JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Deployment of a Block chain-Based Self-Sovereign Identity

[1] Minakshi J. Bhosale [2] Prof. Antosh M. Dyade
[1] Computer Science & Engineering [2] Computer Science & Engineering,

Abstract— Digital identity is unsolved: when a few years of analysis there's still no trustworthy communication over the net. to produce identity among the context of mutual distrust, this paper presents a block chain-based digital identity answer. While not relying upon one trustworthy third party, the projected answer achieves passport-level lawfully valid identity. This answer for creating identities Self-Sovereign, builds on a generic demonstrable claim model that attestations of truth from third parties have to be compelled to be collected. The claim model is then shown to be each block chain structure and proof technique agnostic. Four totally different implementations in support of those 2 claim model properties are shown to supply sub-second performance for claim creation and claim verification. Through the properties of Self-Sovereign Identity, lawfully valid standing and acceptable performance, our answer is taken into account to be appropriate adoption by the overall public

Index Terms—Block Chain, Identity

I. INTRODUCTION

Through businesses Associate in nursing establishments existing in an system of mutual distrust, identity has gotten fragmented. This has junction rectifier to massive amounts of our identity information being duplicated onto the servers of authorities. Current identity solutions need United States of America to carry several plastic cards that we tend to use to spot ourselves or pay with. we'd like to possess a username and watchword for several completely different websites. This suggests that the people whose information is hold on don't have any -or little- management over this information. Furthermore, these servers that collect privacy sensitive information become prime targets for attacks: honey pots. we tend to still have a digital identity downside, despite the fact that solutions have already been projected for this identity downside several decades past. The idea of public keys has been around since 1976, once Diffie and playwright created their (DiffieHellman) key exchange technique. supported this public key idea, Pretty sensible Privacy (PGP) has been around since 1991 [1]. However, it's conjointly been identified for nineteen years [2] that PGP, created twenty seven years past, isn't being adopted. to the present day this adoption downside persists. There has nevertheless to emerge a digital identity resolution that solves the digital identity psychosis.

Block chain's versatility is primarily due to its immutable and almost indestructible nature. These attributes have caught the attention of researchers and developers interested in applications and environments where the need for the integrity of identity and content are as paramount as the safe delivery and record of transactions. Self-sovereign digital identity in particular is often cited as a human right that nation states need to embrace with as much conviction as education and lifelong learning are considered to be a public good. Although the block chain has long been identified as an opportunity for driving much-needed

Change in the core processes of the education sector, use cases to date have been limited in scope and execution, with block chain advocates and education policy makers seemingly disconnected on fundamental issues such as governance, self-sovereignty, interoperability, choice of block chain platforms and overall trust in standards and the integrity of the infrastructure.

II. LITERATURE REVIEW

One can be tempted to mention that the conception of Self-Sovereign Identity finally solves our twenty seven year recent digital identity downside. However, whereas the companies and establishments not got to trust one another, they additionally don't trust the user to be truthful. This paper can rest on the findings of previous Self-Sovereign Identity initiatives like Sovrin1 and uPort2 and leverages a block chain to resolve this trust downside. By utilizing a block chain, users may be tied to the claims they create and herewith be caught guilty if they plan to cheat the system. Users may be caught committing identity fraud. In distinction to the antecedently mentioned solutions, this paper can gift AN academically pure model for Self-Sovereign Identity. In our model there doesn't got to be a foundation assignment infrastructure. In our model there's no risk of the block chain owner or fifty one of the network to hard-fork a user out of existence [1]. There'll be no third party au fait of attributes: there'll be no vender lock-in. A key property of our model is open enrollment: any user will merely begin mistreatment the answer while not requesting permission.

The first half the matter we have a tendency to observe within the current identity scheme, is that the proven fact that identity holders ought to conjointly be the identity house owners. This half may be a lot of formally described because they want for Self-Sovereign Identity. The second half of the matter consists of the passport-level attributes in this identity. In alternative words, identities that square measure recognized by governments and so have legal price. Within the context of block chains we will formalize this last half of the matter
As the want for wrongfully valid signatures. This section can initial explain the issues of Self-Sovereign Identity then the Section can follow up with the outline of wrongfully valid signatures.

