Blockchain-based Infrastructure for Proof of Existence in eGovernment

Alessandro Vizzarri[a]

[a]Radiolabs, Consorzio Università Industria, Laboratori di Radiocomunicazioni, Rome, Italy

Abstract

The explosion of the digital technologies is affecting several and different sectors. In this scenario the public sector has a crucial role. The eGovernment (eGov) sector has to adopt the necessary methodologies and technologies in order to enable the digital applications for the own clients, namely the citizens. A powerful data sharing together with the data integrity and the temporal traceability is strongly recommended in the public sector. This concept is an important key factor for the transparency between citizens and the public entities. In this direction the Proof of Existence (PoE) gives the possibility to certify the ownership of a specific document. The paper analyzes the different architectures for the information systems used in typical public scenarios. Peer-to-peer architectures as Bitcoin blockchains also analyzed in order to evaluate their contribution for a transparent PoE in a public context. The final conclusions remark the importance of the data integrity verification and the temporal traceability enabled by the bitcoin blockchain.

Keywords

Blockchain, eGovernament, Proof of Existence

1. Introduction

The explosion of the digital technologies is affecting several and different sectors: eHealth [1, 2], automotive [3] or energy [4, 5, 6] are the first examples of how digital applications will create an important digital ecosystem. To provide connectivity to persons and to smart objects worldwide, some telecommunication architectures have been proposed in the literature, including fixed access and ultra-dense wireless networks and satellite [7, 8]. Moreover the introduction of new technologies and electronic devices characterized by an increasingly computational power is favoring digitalization in several fields [9, 10, 11, 12, 13, 14, 15, 16, 17].

One of the most challenging applications is the public sector, whose scenario has a crucial role. The eGovernment (eGov) sector has to adopt the necessary methodologies and technologies in order to enable the digital applications for the own clients, namely the citizens [18]. This digitalization process forces the public entities to guarantee the integrity of the digital data exchanged not only with the citizens but also with other public entities. A powerful data sharing together with the data integrity and the temporal traceability is strongly recommended in the public sector. This concept is an important key factor for the transparency between citizens and the public entities. In this direction the Proof of Existence (PoE) gives the possibility to certify the ownership of a specific document. The paper presents how the bitcoin distributed architecture is useful for the PoE in a public context. The section 2 illustrates the traditional approach for information systems and the different architectures used for eGov. The section 3 describes the bitcoin blockchain technology. The section 4 analyzes a possible implementation of a blockchain-based information system for eGov applications. In the section 5 final conclusions are evidenced.

2. Traditional Approach

In the eGov context, the interaction between citizens and public entities takes place in different ways depending on the information systems and architectures that are used. By the first proprietary information systems we moved to the cloud-based information following different paradigms, as Service as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). All these information systems can be based on different architectures: centralized, decentralized and distributed scheme [19]. All of them present issues regarding security and data management. In particular, in case of a document transmission procedure or digital payments, the necessity for guaranteeing data integrity is very important [20].

SYSTEM 2020: Symposium for Young Scientists in Technology, Engineering and Mathematics, Online, May 20 2020

alessandro.vizzarri@radiolabs.it (A. Vizzarri)

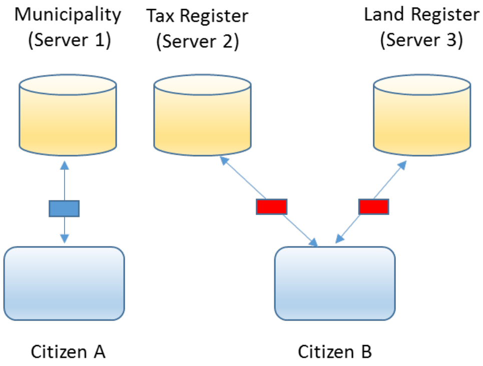


Figure 1: Centralized Information System

2.1. Centralized Information System

In a centralized information system, each client can interface with a single server for a given service [21]. As shown in Figure 1, if the citizen A needs to benefit from the services of the municipality will be connected to the dedicated server (server 1). If the citizen A needs for interaction with Tax Register (server 2) or Land Register (server 3), he has to open other sessions on different server (e.g. server 2 and server 3). In this system, the citizen A may prove the PoE only to the server 1 within the same session. In order to submit the PoE to the server 2 and to server 3, the citizen A needs to:

