Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 2, 977-983 (2021)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Blockchain-Based Decentralized Digital Self-Sovereign Identity Wallet for Secure Transaction

Md. Tarequl Islam[1,*], Mostofa Kamal Nasir[1], Md. Mahedi Hasan[2], Mohammad Gazi Golam Faruque[3], Md. Selim Hossain[4], Mir Mohammad Azad[3]

[1]*Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail-1902, Bangladesh*

[2]*Department of Management and Information System, Prime University, Dhaka-1216, Bangladesh*

[3]*Department of Computer Science and Engineering, Khwaja Yunus Ali University, Enayetpur, Sirajganj-6751, Bangladesh*

[4]*Department of Computing and Information System, Daffodil International University, Dhaka-1207, Bangladesh*

ARTICLE INFO

Article history:
Received: 24 January, 2021
Accepted: 07 April, 2021
Online: 22 April, 2021

Keywords:
Decentralized identifier
Distributed ledger
Identity management
Self-sovereign identity
User-controlled identity wallet
Verifiable credential
Zero-knowledge proof

ABSTRACT

Blockchain (BC) as the widespread innovations in the 21st century has recognized itself to be immutable, tamper-resistant, decentralize and secure. This emerging technology is used as a functional technology for refining present technology and forming new applications for its robustness and disintermediation. Decentralized Digital Self-Sovereign Identity (DDSSI) is an identity mapped with individual identity information along with the user's reputation in the transaction. User's information will be preserved in the decentralized cloud server which will be controlled and maintained by the user. In this research work, we suggest a Blockchain-centered DDSSI wallet to modernizes the existing identity management system that will be used to identify as well as access control to provide validation and endorsement of entities in a digital system. BC technology in this innovation ensures credible and safe information in a transaction besides. Here, we use Bitcoin cryptocurrencies to generate secure and unique DDSSI public key addresses by integrating the private key with the random number for transferring and accepting information and a token-based system to identify customer reputation.

1. Introduction

The Internet of Things (IoT) targets linking the whole thing from human-being, households, organizations, and objects in the real world. About 13.5 billion devices will be connected which are equipped with actuating and sensing abilities [1]. This very fast-growing innovation in the digital ecosystem with the diversity of e-services, a variety of entities, billions of people, trillions of devices need to have their own digital identities to be easily identified and interrelate with each other in this virtual world safely and securely. In the early decades, credentials as username and password were commonly used for every individual to do registration, access and manage in the different online platform. Societal security address, National identification number, passport number, and other authentication numbers were used in the traditional approach. The systems have a centralized databank for storing individual records [2]. The national identity management systems experience security instabilities subject to system downtime, attacking hackers and software up-gradation as well as network traffic restrictions [3]. Identification, authorization and authentication process of individuals must have mechanisms to manage the information about individual trustworthily. In recent times, the internet security issue is very challenging and crucial. The secure access demand is a very significant assurance for the information technology workforce. As a result, individual information is often tampered with or leaked. Therefore, society demands secure identity management. With the benefits of BC technology, identity management offers a decentralization feature without using any centralized database or dedicated databank where information can be stored and verified your identity on the internet. Our DDSSI ensures secure, safe and authentic identity management with the integration of BC technology. DDSSI is a unique perfect in which somebody, organization, or entities completely preserves as well as panels their data that is not administered by the federal system which can never be unconcerned from the identity owner. The necessities of the SSI are designated below:

[*] Corresponding Author: Md. Tarequl Islam, Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh, Email: tareq.cse@gmail.com

https://dx.doi.org/10.25046/aj0602112

The owners of the Identity have full control over the data. Data reliability, safety, and confidentiality are ensured by the system where central authority is not mandatory for reliance.

It arranges for full transportability of the information where owners can procedure their uniqueness documents in where they want for example accessing an online service.

Changes to the data are clear, and clearness is continued by the system [4]. BC proprietors are recognized by public-key cryptography based on unique elucidations to develop the conception of asymmetric cryptography to assign digital identity. Several features of BC mark the technology appropriate for well-organized and secure identity supervision: BC is a digital ledger system that is immutable and transparent (based on permissions or permission-less) where immutability and transparency are important for identity management. Single point of catastrophe and denial of service (DoS) attacks can be unaffected by BC technology. BC offers a proficient application of public-key cryptography and hashing which:

- can be persistent for digital identity control.
- provisions protect the integrity and validity of identity-centered records.
- can be developed for third-party attestation of proceedings.
- supports simplifying agreement-oriented record delivery with smart contracts. technology.