III. PROPOSED SYSTEM

The design for our true Self- Sovereign Identity model leans on the properties of personalized Block chain structures like

- Trust Chain or The Tangle
- Generate Provable Claims
- Zero Knowledge Proof
- Generate Claim Data

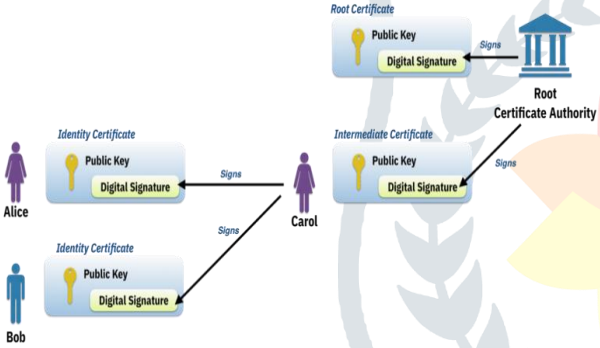

Figure1. Data Flow Diagram

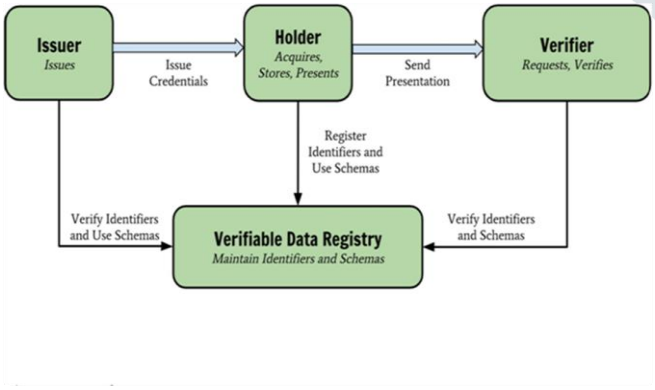

Figure2. Proposed System Architecture

SR NO	Field	Description
1	Name	Name of attribute
2	Time Stamp	The time of Claim Creation
3	Validity Term	The time after claim is not valid
4	Proof Format	The time of proof for the Claim
5	ProofLink	The Strong link to the proof for the claim

Table1 Attribute Data

Trust Chain or the Tangle

The claims which are able to be conferred don't hold any intrinsic truth. Users will build false claims and users will erase their identity (also known as a whitewashing attack). That's to mention that data delivered by a user ought to solely be regarded as the truth, if the user will offer proof for the claim. Establishment of truth can have to be compelled to involve multiple parties, which provide attestations. The trust in alternative parties attesting to the reality of a user's claim then adds up to the trust within the user's claim.

Generate Provable Claims

The most necessary property of Self-Sovereign Identity, Regarding the look of claims is that of protection. The users Right to privacy and also the right to be forgotten may be joined into the need for a mechanism to disclose data to specific parties on demand. Moreover, once shared, the knowledge the other party receives shouldn't be appropriate re-use. In other words, the received data ought to hold truth just for the party the knowledge was disclosed to. This lends itself nearly perfectly to a Zero-Knowledge Proof structure.

Chains of claims

When planning this chain of claims, we have a tendency to acknowledge that there square measure completely different use cases for claims. Some claims might be expected to last forever (once one hits the age of twenty one, one will ne'er become younger). Some claims might not gift an active risk once used while being revoked (receiving a parking allow for associate address you now not live at),even though they must be detected and admonished. Lastly, in the worst case, some claims might need period of time proof of correctness (not being a terrorist once checking in to the airport). looking on the employment case for the attribute, we identify 3 levels of increase for the audit logs: a passive, an intent-based associated a full of life model.

