NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 6, ISSUE 5, May-2019

A SYSTEMATIC LITERATURE MAPPING ON SECURE IDENTITY MANAGEMENT USING BLOCKCHAIN TECHNOLOGY

Ishaq Azhar Mohammed
Sr. Data Scientist & Department of Information Technology Dubai, UAE
ishaqazhar14@gmail.com

ABSTRACT
Although a safe exchange of information, services, and technologies are possible via centralized digital organizations, there are significant concerns associated with the digital revolution. Without the users' knowledge or permission, telecommunications companies gather and absorb information that is utilized for data analysis, profiling, and exploiting purposes by third parties [1]. The continuation of service providers' centered solutions is wasteful due to duplication, it has significant security flaws, and it is burdensome for consumers. To accomplish the security and privacy of dispersed digital identities, it is necessary to authenticate and verify the digital individual's identity [1]. Nevertheless, thorough research on the elements of identity management, as well as user data protection and privacy measures in the identity management system, is still lacking in the published studies, according to the researchers [1,2]. Managing and verifying digital identities is undoubtedly among the most important applications of blockchain technology for various developments. Throughout 2018, millions of individuals all around the globe were affected by data breaches involving their personal information. It is necessary to develop more secure methods of storing, exchanging, and validating sensitive material. In this respect, developing blockchain solutions for identification systems may help address some of the issues experienced by most centralized databases.

Keywords: Blockchain, identity theft, IdM solutions, Identity management, Isolated Identity Management model, Centralized IdM

INTRODUCTION
A digital identity is an internet persona that is established by a person in cyberspace and maintained by that person. In the same way as the metadata on a passport distinguishes the ownership for a particular purpose based on details such as an E-mail address, a proxy server, or even some URL [2]. Therefore, because we are progressing towards the usage of digital technology, we need a platform that can identify who is the intended user. In today's world, government programs, customized services, and commercial services apps all save and convert personal information about their users per their requirements. The authentication system on the web is still kept in certain central repositories and controlled by third parties that manipulate user data and delete them without permission [3]. The possibility of identity theft, security theft, and other forms of fraud creates a state of anxiety and necessitates the use of very effective IdM solutions. Digital identity is a very significant and worldwide problem that has to be addressed as quickly as possible. This paper will explore in detail how security identities are mapped into blockchain technologies.

PROBLEM STATEMENT
The main problem that this paper will try to solve is to analyze how secure identity management can be mapped using blockchain technology. According to current statistics, 16.7 million individuals in the United States alone were victims of identity theft in 2017, with total financial losses totaling a whopping $16.8 billion [4]. If people are not familiar with the term, identity theft refers to the unlawful use of another person's personal information for any kind of criminal benefit, most often monetary gain. Various methods, ranging from large-scale data breaches to customized phishing assaults to cruder methods such as credit card theft, are used to carry out the criminal enterprise. The Equifax data breach serves as an excellent illustration of how inadequate data protecting processes may result in the loss of millions of customers' personal information [4]. Identity theft isn't the only way our personal information may be misused or accessed by others. Essentially, the information that we give to different social networking platforms is completely at their discretion and may be distributed to anyone they want.

LITERATURE REVIEW

A. Identity Management and blockchain background

This part provides a high-level overview of identity management, including the models that have been utilized and the difficulties that have been encountered. In the next section, a detailed explanation of blockchain technology, including its many kinds and applications, is presented. Identity and Identity Management have long been a subject of discussion in academia as a new area of investigation. Because of the prevalence of digital identities and the large number of people who use them, identity management has risen to the top of the priority list in this Internet-based age of information. The fact that the majority of the population today has some kind of digital identity is because they spend a significant amount of time on the Internet and utilize the services that are available via the Internet. Traditional identity and access management methods have been intended to be successful for service providers, but ineffective for users, who must remember numerous passwords to access various online sites. A categorization of different IdM methods is provided by, which considers factors such as private information and accessibility of IdM solutions, among other things. At its most fundamental level, IdM is comprised of a network operator and a consumer who may conduct any kind of business without feeling worried about the privacy and security implications of each transaction. By adding an authentication mechanism, it is possible to assist build confidence between the two parties.

B. Identity management models

Scholars have categorized IdM models into 3 groups - Isolated IdM, Federated IdM, and Central IdM - after analyzing the current identity managing model. When using isolated identity management, the identity provider assigns a unique identification to each user to grant them accessibility to the isolated system that they have requested for instance a user name or a password). Because of the variety of internet services available now, isolated IdM has been utilized less often in the modern world.