BC eradicates domination in identity management, as it is not controlled by a central power that permits identity and records amalgamation on a worldwide scale. BC chains inducements via crypto-currencies that can be applied for convinced responsibilities such as providing incentives to the participants for data sharing.

2. Background Work

This section represents the advancement of identity management systems: Centralized ID System, Integrated ID system, and Self-sovereign ID system.

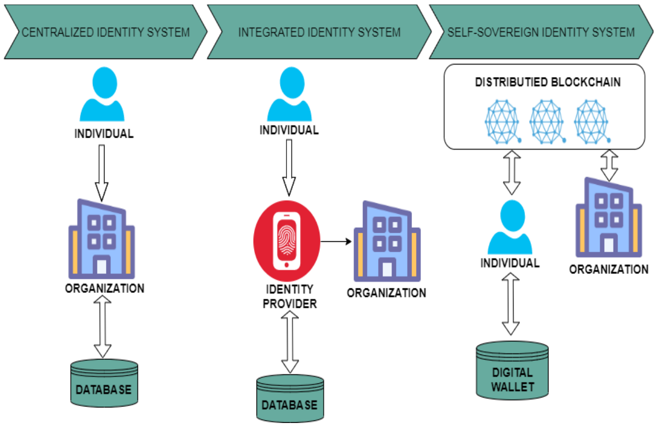

Figure 1: Advancement of the Identity Management System

2.1. Centralized Identity System (CIS)

A centralized identity system is the SILOED and the simplest traditional identity system which was used in the early days of the internet. Organization issues digital credentials that users can use to access the services of the organization [5]. In this system, the organization controls and stores the identity-related credential of the user. Besides, to obtain service, the user needs separate credentials for each system or organization. The trust association between user and organization is built on a mutual secret, in most circumstances, log-in username is typically linked with a password. Recently, with the advancement of the Internet of Things, every organization, and billions of people are now connected over online, problems such as fraud are rising fast.

2.2. Integrated Identity System (IIS)

This integrated identity system incorporates a third-party enterprise or confederation to act as a centrally controlled identity provider between an organization and user [6], [7]. In IIS, the identity provider issues digital credentials to the user to access the services of the organization integrated with the identity provider. IIS resolves two major issues, firstly, IIS provides seamless access to the services of the organization where the liability of handling identity as well as password confidentially by integrating an entity who provides identity, which is a supplementary duty besides the core commercial procedures and secondly, it eliminates the encumbrance from account holders to accomplish numerous identity-associated information for numerous entities by proposing a Single-Sign-On (SSO) benefits. IIS works as a user login to the identity provider portal, which then “federates” login to the facility using numerous protocols such as OAuth, SAML, or OpenID [8] Connect. Trust between the user and the identity provider is preserved similarly to CIS.

2.3. Self-Sovereign Identity System (SIS)

SIS is a two-parties relationship identity system which is the advancement of IIS, where no third entity coming between the user and the organization [7]. SIS directly connects user and organization as a peer. Users have full control over their confidential and personal data by using a digital wallet. SIS wallet stores all the trustworthy and private data on the system that is maintained by the user. SIS introduces three significant entities i.e. owners, issuers, and verifiers. Credentials are created and issued to the owners by an issuer who gets credentials from an issuer, stores it, and submits these credentials to the verifier to verify once required [9]. The verifier accepts and authenticates credentials claimed by owners.

2.4. Blockchain and Bitcoin

To keep pace with the era, there is no alternative way to the development of technology. A trustworthy system is a key objective to deal with profound data such as commercial transactions with digital currencies even when it is very difficult where no authentication nor assessment apparatuses are delivered. This framework presented two essential thoughts[10]. The first one is Bitcoin which is a virtual value of cryptocurrency without depending on any centralized organization. Somewhat, the currency is held collectively and securely by a distributed network of the user that makes up an auditable and confirmable network. The other concept, whose reputation has away even further than the cryptocurrency itself, is BC. BC is the approach that consents communications to be tested by a group of untrustworthy users. It delivers a disseminated, immutable, apparent, confident and auditable register [11]. The BC can be accessed willingly and entirely, permitting access to all contacts that have arisen since the first transaction of the approach, and can be certified and organized by any individual at any instance. The BC protocol organizes data in a chain of blocks, where a set of Bitcoin transaction details accomplished at certain instances are stored. Every block is associated with the prior block, for developing a chain. To support and operate with the BC, network peers have to provide, the functionalities of storage, transmitting, mining and wallet amenities [5] are delivered by network peers to control and provision with the BC. BC is a digital ledger where a paired node shares their data transacted between them. As it was earlier stated that this approach is deliberated as the key contribution of Bitcoin since it resolved a long-lifelong commercial issue known as the dual-spend problem. The explanation anticipated by Bitcoin comprised in looking for the consensus of the most mining nodes, who affix the effective transactions to the BC. Although the BC concept was initiated as a means for a cryptocurrency, it is not obligatory to improve a cryptocurrency to practice BC and construct the decentralized solicitations [12]. A BC is a chain of time-stamped blocks that are connected by hashing address of cryptocurrency and is the process by which data is distributed among all nodes [13].