- connect to them
- open other sessions
- transfer the signed document

Security vulnerabilities can occur. The citizen B instead can forward the PoE to the server 2 or to the server 3 server thanks to the active sessions. Anyway, the citizen B cannot forward the PoE to the server 1. To do it, the citizen B has to open other session on the server 1. The data repository is centralized for each data type or service. Security policies are managed by a trusted third party. Since not all the servers are linked among them, the data sharing is quite difficult and it can be affected by errors. Data integrity should be guaranteed by a trusted third party. In this scenario several issues can be identified. The PoE can be altered by the citizens and the public entities. In fact, timestamp or the document can be modified. The digital identity of the citizen A can be stolen or sniffed. The e-mail notifications can be also corrupted.

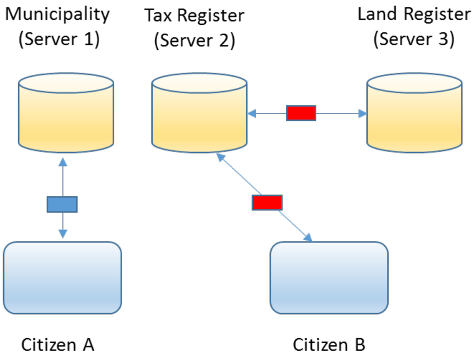


Figure 2: Decentralized Information System

2.2. Decentralized Information System

The figure 2 depicts a decentralized information system [22]. The server 2 and server 3 are linked among theme and they interact with the citizen B. The citizen A instead interacts with the server 1 because he has a municipality active session.

Server 2 and server 3 interact with each other but not with the server 1. They cannot share the data stored on the server 1. We have only a partial sharing of information: from/to server 2 to/from server 3. The security management can regard the server 2 and server 3. Server 1 can follow other policies or trusted third party certifications. The data repository is centralized for each data type or service. Security policies are managed by a trusted third party. Since not all the servers are linked among them, the data sharing is quite difficult and it can be affected by errors. Data integrity should be guaranteed by a trusted third party. In a system of this type, the citizen A is in the same situation described in the previous section. Citizen A may prove PoE only to the server with an active session. In case of PoE submission to the server 2 and server 3, citizen A needs to connect to them, to open other sessions and transfer the signed document. The citizen B can instead submit the PoE to the server 2 or to the server 3 thanks to the active session on server 2. Anyway, he cannot forward it to the server 1. In order to do it citizen B has to open a new session on it. In this scenario the same issues of the previous scenario are identified: PoE corruption, digital identity theft and alteration of e-mail notification.

2.3. Distributed Information System

In a distributed information system (Figure 3), all servers are interconnected among them. The data sharing is allowed on the basis of appropriate policies. The

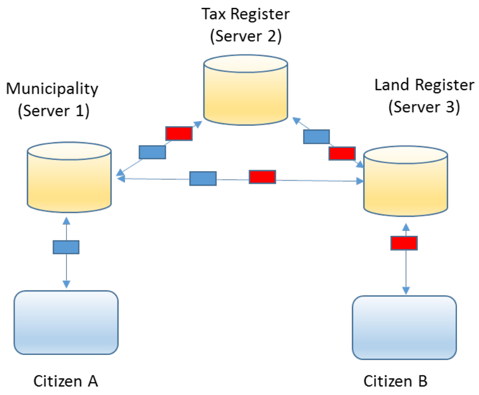


Figure 3: Distribuited Information System

client nodes can connect to one of the network servers. As shown in the figure 3, the citizen A may access the services of the municipality through the server 1. If the citizen A needs to access the other servers, the server 1 can manage the interconnections with them. The citizen B is in the same situation of the citizen A. After accessing the server 3, he can be redirected to the server 2 or server 1 for other services.

