs/1710.02019
10. M. Schanzenbach, G. Bramm, and J. Schutte, “reclaimID: Secure, ¨ Self-Sovereign Identities using Name Systems and Attribute-Based Encryption,” CoRR, vol. abs/1805.06253, 2018.
11. A.Othman and J. Callahan, “The Horcrux Protocol: A Method for Decentralized Biometricbased Self sovereign Identity,” CoRR, vol. abs/1711.07127, 2017.
12. U. Der, S. Jahnichen, and J. S ¨ urmeli, “Selfsovereign ¨ Identity - Opportunities and Challenges for the Digital Revolution,” CoRR, vol. abs/1712.01767, 2017. [Online]. Available: http://arxiv.org/abs/1712.01767 20
13. F. Guggenmos, J. Lockl, A. Rieger, and G. Fridgen, “Challenges and Opportunities of Blockchain-based Platformization of Digital Identities in the Public Sector (Research in Progress),” in ., 06 2018.
14. M. Al-Bassam, “SCPKI: A smart contract- based PKI and identity system,” in Proceedings of the ACM Workshop on Blockchain, Cryp tocurrencies and Contracts. ACM, 2017, pp. 35-40.
15. P. DUNPHY, F. A. P. PETITCOLAS, A First Look at Identity Management Schemes on the Blockchain, IEEE Security & Privacy, 16, 4, pp. 20-29, 2018.
16. Andreea-Elena PANAIT, Ruxandra F. OLIMID, Alin STEFANESCU, Identity Management on Blockchain – Privacy and Security Aspects in 2019.