Table 1: Comparison of different types of an identity management system

	PKI	Bitcoin Based	Ethereum Based	Reputation	Privacy	Year
Namecoin		●				2014
Certcoin	●	●				2014
Fromknecht	●	●				2014
Uport	●		●			2015
Soverin	●			●	●	2016
Jolocom	●		●			2016
Chainanchor	●				●	2016
NEXTLEAP	●		●		●	2017
Azouvi	●		●		●	2017
Axon	●	●			●	2017
Augot	●	●			●	2017
SCPKI	●		●		●	2017
DDSSI	●	●		●	●	2021

The Namecoin [14] used a Bitcoin-based BC system to provide domain naming systems along with the IP address identification. The next that has been modified by Namecoin, Certcoin [15] forms decentralized validation system PKI. A paper of decentralized PKI [16] proposed certcoin factors to certify the preservation of identities where entities could not register multiple times. Privacy-awareness in blockchain-based PKI [17] scrutinizes privacy desires when planning decentralized PKI methods and a blockchain-based PKI with concealment consciousness has been signified here. According to a user system for verified identities [18] amend the Bitcoin stack to construct an identity management resolution and introduce a zero-knowledge proof. Secure identity registration on distributed ledgers [19] are other decentralized systems along with confidentiality preserving landscapes using blind signatures. Besides, several setups and researchers collaborating with technological experts are concentrating on the improvement of identity methods such as Evernym, Uport [8], [20], Shocard [21], Civic [22], Jolocom [23], Bitnation [24] and Sovrin [8] to solve the digital identity problem. We also propose PKI based DDSSI identity system where we use a Bitcoin system along with the combination of privacy [25] and reputation with the collaboration of BC [26].

3. Proposed Method

In this research, we suggest a DDSSI structure using a Bitcoin cryptocurrency-based BC system. Unlike other identity systems, our proposed method contains three parts: i) identity address ii) user information and iii) reputation task of the user. Here, we use bitcoin cryptocurrency to generate secure addresses by Elliptic curve formula where a random number is integrated with a user private key. In general, a pseudo-random number generator generates a random number that is almost deterministic. Therefore, we have proposed to ingrate private keys with a random number to generate the secure address. The private key (pK) is very important in cryptography. Here, we integrate a user-defined private key and a random number to generate a digital identification address ($dSI_{address}$) for transferring and accepting data by using SHA-256 hash function. In this system, the number of bits is reduced and the security is enhanced compare to RSA encryption [27]. User information (dSI_{info}) is user-controlled data as biometric data, images and other attribute inherited from national identity (NID). User can set any other attribute belongs to them those are encrypted by pK and are hashed to create dSI_{info} which is controlled and maintained by the user. User can update their information at any time. uRtoken is used to detect user behavior. Therefore, a user is individually recognized by the amalgamation of their record, public key Bitcoin address, and uRtoken.