All the servers can interact among them. This enables the data sharing. Security vulnerabilities can also occur in this scenario. The PoE can be altered by the citizens and the public entities. In fact, timestamp or the document can be modified. Data integrity should be guaranteed by a trusted third party. The PoE can be altered by the citizens and the public entities. In fact, timestamp or the document can be modified. There is any possibility to prove the temporality of the actions of the data.

3. Blockchain-based approach

An alternative distributed architecture for information system can adopt a peer-to-peer scheme. All the nodes can represent either client either server (Figure 4). This scenario is well modelled by the bitcoin blockchain. It refers to a “Public Distributed Verifiable Cryptographic Ledger” [23] [24]. These important properties are defined as follows:

- Public: All participants gain the access to “read”
- Distributed: Data Communication is Peer-to-Peer and Fully Decentralized
- Asymmetric Cryptography: Public and Private Keys used for digitally signing the transactions

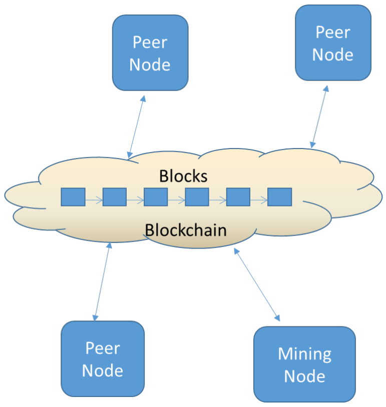


Figure 4: Blockchain Scheme

- Ledger: is a verifiable transactional database. Every peer can download locally the ledger and then hold it on a local device.

All the user nodes communicate in term of transactions exchanged among them. The technology uses ECDSA cryptography curve to authenticate and identify the nodes. Moreover, it allows the nodes to securely manage and add transactions to the ledger. The transactions are verified and confirmed by dedicated nodes (mining nodes). This implies there is no need for a central authority [25].

3.1. Wallet

When a peer wants to connect to the bitcoin blockchain, it has to download a dedicated software tool. This generates a couple of keys, a private and a public key locally, which are to be used for transactions.

- Private key: 256-bit hexadecimal number
- Public key: 130-bit hexadecimal number
- Bitcoin address: 160-bit hash of the public portion of a public/private ECDSA keypair
- Amount of bitcoin to spend

3.2. Transactions

In Bitcoin blockchain a transaction is a transfer of a kind of asset between the nodes. Assets can be cryptocurrencies as bitcoin or other non-monetary entities. Thus, is a node wants to transfer an asset to another node, a transaction has to be performed. Main parameters related to transactions are listed in the Table I. Two transaction hashes are present as references to

Size [Bytes]	Field	Description
32	Transaction Hash	Pointer to the transaction containing the Unspent Transaction Output (UTXO) to be spent
4	Transaction Hash	The index number of the UTXO to be spent; first one is 0.
1-9 (VarInt)	Unlocking-Script Size	Unlocking-Script length in bytes.
Variable	Unlocking-Script	A script that fulfills the conditions of the UTXO locking script.
4	Sequence Number	Currently disabled Tx-replacement feature, set to 0xFFFFFFFF.

Table 1

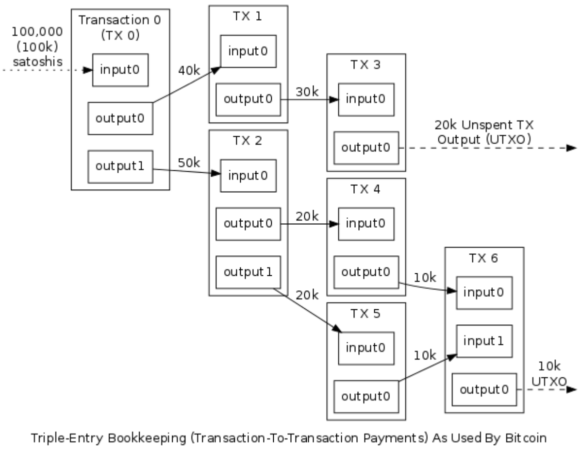
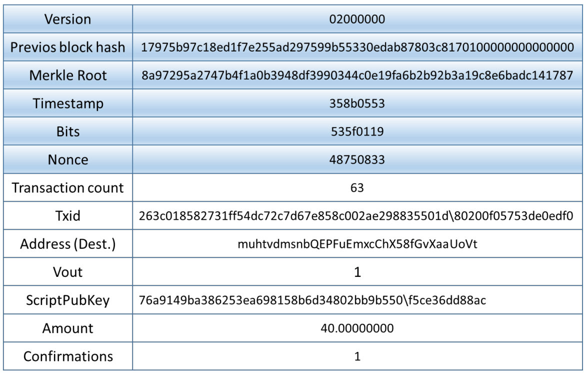