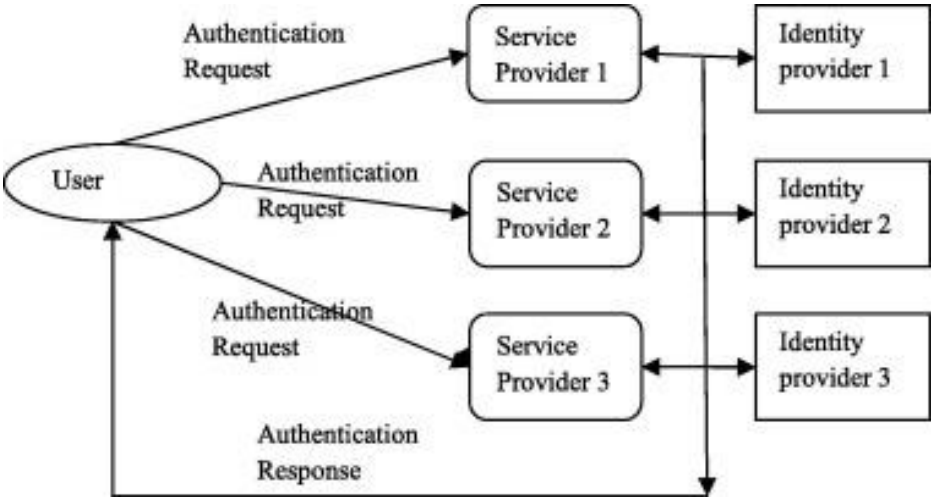

Fig i: Architecture of an Isolated Identity Management model

Federated IdM is comprised of a collection of service providers that establish a set of standards and are responsible for recognizing the users' IDs [7]. Each user who is a member of a group has access to most of the services supplied by all of the providers in its unit, and this includes the offerings by all of the stakeholders in the group. By utilizing a user-centric strategy, an expansion of the pre-established Federated IdM is achieved. A PRIME initiative has developed a special data processing platform [7,8]. The federated service provider differentiates the registration entity and other entities that are authenticated to validate the numerical identification [8]. It is the responsibility of an Identity Provider to manage and authenticate all users, and it also serves as a central hub for a variety of Web-based service providers. The user may register in service provider service A and may access service b utilizing the authentication procedure which verifies the recipient's claim, using the same identity [7]. Federated entities include the single sign-on services provided by Facebook and Google.

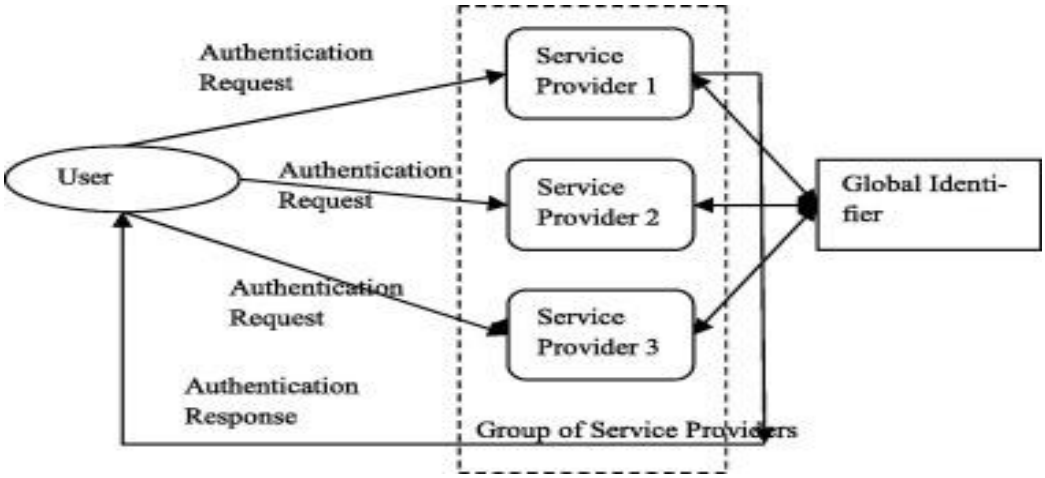

Fig ii: Federated Identity Management model

For centralized identity management, there is a single common identity provider, and every service provider uses the same identification and credential. All services are accessed using the same details by the user. Additional classifications for this paradigm include the meta-identifier model, the Common identifier model, and the Single Sign-On (SSO) model. In this method, the central service provider retains control by gathering and validating the username and password to obtain online services according to their authentication system [8]. Users' identities are verified via a central authority in the DLT-based method, and additional validation is carried out using personal data stored in the DLT layer [9].