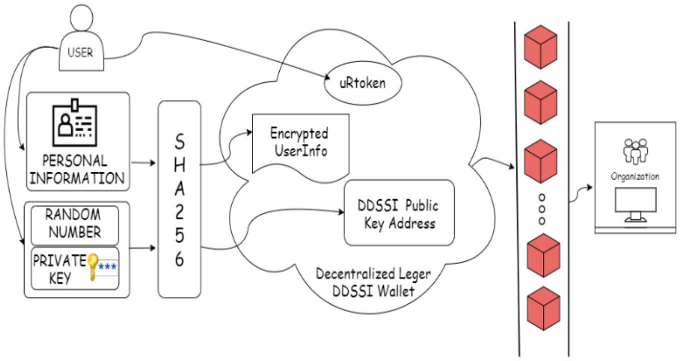

Figure 2: Block diagram of DDSSI Wallet

An entity user may change their information even the address $dSI_{address}$ may be updated which will not impact the user behavior uRtoken. While updating the user information, a new hash value to be generated and uRtoken will not be impacted and migrated to the new one. Users may request to change their address. In this case, the user information and token will be transferred to the new one. In both cases, the old information is stored in BC. Sidestepping the attackers conceal their credentials by altering their addresses. The amendment of the user's information must require their aforementioned address which was delivered to ensure the acceptability of the information alteration process. Reputation is the behavior in which the aspect of identity in the scheme is noted. uRtoken is one type of reputation system where no one can alter the manipulator's information to confirm the protection of the individuality connected information. As soon as manipulator comportment meets the execution situations, the convention is inevitably completed with the data precisely written or improved, confirming the safety of the associated information.

3.1. Algorithm

Input: a ϵ Private key, National Identification Number, Random Number, user information

output**:** a gateway to access enterprise platform, validation and mine transactions

- Generate Bitcoin address $dSI_{address}$ by using a random number of generator and Private key (pK)
  $dSI_{address}$ = *SHA256(RANDOM_NUMBER, pK)*
- Create user digital identity information by hashing and encrypting user information and NID by the private key.
  $\mathbf{dSI}_{info}$ = *SHA256(NID$_{info}$, entity information)*
- *Organize wallet to authenticate and authorization of access.*
  $\mathbf{dSI}_{wallet}$ = *(*$\mathbf{dSI}_{info}$*,* $dSI_{address}$*, uRtoken) where uRtoken:* ϵ *(Reputation of user)*

Another way, uRtoken is cast-off to recognize the manipulator's character which is an object of the manipulator in a physical world to distinctively recognize. The feature of uRtoken is that the alteration of distinctiveness information will not distress the manipulator's character by avoiding the formation of various identities, the system accomplishes uRtoken alteration when a manipulator changes his uniqueness info.

Another way, uRtoken is cast-off to recognize the manipulator's character which is an object of the manipulator in a physical world to distinctively recognize. The feature of uRtoken is that the alteration of distinctiveness information will not distress the manipulator's character by avoiding the formation of various identities, the system accomplishes uRtoken alteration when a manipulator changes his uniqueness info.

An alternative form of uniqueness amendment is the modification of manipulators' Bitcoin-based public identity. Once a manipulator desires to alter his Bitcoin-based public identity, the scheme will also create a new address, and the ancient identity will persist warehoused in the BC. Consequently, the individuality information and uRtoken are lifted from the ancient identity to the reorganized one, circumventing the invader's hide their uniqueness by changing their identity. It is well-known that the alteration of a manipulator's address entails the manipulator deliver his ancient address of the ID to confirm the lawfulness of the address amendment procedure. Once a manipulator always behaves honestly and energetically, the manipulator's reputation should be high, and verse vice. As a result, the uRtoken score of a manipulator replicates the manipulator performance variation with time.

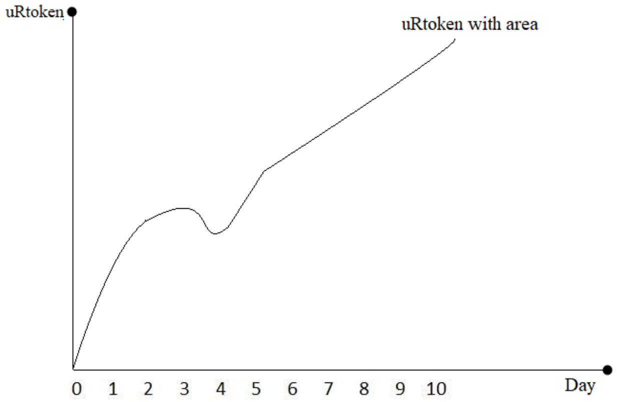

Figure 3: Identification of user behavior by reputation token.

The uRtoken is symbolic related to the repute parameters and inducement responsibilities. In this paper, we recommend a new perception uRtoken day that gathers the stricture apprehending the entire number of days a manipulator grasps uRtoken. For example, a manipulator has convinced figure of uRtoken at time t, at that time the manipulator's uRtoken day upsurge by uRtoken at time t+1. In other words, a manipulator's uRtokenday is a snowballing function of time, and it rises quicker when the manipulator has more uRtoken. When uRtoken of a manipulator is positive, the manipulator's uRtokenday resolve reliably rises gradually.

