Estimation of a good fit with Blockchain and Identity and Access Management((IAM)

D.Nancy kirupanithi[1], Dr. A. Antonidoss[2]

[1]Research Scholar, Hindustan Institute of Technology and Science, computer science and Engineering
[2]Associate Professor, Hindustan Institute of Technology and Science, computer science and Engineering

Abstract - *Every time you Login with your Facebook account or Login with Twitter page on a website or use login credentials issued by your employer or school, you're using Identity and Access Management (IAM) technologies in the background. IAM has become central to our online interactions, but like a lot of infrastructure are not known to the users. At least when it's well designed and implemented it is not known. IAM is evolving rapidly, the stakes are high. Enterprises face an increasingly complex and puzzling digital identity landscape. There is also growing concern that businesses know too much about the people. And therefore end users should reclaim their control over their own identities. We provide a balanced perspective, and the ways in which blockchain technologies may or may not serve the needs of IAM.*

Key Words: IAM, Login credentials, digital identity, identity landscape

1. INTRODUCTION

Blockchain technology is also called distributed ledger technology (DLT). It is gaining attention to a greater extent. Proponents advocate it for a wide variety of use cases, including IAM. Blockchain is a broad class of relatively new data security methods, with certain properties of prospective value in IAM. IAM companies have launched identity registration solutions on the blockchain while others are developing new blockchain inspired infrastructure for distributing information about users called attributes and used to inform decisions about whether to grant access to resources, which is a key element of IAM.

To verify how Blockchains have anything to Offer with Identity to provide an in-depth analysis of blockchain and IAM, and to provide a look through which to view and evaluate cooperative developments. A growing amount of hype and skepticism are being faced. And they seek to provide a balanced perspective and to explain the ways in which blockchain technologies may or may not serve the needs of IAM. The starting point should appreciate what the first blockchains were designed to do with cryptocurrency, and then to build carefully on that in answering whether these new and innovative technologies can help with IAM. This paper should help those devising new IAM solutions, and those acquiring solutions and needing to evaluate blockchain-based approaches. Perhaps most importantly, we hope to provide guidance in evaluating current and new blockchain based IAM solutions as they come along. In analysis, it is apparent that blockchain technologies are cooperatively a work in progress.

This paper is wrapping up of the early awareness about their general security properties; on closer assessment we find that the original public blockchains are normally not a good fit for IAM. The intention of bitcoin is that the cryptocurrency is meant to exchange electronic cash without any centralized system and also with trust. It is primarily different from that of enterprise IAM that on average requires more precise key lifecycle management and access controls than public blockchains. Several new blockchain technology developments has shown promise for improving picky aspects of IAM which are listed as the provenance of identity attributes and cryptographic keys. Any ongoing examination of blockchain technologies for IAM begins with a understandable problem statement and an approval of the degree in blockchain security.

1.1 Privacy

There are always some challenges and restrictions in terms of blockchain when combined in role within IAM. Digital identity is closely linked with issues of privacy and data protection, particularly following the data protection regulations such as General Data Protection Regulation (GDPR). The guidance offered in GDPR will ensure that companies have effective data rights management strategies enforced. And even then privacy odds ways with the notion of an immutable ledger distributed to a considerable number of nodes involved. Blockchain to be of genuine value in the IAM space, a consensus algorithm has been built so that identities and private information should not be stored on public blockchain.

1.2 Security

The security of the blockchain which is a centralized network is another challenging obstacle. Distributed security is normally far more difficult to achieve than centralized security. It is mainly because of the broader attack surface. And also cryptographic key security is a foundational element of the blockchain concept. This means that protecting the keys using cryptography which allow access to the ledger. The blockchain applications are a paramount for blockchain solutions as it is helpful to be secure. Protection means not only securing keys as robustly as possible, but also the recovery of lost private keys without introducing an escrow agent. Such a third party would nullify the disintermediation notion of the blockchain. All of these security concerns, then, need to be solved before concepts such as Self Sovereign Identity using blockchain can become genuinely put into mainstream.

2. When IAM Meets the Idea Of Blockchain

It seems the technology market in fig-1 has an emerging champion called Blockchain technology. Blockchain can change the world on everyday working basis. Blockchain may affect the realm of Identity and Access Management which is really interesting. Many IAM architects has similar thought process while shifting through the available information. But this can be a bit confusing as most technical information are relied on Blockchain. It tends to focus on Bitcoin and financial services future to a larger extent. It may be useful to envision and I really mean to visualise how IAM solutions may benefit from ideas adjacent the use of Blockchain technology. We know one of the core IAM disciplines is the domination and management of digital identities, entitlements, and assignment of entitlements to identities within an enterprise environment. This is to ensure identities that can verifiably access resources based on their entitlements. From the governance perspective, that means the right entitlements should be assigned to the right identities. The assignment must be certified periodically by reconciling identity and entitlement data, typically in a central repository.