Figure 5: Example of Bitcoin Transactions

the Unspent Transaction Output (UTXO). The unlocking script is a dedicated script containing the conditions enabling the transactions between the nodes. Finally, a sequence number is present. It is a number used for updating unconfirmed time-locked transactions before their finalization. It is currently disabled. Figure 5 shows an example of bitcoin transactions.

3.3. Block Information

All transactions are included in blocks. Each block contains information of several transactions made by the nodes belonging to the blockchain. These information are globally published and distributed. As shown in the Figure 6, they mainly refer to:



Version	02000000
Previos block hash	17975b97c18ed1f7e255ad297599b55330edab87803c8170100000000000000000
Merkle Root	8a97295a2747b4f1a0b3948df3990344c0e19fa6b2b92b3a19c8e6badc141787
Timestamp	358b0553
Bits	535f0119
Nonce	48750833
Transaction count	63
Txid	263c018582731ff54dc72c7d67e858c002ae298835501d\80200f05753de0edf0
Address (Dest.)	muhtvdmsnbQEPFuEmxcChX58fGvXaaUoVt
Vout	1
ScriptPubKey	76a9149ba386253ea698158b6d34802bb9b550\f5ce36dd88ac
Amount	40.00000000
Confirmations	1

Figure 6: Information stored in the block

1. Block Header, with:
    a) Version
    b) Hash of previous block (chain)
    c) Merkle root hash of block
    d) Timestamp
    e) Bits number
    f) Nonce number
2. The sequences of signed and verified transactions
3. Transaction ID
4. Destination Bitcoin Address
5. Vout: flag value for enabling (1) or disabling (0) bitcoin spending
6. Amount of bitcon to spend. It is expresses in Satoshi units (0.00000001 Bitcoin = 1 satoshi)
7. Number of confirmations needed for validating the block
8. Number and list of transactions

3.4. Merkle root

In the bitcoin blockchain, each block of data is linked to the successive with specific criteria based on transaction hashing. When a block is validated and another block needs for validation, a Merkle Tree cryptography scheme is adopted (Figure 7). In fact, transactions ID are hashed through a double SHA (256) algorithm, as shown in Figure 7.

The result of this double hash is put into the block header as TX_root record. Prev_Hash record in the current block header is the result of the previous block hashing using SHA (256) algorithm.

This mechanism for chaining the data blocks gives the possibility to trace all the transactions between the nodes in terms of how, from-to and when an amount of bitcoin was spent.

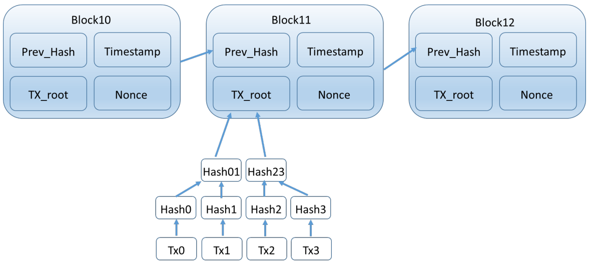


Figure 7: Merkle Root in the Bitcoin blockchain

3.5. Proof of work

When a set of transactions is put into a block, this data block has to be validated by the miner nodes. The proof of work is a set of data to hardly produce for some nodes and easily for other ones.