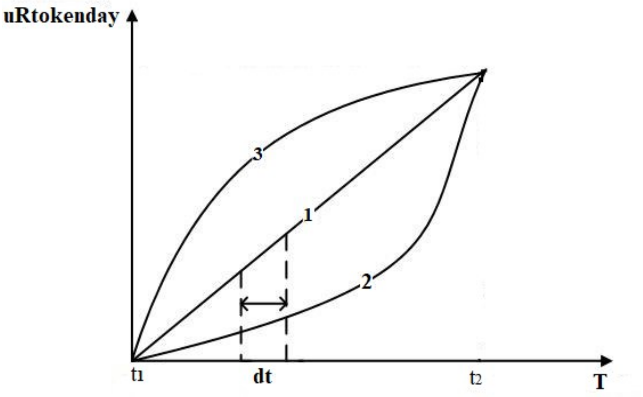

Figure 4: Changing the behavior of uRtoken concerning time.

Consequently, uRtokenday organizes not only replicate the number of tokens that manipulators holding, but also imitate the days that uRtoken holds the day. When the manipulator holds a static uRtoken, and the manipulator's uRtokenday will increase linearly. On the other hand, when the manipulator holds a smaller amount of uRtoken primarily and gains more and more uRtoken concerning time. As a result, the user's uRtokenday rises convexly. In the same way, if the manipulator holds a greater volume of uRtoken at first and loses it progressively. In this case, the manipulator's uRtokenday will be increased concavely.

- ΔuRtoken$_i$ = 0 which indicates that the amount of uRtoken held by the manipulator i with time T remnants unaffected.
- ΔuRtoken$_i$ < 0 which represents that the quantity of uRtoken held by the manipulator i with time T is diminished.
- ΔuRtoken$_i$ > 0 which represents that the quantity of uRtoken held by the manipulator i with time T is improved.

Let us consider m manipulators in a particular scheme. In the first stage, the manipulators are graded according to the rising sequence, and we signify the manipulator address of the manipulator with the minimum Si as S1, and so on. In the second phase, we bounce 1 to manipulator 1, and 2 to manipulator 2, and so on. Here, when the manipulators with a similar representative deviation, the score will remain similar. In other arguments, if Si = Si+1, then Rsi = Rsi+1 = i, which resultant the extreme value of the status score k is a reduced amount of or equal to m.

Table 2: Ranking Score of uRtoken

S_i (ascending)	S_1	S_2	……	S_{m-1}	S_m
R_{si}	1	2	…….	k-1	k

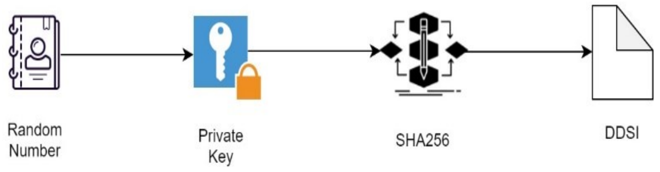

Figure 5: Bitcoin address generation

3.2. Bitcoin Address Generation

The random numeral is a procedure through which an expedient, produces an order of facts or signs that cannot be sensibly forecast restored than by a haphazard casual. Random number producers which is hardware random-number producers which produce haphazard records as an occupation of present charge of some physical environment quality. Produce haphazard information within a min and max series that describe and category the outcomes as well as to create a usual of one to ten thousand arbitrarily chosen information. By integrating a private key with a random number, we can generate a secure number. A sequestered key, also recognized as an undisclosed key, is adjustable in steganography that is cast-off with an algorithm to encrypt and decrypt code. Clandestine secrets are only communal with the key's producer, creating it extremely protected. Private keys play an important role in symmetric cryptography, asymmetric cryptography, and cryptocurrencies. The SHA is one of a numeral of cryptographic hash functions. A cryptographic botch is like a signature for a piece of information. If you would compare two cliques of raw data, it is always restored to hash it and equivalence of SHA256 principles. It is the fingerprints of the information. Even if only one sign is altered the algorithm will yield diverse hash value. SHA256 algorithm produces an almost-unique, static size 256-bit hash. Hash is also known as a one-way occupation. This type is appropriate for scrutiny truthfulness of our data, contest hash verification, anti-tamper, digital autographs, BC. If we generate a random number and add it to a user-defined private key, then we pass it SHA256 hash-based algorithm to generate DDSI number.