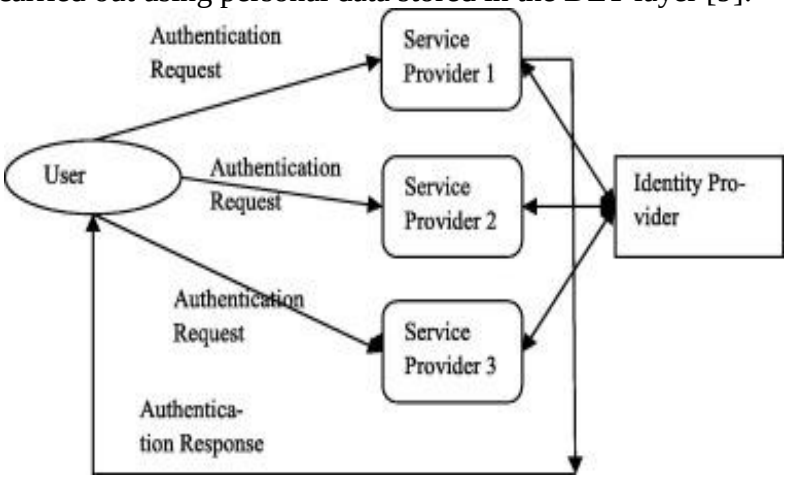

Fig iii: Architecture of centralized IdM model

C. Motivation: Need for Blockchain

To solve digital identification problems, the basic tenets of self-governed identity [15] may be accomplished by using the blockchain. The consensus method meets the requirement for confidence in the characteristics confirmed. Because blockchain is a tamper-resistant database, entries may be kept for a long time. The SSI method is user-centric and requires that the user maintain complete control over their data. The chain structure providing the chain by chain identification, like the trust chain [10] or the tangle [11], is fully controlled. This chain structure may also lay down the concept of existence that allows users to forget about it. This is the assertion Blocking personal data and verifying claims guarantees privacy and data reduction. The blocks may be interoperable and portable with different systems [11].

D. Blockchain for identity and data management

Procedures and guidelines have been established from a security viewpoint and are now on confidential information. Communication agencies are exchanging information in a hazy manner, and it is important to keep a record of what data is being exchanged and what information is being allowed access. The degree to

which personal data may be linked together has an impact on the anonymity of an individual's identity [12]. It is critical to offer selective sharing of PII while also tracking PII to address concerns about personal data privacy. PII is defined as a suitable subset of identifying personal details within a range of topics such as driver's license, address, passenger passports, surname, birth date, etc [12]. Secondly, PPII is a collection of all the elements of full identity, whereby complete identity is the combination of all attributes, such as a bank name, a portion of an email address, a denomination, a partial name, or any other combination of these [13]. As digital identities are segmented into various contexts based on personal information, such as personally identifiable information (PII), prospective personally identifiable information (PII), and non-personally identifiable information (non-PII), In different contexts, the circumstance and the role-play a significant influence in the activation of identity characteristics for identification and user authentication [13]. Based on the OAuth protocol, several companies have created their proprietary authentication mechanisms that are not available to the general public. Data privacy and management are now performed in all parts of the world under the guidance of international standards organizations. Regulation (GDPR) [13,14] is being implemented by the European Union to safeguard customers by restoring ownership of their identifying data to the individuals who own it, thus protecting consumers [13]. In acknowledgment of the requirement for a person to control a digital identity, GDPR-compliant digital rights are combined with the SSI concept of user-centric identity.

E. The Importance of Blockchain Technology in Identity Management

Blockchain technology is renowned for its security. Due to the lack of a centralized location from which cybercriminals may take data, information kept on the blockchain is impenetrable to cyber-attacks that often occur with centralized databases [15]. Aside from that, the blockchain records all transactions that take place between identity holders and businesses, guaranteeing full transparency at all times. Additionally, decentralized digital ledger technology provides individuals with the freedom to establish encrypted user identity, which can be accessed quickly and easily via mobile apps and may be used to authenticate identification as and when necessary. This is safer than carrying conventional identification papers in wallets and purses. It should unsurprising that blockchain technology is being utilized in a range of identity management and authentication solutions across a broad range of industries today, from humanitarian operations to the banking system.