Bitcoin blockchain adopts the hashcash proof of work based on a partial hash inversion. A miner node must complete the proof of work requested by a specific block. The difficulty of this work is runtime adjusted in order to respect the maximum temporal interval of 10 minutes for the generation of a new block. A block is validated if its hash result is less than a target value. After a block validation, a miner node receives a reward (e.g. in bitcoin) for the completed work.

4. PoE in eGovernment Applications

Some strategies for securing data in applications concerning smart objects have been proposed in the literature [26], [27]. Nevertheless, the bitcoin blockchain, with its decentralized structure, can be very useful in the eGov scenario. The possibility of the nodes to communicate in a peer-to-peer modality is positive from a social participation point of view. Citizen and public entities are nodes of the same blockchain. They can read, write and share the same data included into the blocks. This approach can increase the citizen's trust in public authorities. The need for transparency by the citizens is an important enabler for a blockchain-based infrastructure. In the previous eGov infrastructure it is not possible by the citizens or public entities to assure the Proof-of-Work of a document and to guarantee the data integrity without the involvement of a trusted third party. In any case this cannot exclude the risk of data corruption of modification. In a peer-to-peer scheme as that provided by the bitcoin blockchain, the involvement of a trusted third party for the security certification is not necessary anymore. Citizens and public entities have the same permissions (Figure 8). In this context Municipality is the Peer 1, the Tax Register is the peer 2, the Land Register is the Peer 3, the Parking Center is the Peer 4, Citizen A is the Peer 5 and the Citizen B is the Peer 6. They can manage and share the data among them through the blockchain.

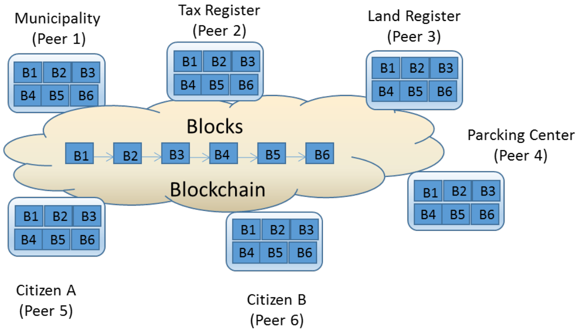


Figure 8: The Bitcoin blockchain-based approach for eGov applications

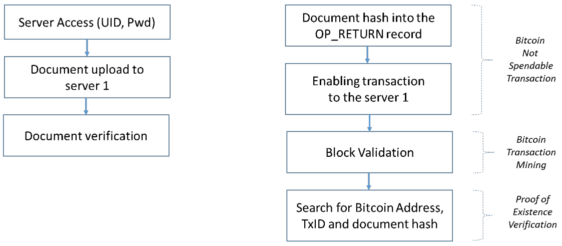

Server Access (UID, Pwd)
Document upload to server 1
Document verification
Document hash into the OP_RETURN record
Enabling transaction to the server 1
Block Validation
Search for Bitcoin Address, TxID and document hash
Bitcoin Not Spendable Transaction
Bitcoin Transaction Mining
Proof of Existence Verification

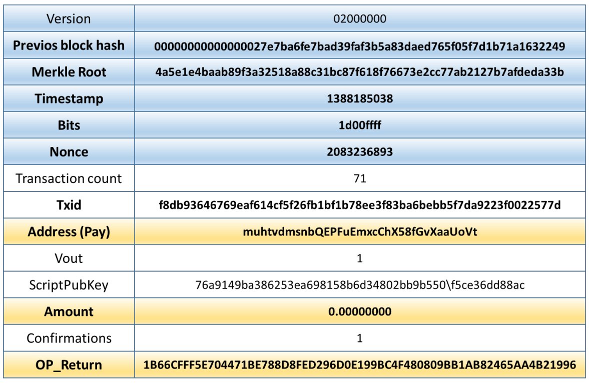
Figure 9: Workflow comparison for the two different PoE approaches. Leftmost (a) the traditional approach. Rightmost (b) the blockchain-based approach

The data exchange in the bitcoin blockchain is enabled by a specific record of a transaction called OP_ RETURN [28]. It a valid opcode used in a bitcoin not spendable transaction, which allows the insertion of a data stream with a maximum length of 80 Bytes. In this way the citizens can share the hashes of documents (e.g. SHA (256)) through the OP_RETURN opcode. The peers hold a local copy of the bitcoin ledger containing all transactions among all the nodes belonging to the blockchain. Finally, the peers manage the same wallet as defined in Section 3.