IV. EXPERIMENTAL RESULTS

1. UI Screenshot

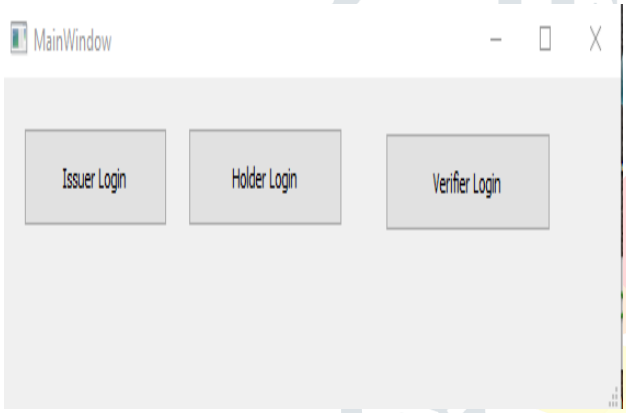

Figure3 UI Screen Shot

2. Block Chain Creation

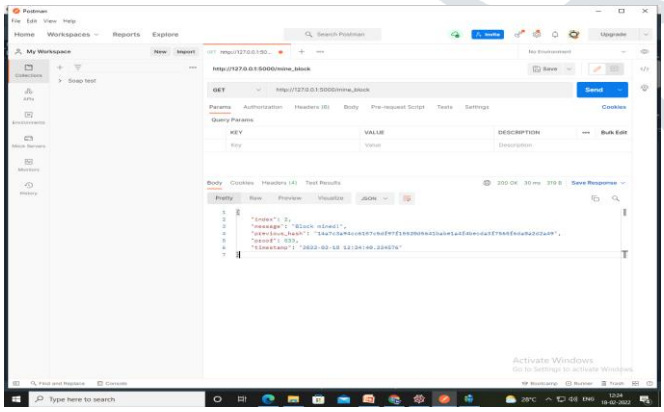

Figure4 Creation of Block Chain

3. Chain of Request

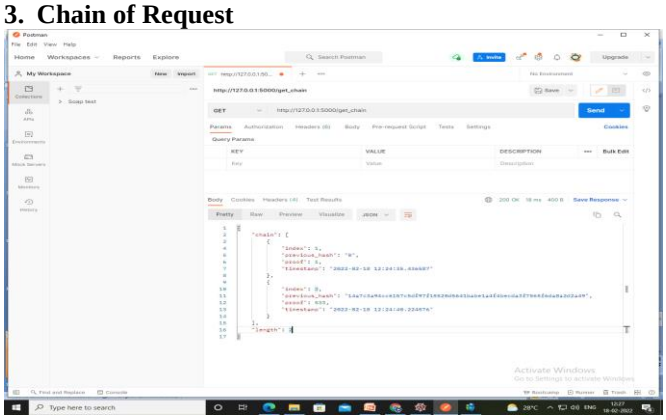

Figure5 Creation of Block Chain

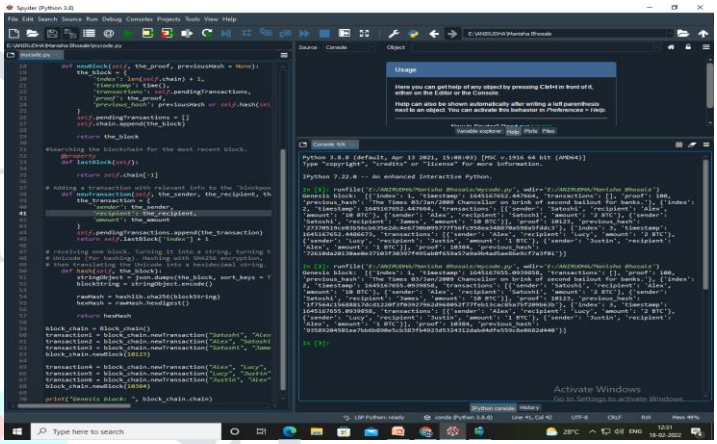

Figure6 Message Passing

CONCLUSION

After twenty seven years, the online of trust finally features a likelihood to become reality. This paper has bestowed the bottom work for a Self-Sovereign Identity answer that is in productions to be used by voters within the latter half 2018. As such, this makes the answer of this paper the second (after Estonia) digitized passport answer to travel live in the world. the answer of this paper is that the world's 1st permission less localized digitized passport and a real peer-to-peer identity commons. For the primary time, voters can become the house owners of their own identities. now not is that the identity of users within the hands of one (federated) authority.

REFERENCES

[1] Philip Zimmermann. Why i wrote pgp. PGP User's Guide, 1991.

[2] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. USENIX Security Symposium, 348, 1999.

[3] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. A survey of attacks on ethereum smart contracts (sok). In International Conference
on Principles of Security and Trust, pages 164–186. Springer, 2017.

[4] Christopher Allen. The path to self-sovereign identity. 2016. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-so
verereignidentity.
html.

[5] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), 2015 IEEE, pages 180–184. IEEE, 2015.

[6] Pim Otte, Martijn de Vos, and Johan Pouwelse. Trustchain: A sybilresistant
scalable blockchain. Future Generation Computer Systems, 2017.

[7] Serguei Popov. The tangle. 2016. Available: http://untangled.world/iotawhitepaper-
tangle/.

[8] Michal Feldman, Christos Papadimitriou, John Chuang, and Ion Stoica. Free-riding and whitewashing in peer-to-peer systems. IEEE Journal on
selected areas in communications, 24(5):1010–1019, 2006.