3.3 Elliptic curve along with bitcoin address

We can generate secure random number by programming coding using java, C++ etc. Generating cryptographic pseudorandom numbers, total number of combinations have been found:

$2^{(32*8)} = 2^{256} =$ 115,792,089,237,316,195,423,570,985,008,687, 907,853,269,984,665,640,564,039,457,584, 007,913,129,639, 936 (78 digits or approximately 10^{77})

After generating the pseudorandom numbers, we have added the private key as a password. As a result, we will get.

Random number = SHA256(SHA256(password)))

Password: selimtareq@csekyau-12. The 32 bytes signature generating by cryptographic secure SHA256 algorithm that is almost impossible to guess and decryption to the original number in impossible. This omnidirectional algorithm generates HashA1 value that is always 256 bits in length.

By using elliptic curve cryptocurrency can be calculated: $y^2 = x^3 + ax + b$. Elliptic curve assets:

- If a line crosses twofold themes P and Q, it crosses the third point -R.
- If a line is a digression to the curve, an alternate point will be crossed.
- The curve will be intersected by all vertical lines at an extent.

3.4. Calculation of BITCOIN Public Key

Elliptic curve (ECC) was developed by Neal Koblitz and Victor Miller in 198 and used in Bitcoin or Litecoin Cryptocurrencies. A 256-bits ECC key is more beneficial in terms of security compared to RSA public key encryption of 3072 bits. Therefore, processing power consumption is also very less for using ECC. Ellipses are designed by quadratic curves (x^2) where the elliptic is cubic (x^3).

Public Key Version Hash D =Version "00 " || HashD2: Hash the Public Key Version Hash D value using the cryptographic hash function SHA256. This omnidirectional Secure SHA256 algorithm generates 256 bits signatures. The Public Address Compressed is the Public Key Checksum D value coded into a Base58 value. The Public Key Compressed value can be made public and can be transformed into QR cryptographs and can be written on paper wallets.

Koblitz curve using standard efficient cryptography tools	
Parameter	*Value*
a, b	The ellipc arc is defined by the constant a and b, $y^2 = x^3 + ax + b$, $a = 0$, $y^2 = x^3 + ax + b$, $b = 7$
p	The finite number of elements is the prime number p. F_p is called the prime field of order p along with class modulo p, where the p elements are denoted 0, ..., p - 1. This means prime number p should be used for all the finite field math operations (better known as modulo operation), for example: $y^2 \bmod p = (x^3 + ax + b) \bmod p$. The output of the math operation should never be bigger than the p value. $p=2^{256} -2^{32} -2^9 -2^8 -2^7 -2^6 -24 -1=2^{256} -2^{32} -977$
G	On the elliptic curve, the predetermined base spot (xG, yG). By the equation, $yG = (x_G^3 + 7)^{1/2}$, we can obtain yG coordinate Therefore, xG and yG are the first and last half of the coordinate as followings: xG: 79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798 yG: 483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
n	n is the prime number of basepoint. 32 bytes number in the series [1, n - 1] is a endorsed private key. Thus the range of any 32 bytes number from 0x1 to 0xFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD 25E8CD036 4140 is a valid private key.
h	The cofactor: 01

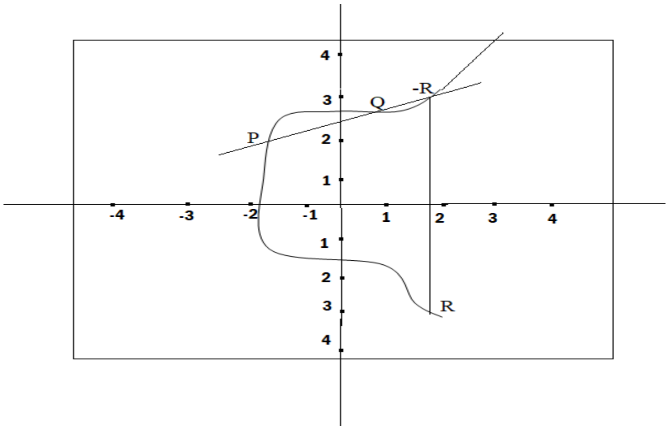

Figure 6: Generation of public key using elliptic curve approach.