F. User Data Privacy

The disclosure of sensitive information on a person's identity may be detrimental to both the client and the business. Personal identification data should not be linkable to discover identities to guarantee privacy in IdMs (s). The proper use of pseudonyms and permission may aid in the creation of privacy while also improving identity management [16]. Privacy-enhancing techniques such as minimization of personal information are among those available. It guarantees that data is presented for situations where there is a need to know and a need to retain. A variety of methods to safeguard personally identifiable information have been developed as a result of research in the area of data privacy that has focused on data anonymity. The k1-anonymity approach [16] provides a way to connect information and requires that the information set cannot be distinguished from other k-1 personnel files [16,17]. Another set of solutions suggested varied representation and distribution of sensitive data to guarantee safe data exchange and minimization of data exposure in [17] as well as [17]. Other methods, such as troubling data or encrypting information, have also been tried, although they are inefficient when used in large-scale distribution networks. Blockchain technology creates a public, verifiable, open record of transactions that can be accessed by anyone. [17] proposes the use of blockchain technology to provide sensitive information privacy in IdMs. With the usage of the blockchain for public client's personal information of the user being kept securely, the proposed system guarantees data ownership, interoperability, and complete access control. The authentication of PII claims, on the other hand, has not been taken into consideration in this approach. Current blockchain-based technologies have either made use of blockchain access to guarantee privacy, or they have tied authentication to a decentralized identifier (DID) and stored sensitive information on the user's computer or mobile device, respectively.

BITCOIN FUUTRE IN US

Ever since the launch of Bitcoin in 2008, the first decentralized peer-to-peer electronic currency system, blockchain technology has advanced significantly [17]. Today, entrepreneurs across a wide range of industries are beginning to see the advantages of the technology that underpins Bitcoin. Many industries, ranging from medical to banking, are exploring methods to incorporate blockchain technology into their infrastructures. Blockchain technology, under its decentralized and trustless character, has the potential to open up new avenues for company growth while also enhancing transparency, increasing security, and simplifying traceability [18]. Blockchain and finance are just the beginning of what is possible. Banks, when seen from a macroeconomic viewpoint, function as important value storage and transmission hubs. With the ability to perform the same purpose as traditional ledgers while being digitalized, secure, and tamper-proof, blockchains have the potential to significantly improve accuracy and information exchange in the financial services ecosystem. Credit Suisse, for example, has formed a partnership with New York-based startup Paxos to utilize blockchain technology to settle US stock transactions [18]. Meanwhile, JPMorgan Chase has launched the JPM Coin, which it plans to use to simplify transactions between institutional accounts. The JPM Coin is the bank's first foray into the blockchain sector. Other institutions, such as Goldman Sachs and Citigroup, have also conducted blockchain tests.

ECONOMIC BENEFITS

The economic benefits to the United States come in as more users using blockchain technology develop increased confidence in the system. This attracts more customers to do their transactions without worry about losing their confidential information to cybercriminals. More generally, blockchain has the potential to disrupt the $5 trillion+ banking sector by disintermediating the fundamental services that banks offer, ranging from payments to clearing and settlement systems, among other things. Banks make a lot of money facilitating payments – cross-border transactions produced billions in payments income [18]. But blockchain technology provides a safe and inexpensive method to pay, thus eliminating the need for third-party authentication and improving backlogs with a conventional bank transfer. Additionally, the economic advantages of using Blockchain technology may help to improve the economy of the United States by increasing levels of monitoring, tracing, and confidence in transactions. To maximize the effectiveness of cross-border transactions, blockchain startup Ripple has formed partnerships with over 300 clients, comprising banking institutions such as Santander and Western Union. Its current solution enables banks to communicate in real-time through a two-way protocol that enables real-time messaging and settlement. As part of a pilot program, Switzerland's central bank utilized R3's distributed ledger technology to process large transactions among banking firms utilizing digital currency [18].

CONCLUSION

This paper provides an analysis of mapping on secure identity management using blockchain technology. The findings from this analysis show that blockchain-based identity verification guarantees users transparency, security, and ease of use for individuals and organizations. And, although we continue to depend largely on conventional means of identity management, any little step that a cryptocurrency expert makes toward blockchain use is a significant step forward. Cryptocurrency services and vision are built on blockchain technology. As per this paper cited above, the blockchain "serves as a server for transactions and as a process of attaining agreement on the sequence where the transactions were recorded." To be precise, Bitcoin (the system, not the money) is used by cryptocurrency companies as the foundation blockchain, upon which other components of the cryptocurrency infrastructure are constructed. Simply said, blockchain technology allows cryptocurrencies to stay decentralized and safe while still being decentralized.