4.1. Processes

In figure 9 the two different approaches are shown: the traditional and the blockchain-based.

The traditional approach expects the document send-



Version	02000000
Previos block hash	**000000000000000027e7ba6fe7bad39faf3b5a83daed765f05f7d1b71a1632249**
Merkle Root	**4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b**
Timestamp	**1388185038**
Bits	**1d00ffff**
Nonce	**2083236893**
Transaction count	71
Txid	**f8db93646769eaf614cf5f26fb1bf1b78ee3f83ba6bebb5f7da9223f0022577d**
Address (Pay)	**muhtvdmsnbQEPFuEmxcChX58fGvXaaUoVt**
Vout	1
ScriptPubKey	76a9149ba386253ea698158b6d34802bb9b550\f5ce36dd88ac
Amount	**0.00000000**
Confirmations	1
OP_Return	**1B66CFFF5E704471BE788D8FED296D0E199BC4F480809BB1AB82465AA4B21996**

Figure 10: Block example.

ing to a specific server. The control of data integrity can be separately performed by the citizen and public entities control on own devices. Each of them can verify a data integrity that can be different from the other. With the blockchain-based approach, the citizen A can access the server 1 for municipality services. He can compute the document hash and store it into the OP_RETURN record of an unspendable bitcoin transaction. The same situation is for the citizen B. Once the not spendable transaction is confirmed, the document is officially certified and demonstrated to exist before the time the transaction was confirmed. In this way the other peers (server 2 and server 3) from public entities can verify the PoE. Within the bitcoin blockchain, they can search for the following information:

- Bitcoin Address of citizen A
- Transaction ID (TxID)
- Block height

4.2. Block information

The corresponding block is shown in Figure 10. We suppose it as the successive block of block listed in Figure 4. Not only data in the present block header are different from the previous one, but also those in the block body. Being a not spendable transaction, the corresponding amount is equal to 0.0 Satoshi. Hashes are put into the OP_RETURN of an unspendable transaction. They are included in the block.

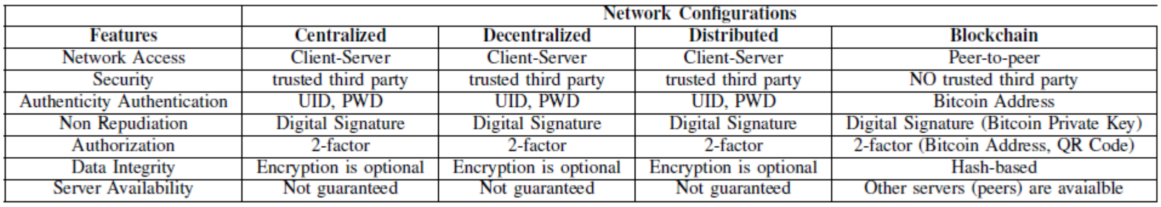
4.3. Final Comparison

Table II presents a final comparison among the previous scheme for certifying a PoE. All network configurations adopt an asymmetric cryptography based on a pair of keys (public key and private key). The previous network architectures manage services and data with the involvement of a trusted third party for the security certification. The blockchain scheme does not need it. All the nodes participate to the blockchain and guarantee themselves. They can share data with anonymity. The Bitcoin Address is used for authentication and 2-factor authorization. The other network architectures use a User ID (UID) and a Password (PWD). They can be affected by a temporary server unavailability with negative effects on services and data exchanged.

Adopting a peer-to-peer scheme, a blockchain architecture can guarantee the connection of at least one server. Anyway, each node holds locally a copy of the ledger containing all transaction information. Finally, the most important aspect is related to the data integrity and to the temporal data traceability. All timestamp stored in the blocks are linked among them. It is quite impossible to modify or corrupt a particular data block because an attacker should resolve all hashes of all the data blocks belonging to the bitcoin blockchain.