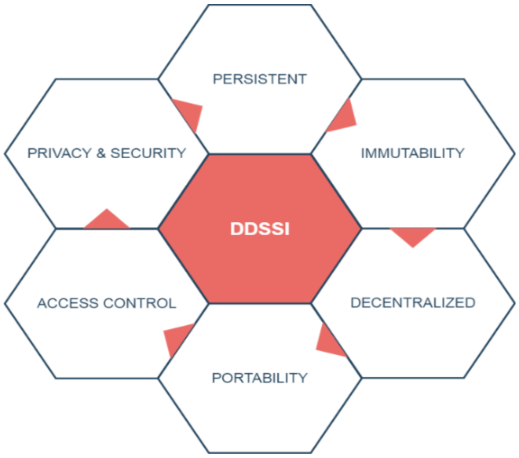

Figure 7: Fundamental characteristics of DDSSI

4. Major Outcomes of DDSSI

There are lots of benefits to using this proposed identity management system that can make the system is desirable for every nation, organization and person to maintain secure and timely manner transaction.

Existence: Each user must have a unique self-governing digital existence in the DDSSI system.

Control: User acts as decisive experts who must have full control over the data as well as their identities.

Access: Users must be able to access their identities effortlessly without any overseer. They should be cognizant about any alterations at each time that have been amended to all claims correlated to their identities at each time.

Transparency: All the algorithms and systems that are being used in the DDSSI wallet must be transparent. Therefore, each user can monitor how they are controlled, reorganized and worked accurately.

Minimization: Disclosure of information must be minimized and provide data as minimal as necessary.

Persistence: Data must be retained unchanged even the system is being upgraded or any changes made in the algorithm. User identities must be perdurable until the user's desire.

Portability: Each user can disseminate their identities and make them usable once they need it even, they can dispel third-party dependency. Similarly, the user can transmit the identity when they need it.

Interoperability: Identities must be adequate anyplace in the sphere as serviceable as possible, the system would drop flexibility without ensuring interoperability.

Protection: User rights acts as a key purpose and guideline principle of an owner. The boundary of user rights must be stated and protected.

Consent: Individual identity repositories may be stolen by the intruder. Users must have a prior agreement for using their identity.

Apart from those properties we propose one further requirement Non-repudiation to make any transaction trustworthy between DDSSI owners. Therefore, one entity can't throw away the validity of a claim or action taken earlier. Based on the above features we propose a typical architecture of DDSSI to provide a decentralized secure and safe platform to store user's identity information and every smart transaction that happened by itself. Compare to other approaches, it would be more beneficial as this approach used reputation-based transaction management as a digital signature of behavior by that users can define borders within which they make the decision and outside of which they negotiate with others as peers.

5. Conclusion

In every single moment, an enormous digital revolution is experienced in the world. And now, the physical entity along with digital instances is merging to form a single reality. Therefore, we unquestionably need a new approach to manage all the digital entities. Specifically, the approach should have privacy and security in every circumstance. That's why DDSSI shows light in the way for this picture-perfect solution. In practice, the approach offers rights and full control of user identity along with makes the system manage it effortlessly. As we have used the immutable decentralized BC with Bitcoin technology to maintain the system safe, secure and fast. Therefore, in the coming days, we believe that the proposal would be the best approach to make the system decentralized.

References

[1] X. Zhu, Y. Badr, "Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions," Sensors (Basel, Switzerland), **18**(12), 1568–1573, 2018, doi:10.3390/s18124215.

[2] M.B. Ferreira, K.C. Alonso, "Identity management for the requirements of the information security," IEEE International Conference on Industrial Engineering and Engineering Management, 53–57, 2014, doi:10.1109/IEEM.2013.6962373.

[3] P.R. Sousa, J.S. Resende, R. Martins, L. Antunes, "The case for blockchain in IoT identity management," Journal of Enterprise Information Management, (January), 2020, doi:10.1108/JEIM-07-2018-0148.

[4] M.A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, H. Ning, "Distributed ledger technology for ehealth identity privacy: State of the art and future perspective," Sensors (Switzerland), **20**(2), 1–20, 2020, doi:10.3390/s20020483.

[5] N. Naik, P. Jenkins, "UPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain," ISSE 2020 - 6th IEEE International Symposium on Systems Engineering, Proceedings, 2020, doi:10.1109/ISSE49799.2020.9272223.

[6] N. Naik, P. Jenkins, "Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect," Proceedings - International Conference on Research Challenges in Information Science, 163–174, 2017, doi:10.1109/RCIS.2017.7956534.