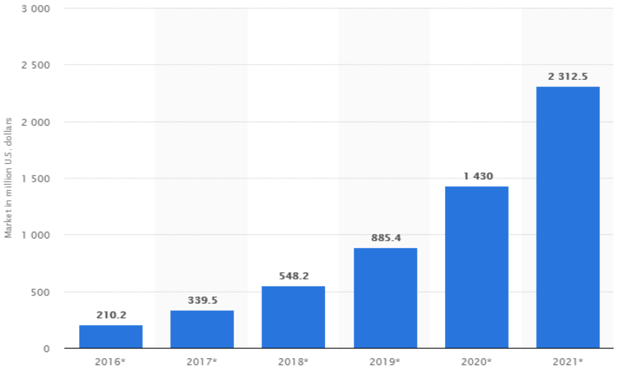

Fig -2: Technology market in Blockchain

Blockchain, in general, is an organizing model for the discovery, transfer, and coordination of all discrete units of anything of value [1]. In this model, Blockchain can track activities related to the unit of value in a tamper-proof and decentralized ledger. Blockchain technology can implement this model by establishing a peer-to-peer network among a set of nodes that each store a copy of the ledger. These nodes ensure the data integrity after adding new records to a block, using a consensus protocol to confirm the validity of the activities and maintain the chain of blocks. The protocol uses a special hashing algorithm to store the data and pointers to external data. This feature of the Blockchain establishes a decentralized governance structure which is theoretically autonomous. Of course, there are many limitations and technical challenges which we leave out for the sake of focusing on the vision. It is possible to envision an IAM-centric Blockchain ecosystem that keeps track of identities, entitlements, entitlement assignment, and access events, all autonomously in a heterogeneous environment. In this model, 'entitlement' is our unit of value (currency) and the registered 'identities' (people or things) are participating in 'access' events (transaction) based on their assigned entitlements. The blockchain ledger is the authoritative registration log for identities, entitlements, and access events that works based on a push model. The consensus protocol among the nodes validates the correct assignment of entitlements to identities and the correct access to resources by validating policies before confirming the assignment. Any change in the assigned entitlements can be thought of as a transaction similar to exchanging coins. Similar to the Bitcoin wallets, our IAM Blockchain can have its clients or plug-in components for just-in-time access to records in the Blockchain.

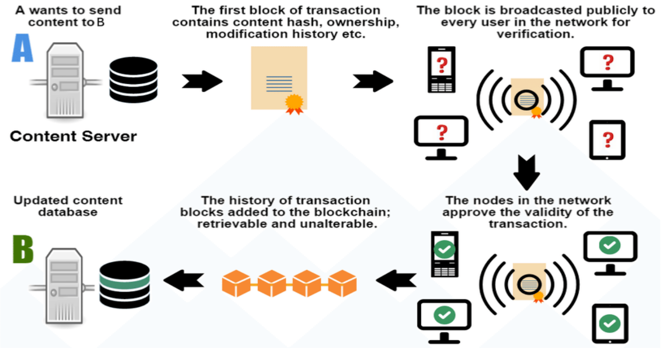
A wants to send content to B
A
Content Server
The first block of transaction contains content hash, ownership, modification history etc.
The block is broadcasted publicly to every user in the network for verification.
?
Updated content database
B
The history of transaction blocks added to the blockchain; retrievable and unalterable.
The nodes in the network approve the validity of the transaction.

Fig -2: Blockchain working model

This example doesn't imply that Blockchain has to (or can) manage all aspects of identity governance and administration but it demonstrates how IAM architects may leverage Blockchain as a new technological component to potentially reinvent IGA capabilities. The hope is to address the existing challenges of IAM record keeping more efficiently and effectively in real-time. Again, this is supposed to be an example idea on how Blockchain may impact IAM solutions, not a validated design in any way.

3. CONCLUSION

This example doesn't imply that Blockchain has to (or can) manage all aspects of identity governance and administration but it demonstrates how IAM architects may leverage Blockchain as a new technological component to potentially reinvent IGA capabilities. The hope is to address the existing challenges of IAM record keeping more efficiently and effectively in real-time. Again, this is supposed to be an example idea on how Blockchain may impact IAM solutions, not a validated design in any way.

REFERENCES

[1] Xu, Xiwei, et al. "A taxonomy of blockchain-based systems for architecture design." 2017 IEEE International Conference on Software Architecture (ICSA). IEEE, 2017.
[2] Xia, Q. I., et al. "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain." IEEE Access 5 (2017): 14757-14767.
[3] Do, Hoang Giang, and Wee Keong Ng. "Blockchain-based system for secure data storage with private keyword search." 2017 IEEE World Congress on Services (SERVICES). IEEE, 2017.
[4] Fan, Kai, et al. "Medblock: Efficient and secure medical data sharing via blockchain." Journal of medical systems 42.8 (2018): 136
[5] Hinarejos, M. Francisca, Josep-Lluis Ferrer-Gomila, and Llorenç Huguet-Rotger. "A solution for secure certified electronic mail using Blockchain as a secure message board." IEEE Access (2019).
[6] mingxin ma 1, (student member, ieee), guozhen shi2,and fenghua li3, (member, ieee). "Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in IOT Scenaio." IEEE Access (2019).

BIOGRAPHIES

Ms.D. Nancy Kirupanithi, is a research scholar of Hindustan Institute of Technology and Science, Chennai. She is pursuing Ph.D in the area of Blockchain.

Dr.A.Antonidoss currently working as Associate Professor in Hindustan Institute of Technology and Science, Chennai. His areas of interest are Cloud Computing and Data Mining.