5. Conclusion

The necessity for guaranteeing the integrity of data and consequentially the PoE is an important topic for the eGov environment. This enable a major transparency and trust in the public entities by the citizens. Since the public entities will become more digitalized in the next years, the information systems have to base on reliable network infrastructures. This paper analyzed different preferred information configurations: centralized, decentralized and distributed. All of them can be affected by the risk of the data corruption. The PoE becomes crucial to certify by citizens or public entities. A blockchain-based system can be used for PoE guaranteeing thanks to its peer-to-peer scheme. Citizens and public entities can exchange hashed data stored in an option bitcoin record, the OP_RETURN. In this way the data integrity can be verified comparing the exchanged hashes. Moreover, the temporal traceability is also made possible due to the linked timestamps stored in the block headers. Next works will be focused on an experimental implementation and on innovative hashing algorithms for data integrity guaranteeing.



	Network Configurations			
Features	Centralized	Decentralized	Distributed	Blockchain
Network Access	Client-Server	Client-Server	Client-Server	Peer-to-peer
Security	trusted third party	trusted third party	trusted third party	NO trusted third party
Authenticity Authentication	UID, PWD	UID, PWD	UID, PWD	Bitcoin Address
Non Repudiation	Digital Signature	Digital Signature	Digital Signature	Digital Signature (Bitcoin Private Key)
Authorization	2-factor	2-factor	2-factor	2-factor (Bitcoin Address, QR Code)
Data Integrity	Encryption is optional	Encryption is optional	Encryption is optional	Hash-based
Server Availability	Not guaranteed	Not guaranteed	Not guaranteed	Other servers (peers) are avaialble

Table 2
Comparison

References

[1] M. Asif-Ur-Rahman, et al., Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things, IEEE Internet of Things Journal 6 (2019) 4049–4062.

[2] P. Ferroni, F. Zanzotto, N. Scarpato, A. Spila, L. Fofi, G. Egeo, A. Rullo, R. Palmirotta, P. Barbanti, F. Guadagni, Machine learning approach to predict medication overuse in migraine patients, Computational and Structural Biotechnology Journal 18 (2020) 1487.

[3] I. Benedetti, R. Giuliano, C. Lodovisi, F. Mazzenga, 5g wireless dense access network for automotive applications: Opportunities and costs, 2017 International Conference of Electrical and Electronic Technologies for Automotive, Torino (2017) 1–6.

[4] D. Bracci, S. Elia, A. Ruvio, A study on a high-reliability electromechanical undervoltage relay immersed in natural ester oil: application in mutual aid system for gensets using, Proceedings IEEE International Conference on Dielectric Liquids ICDL 2019, Roma Italy, (Jun. 2019).

[5] G. Iazeolla, A. Pieroni, A power management of server farms, Applied Mechanics and Materials 492 (2014) 453–459.

[6] C. Boccaletti, S. Elia, M. Salas, M. Pasquali, High reliability storage systems for genset cranking, Journal of Energy Storage 29 (June 2020).

[7] B. Jou, et al., Architecture options for satellite integration into 5g networks, 2018 European Conference on Networks and Communications (EuCNC), Ljubljana, Slovenia (2018) 398–399.

[8] F. Mazzenga, R. Giuliano, F. Vatalaro, Fttc-based fronthaul for 5g dense/ultra-dense access network: Performance and costs in realistic scenarios, Future Internet 9 (2017) 71.

[9] S. Spanò, G. Cardarilli, L. Di Nunzio, R. Fazzolari, D. Giardino, M. Matta, A. Nannarelli, M. Re, An efficient hardware implementation of reinforcement learning: The q-learning algorithm, IEEE Access 7 (2019) 186340–186351.

[10] C. Napoli, G. Pappalardo, E. Tramontana, R. K. Nowicki, J. T. Starczewski, M. Woźniak, Toward work groups classification based on probabilistic neural network approach, in: International Conference on Artificial Intelligence and Soft Computing, Springer, 2015, pp. 79–89.