[7] N. Naik, P. Jenkins, "A Secure Mobile Cloud Identity : Criteria for Effective Identity and Access Management Standards."

[8] S. Foundation, "Sovrin^{TM}: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust," Sovrin, (January), 1–41, 2018.

[9] A. Tobin, D. Reed, "The Inevitable Rise of Self-Sovereign Identity," White Paper, **29**(September 2016), 10, 2017.

[10] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Future Generation Computer Systems, **88**(2018), 173–190, 2018, doi:10.1016/j.future.2018.05.046.

[11] B. Alotaibi, "Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review," IEEE Sensors Journal, **19**(23), 10953–10971, 2019, doi:10.1109/JSEN.2019.2935035.

[12] V. Cheshun, I. Muliar, V. Yatskiv, R. Shevchuk, S. Kulyna, T. Tsavolyk, "Safe Decentralized Applications Development Using Blockchain Technologies," in 2020 10th International Conference on Advanced Computer Information Technologies, ACIT 2020 - Proceedings, Institute of Electrical and Electronics Engineers Inc.: 800–805, 2020, doi:10.1109/ACIT49673.2020.9208830.

[13] Book Review: "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction," - ProQuest, Apr. 2021.

[14] M.T. Hammi, P. Bellot, A. Serhrouchni, "BCTrust: A decentralized authentication blockchain-based mechanism," IEEE Wireless Communications and Networking Conference, WCNC, **2018-April**(July 2019), 1–6, 2018, doi:10.1109/WCNC.2018.8376948.

[15] M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," IEEE Internet of Things Journal, **6**(2), 2188–2204, 2019, doi:10.1109/JIOT.2018.2882794.

[16] C. Fromknecht, D. Velicanu, "A Decentralized Public Key Infrastructure with Identity Retention," Cryptology EPrint Archive, 1–16, 2014.

[17] L. Axon, Privacy-awareness in Blockchain-based PKI, 2015.

[18] D. Augot, H. Chabanne, T. Chenevier, W. George, L. Lambert, "A user-centric system for verified identities on the bitcoin blockchain," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag: 390–407, 2017, doi:10.1007/978-3-319-67816-0_22.

[19] S. Azouvi, M. Al-Bassam, S. Meiklejohn, "Who am i? Secure identity registration on distributed ledgers," Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), **10436 LNCS**, 373–389, 2017, doi:10.1007/978-3-319-67816-0_21.

[20] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, M. Sena, "Uport: a Platform for Self - Sovereign Identity 2016-09-16," 2016.

[21] R. Laborde, A. Oglaza, A.S. Wazan, F. Barrere, A. Benzekri, D.W. Chadwick, R. Venant, R. Laborde, A. Oglaza, A.S. Wazan, F. Barrere, A. Benzekri, "A User-Centric Identity Management Framework based on the W3C Verifiable Credentials and the FIDO Universal Authentication Framework To cite this version : HAL Id : hal-02930106," 2020.

[22] H. Haste, A. Bermudez, The Power of Story: Historical Narratives and the Construction of Civic Identity, Palgrave Macmillan UK: 427–447, 2017, doi:10.1057/978-1-137-52908-4_23.

[23] N. Kulabukhova, A. Ivashchenko, I. Tipikin, I. Minin, "Self-Sovereign Identity for IoT Devices," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag: 472–484, 2019, doi:10.1007/978-3-030-24296-1_37.

[24] S.T. Tempelhof, E. Teissonniere, D. Edwards, "Pangea Jurisdiction," (April), 2017.

[25] E. Hossain, W. Rahman, T. Islam, S. Hossain, "Manifesting a mobile application on safety which ascertains women salus in Bangladesh," International Journal of Electrical and Computer Engineering, **9**(5), 4355–4363, 2019, doi:10.11591/ijece.v9i5.pp4355-4363.

[26] S. Hossain, S. Waheed, Z. Rahman, S.K.A. Shezan, M. Hossain, "Blockchain for the Security of Internet of Things: A Smart Home use Case using Ethereum," International Journal of Recent Technology and Engineering, **8**(5), 4601–4608, 2020, doi:10.35940/ijrte.e6861.018520.

[27] T. Islam, S. Hossain, "Hybridization of Vigenere Technique with the Collaboration of RSA for Secure Communication," Australian Journal of Engineering and Innovative Technology, **1**(5), 6–13, 2019, doi:10.34104/ajeit.019.06013.