REFERENCES

1) P. Maresova, S. Tomsone, P. Lameski, J. Madureira, A. Mendes, E. Zdravevski, I. Chorbev, V. Trajkovik, M. Ellen and K. Rodile, "Technological Solutions for Older People with Alzheimer's Disease: Review", Current Alzheimer Research, vol. 15, no. 10, pp. 975-983, 2018.
2) C. Stirling, S. Leggett, B. Lloyd, J. Scott, L. Blizzard, S. Quinn and A. Robinson, "Decision aids for respite service choices by carers of people with dementia: development and pilot RCT", BMC Medical Informatics and Decision Making, vol. 12, no. 1, 2012.
3) W. Moyle, U. Arnautovska, T. Ownsworth and C. Jones, "Potential of telepresence robots to enhance social connectedness in older adults with dementia: an integrative review of feasibility", International Psychogeriatrics, vol. 29, no. 12, pp. 1951-1964, 2017.
4) A. König, L. Francis, J. Joshi, J. Robillard and J. Hoey, "Qualitative study of affective identities in dementia patients for the design of cognitive assistive technologies", Journal of Rehabilitation and Assistive Technologies Engineering, vol. 4, p. 205566831668503, 2017.
5) C. Gessert, S. Forbes and M. Bern-Klug, "Planning End-of-Life Care for Patients with Dementia: Roles of Families and Health Professionals", OMEGA - Journal of Death and Dying, vol. 42, no. 4, pp. 273-291, 2001.
6) M. Gagnon-Roy, A. Bourget, S. Stocco, A. Courchesne, N. Kuhne and V. Provencher, "Assistive Technology Addressing Safety Issues in Dementia: A Scoping Review", American Journal of Occupational Therapy, vol. 71, no. 5, pp. 7105190020p1, 2017.
7) S. Einterz, R. Gilliam, F. Chang Lin, J. McBride and L. Hanson, "Development and Testing of a Decision Aid on Goals of Care for Advanced Dementia", Journal of the American Medical Directors Association, vol. 15, no. 4, pp. 251-255, 2014.
8) A. Bharucha, V. Anand, J. Forlizzi, M. Dew, C. Reynolds, S. Stevens and H. Wactlar, "Intelligent Assistive Technology Applications to Dementia Care: Current Capabilities, Limitations, and Future Challenges", The American Journal of Geriatric Psychiatry, vol. 17, no. 2, pp. 88-104, 2009.
9) M. Begum, R. Huq, R. Wang and A. Mihailidis, "Collaboration of an assistive robot and older adults with dementia", Gerontechnology, vol. 13, no. 4, 2015.
10) A. Mihailidis, G. Fernie and J. Barbenel, "The Use of Artificial Intelligence in the Design of an Intelligent Cognitive Orthosis for People with Dementia", Assistive Technology, vol. 13, no. 1, pp. 23-39, 2001.
11) C. Ollivet, C. Guigui, C. Hervé and V. Rialle, "What Do Family Caregivers of Alzheimer's Disease Patients Desire in Smart Home Technologies?", Methods of Information in Medicine, vol. 47, no. 01, pp. 63-69, 2008.
12) B. Xie, A. Berkley, J. Kwak, K. Fleischmann, J. Champion and K. Koltai, "End-of-life decision making by family caregivers of persons with advanced dementia: A literature review of decision aids", SAGE Open Medicine, vol. 6, p. 205031211877751, 2018.
13) M. Begum, R. Huq, R. Wang and A. Mihailidis, "Collaboration of an assistive robot and older adults with dementia", Gerontechnology, vol. 13, no. 4, 2015.
14) W. Burleson, C. Lozano, V. Ravishankar, J. Lee and D. Mahoney, "An Assistive Technology System that Provides Personalized Dressing Support for People Living with Dementia: Capability Study", JMIR Medical Informatics, vol. 6, no. 2, p. e21, 2018.
15) S. Czarnuch and A. Mihailidis, "The design of intelligent in-home assistive technologies: Assessing the needs of older adults with dementia and their caregivers", Gerontechnology, vol. 10, no. 3, 2011.
16) A. Hwang, K. Truong, J. Cameron, E. Lindqvist, L. Nygård and A. Mihailidis, "Co-Designing Ambient Assisted Living (AAL) Environments: Unravelling the Situated Context of Informal Dementia Care", BioMed Research International, vol. 2015, pp. 1-12, 2015.
17) M. Mueller, D. Wiley, A. Tentler, M. Bocko, L. Chen, A. Leibovici, J. Quinn, A. Shar, A. Pentland and C. Horwitz, "Is Home Health Technology Adequate for Proactive Self-care?", Methods of Information in Medicine, vol. 47, no. 01, pp. 58-62, 2008.
18) S. Chang and H. Sung, "The effectiveness of seal-like robot therapy on mood and social interactions of older adults: a systematic review protocol", JBI Database of Systematic Reviews and Implementation Reports, vol. 11, no. 10, pp. 68-75, 2013.