[11] M. Wózniak, D. Połap, R. K. Nowicki, C. Napoli, G. Pappalardo, E. Tramontana, Novel approach toward medical signals classifier, in: 2015 International Joint Conference on Neural Networks (IJCNN), IEEE, 2015, pp. 1–7.

[12] D. Połap, M. Woźniak, C. Napoli, E. Tramontana, Real-time cloud-based game management system via cuckoo search algorithm, International Journal of Electronics and Telecommunications 61 (2015) 333–338.

[13] G. Capizzi, C. Napoli, L. Paternò, An innovative hybrid neuro-wavelet method for reconstruction of missing data in astronomical photometric surveys, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 7267 LNAI (2012) 21–29.

[14] G. Capizzi, G. Sciuto, C. Napoli, E. Tramontana, A multithread nested neural network architecture to model surface plasmon polaritons propagation, Micromachines 7 (2016).

[15] M. Matta, G. Cardarilli, L. Di Nunzio, R. Fazzolari, D. Giardino, A. Nannarelli, M. Re, S. Spanò, A reinforcement learning-based qam/psk symbol synchronizer, IEEE Access 7 (2019) 124147–124157.

[16] G. Capizzi, S. Coco, G. Sciuto, C. Napoli, A new iterative fir filter design approach using a gaussian approximation, IEEE Signal Processing Letters 25 (2018) 1615–1619.

[17] M. Matta, G. Cardarilli, L. Di Nunzio, R. Fazzolari, D. Giardino, M. Re, F. Silvestri, S. Spanò, Q-rts: A real-time swarm intelligence based on multi-agent q-learning, Electronics Letters 55 (2019) 589–591.

[18] M. Themistocleous, Developing e-government integrated infrastructures: A case study, in Proc. of the 38th Annual Hawaii International Conference on System Sciences, Hawaii, USA (2005) 228–234.

[19] M. Åke Hugoson, Centralized versus decentralized information systems, in Hystory of Nordic Computing 2, vol. 3, Berlin Heidelberg: Springer (2009) 106–115.

[20] S. Lim, P. Fotsing, A. Almasri, O. Musa, M. Kiah, T. Ang, R. Ismail, Blockchain technology the identity management and authentication service disruptor: A survey, International Journal on Advanced Science, Engineering and Information Technology 8 (2018) 1735–1745.

[21] B. Allen, A. Boynton, Information architecture, In: Search of Efficient Flexibility (MIS Quarterly/December 1991).

[22] C. Bacon, Organizational principles of systems decentralization, Journal of Information Technology 5 (1990).

[23] R. Fergal, An analysis of anonymity in the bitcoin system, in Proc. 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), Boston, USA (2011) 1318–1326.

[24] S. Lim, P. Fotsing, A. Almasri, O. Musa, M. Kiah, T. Ang, R. Ismail, K. Ku-Mahamud, M. Omar, N. Abu Bakar, I. Muraina, Awareness, trust, and adoption of blockchain technology and cryptocurrency among blockchain communities in malaysia, International Journal on Advanced Science, Engineering and Information Technology 9 (2019) 1217–1222.

[25] J. Bohr, Who uses bitcoin? an exploration of the bitcoin community, in Proc. 2014 Twelfth Annual International Conference on Privacy, Security and Trust (PST), Toronto, Canada (2014) 94–101.

[26] J. Dazine, M. A., L. Hassouni, Internet of things security, IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD), Marrakech, Morocco (2018) 137–141.

[27] R. Giuliano, F. Mazzenga, A. Neri, A. Vegni, Security access protocols in iot networks with heterogenous non-ip terminals, IEEE Int. Conf. on Distributed Computing in Sensor Systems (IEEE DCOSS 2014) in Int. Works. Internet of Things – Ideas and Perspectives (IoTIP-14), Marina Del Rey, CA, USA, May (2014) 257–262.

[28] M. D. Sleiman, Bitcoin message: Data insertion on a proof-of-work cryptocurrency system, in Proc. Of 2015 International Conference on Cyberworlds (CW), Visby, Sweden (2015) 332–336.