RESEARCH ARTICLE OPEN ACCESS

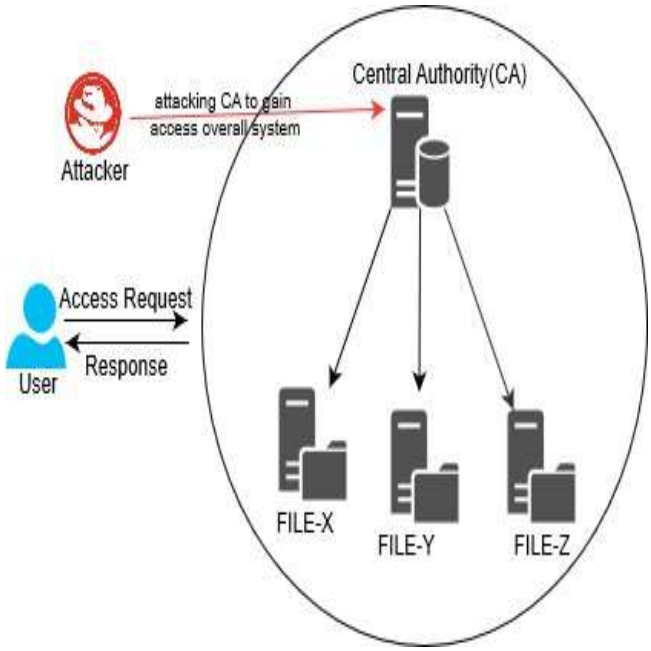
Blockchain-Blockcerts based Birth/Death Certificate Registration and Validation

Nitesh Sharma [1], Mohammad Afzal [2], Asst. Prof Ankita Dixit [3]
[1], [2], [3] Department of Computer Science and Engineering, ABES Institute of Technology - Ghaziabad

ABSTRACT
As we know that Birth/Death Certificates are very essential documents. Birth Certificate can be used as proof of an individual's age, for academics, for jobs and can be used as an identity for various government documents (Passport, Driving License, Voter-ID, etc.). Likewise, Death Certificates can be used by the family of deceased to inherit property, to claim insurance benefits and used by the government to maintain population statistics. In the current scenario, due to the complex procedure of applying and getting a certificate, nearly half of the world's population does not have a birth certificate. Also, authentication of a valid certificate is a laborious task. At the same time, due to the presence of hard copy, missing certificate becomes a crucial problem and re-issuing of that certificate is a hectic process. Presently, the digital certificate is a way to tackle the problem of missing certificates still it is not sufficient as it can tamper easily. Therefore, the objective of this paper is to give the solution to issue Birth/Death certificates and validation of certificates using Blockcerts which is based on Blockchain Technology. Blockcerts is used for issuing and verifying a blockchain-based formal transaction. Blockchain is a shared distributed, decentralized database system used to store information and this information cannot tamper easily. It also provides security services like confidentiality, authentication, integrity and access control list of data.

Keywords:- Blockchain, Blockcerts, Public/Private key cryptography, Decentralized, Shared distributed ledger, Validation, Digital Certificate, Birth/Death Certificate.

I. INTRODUCTION



Both the Birth and Death certificates have their importance. In the process of birth/death registration, an individual's birth/death gets registered in the civil record of a concerned government authority. The birth/death needs to be registered within 21 days [1]. Due to many barriers in the process of birth/death registration, almost half of the world's population does not register their birth. Furthermore, almost two-thirds of annual deaths are not registered [2]. The challenging task is to verify the Genuity of the certificate. Currently, there is a manual process to verify the authenticity of the certificates which is time-taking and lengthy. Though, there are chances of producing fake certificate which may be unnoticed by the verifier. Also, there are high chances of forgery and missing certificates as they are in hard copies.

We are using blockchain technology to remove such problems. In this way, the number of fake certificates production will be slumped [3]. Blockchain is a leading technology that provides us a secured, shared and distributed records of information. As it is not a centralized body, the decisions of mining (creation of new blocks) are made by the majority of blocks. It provides security, as the blockchain is controlled by all its members instead of a centralized authority (as in Fig. 1).

Fig. 1 Tampering in a centralized system

So, if attackers try to harm the system then they have to alter all the blocks in the system which is quite impossible as there may have millions of blocks [4] as shown in Fig.2. The information stored in blockchain will be verified by using Blockcerts. The Blockcerts is an open standard that is used to verify blockchain-based information. In the ecosystem of Blockcerts, there are four components which include generating, issuing, viewing and validating certificates over blockchain [5].

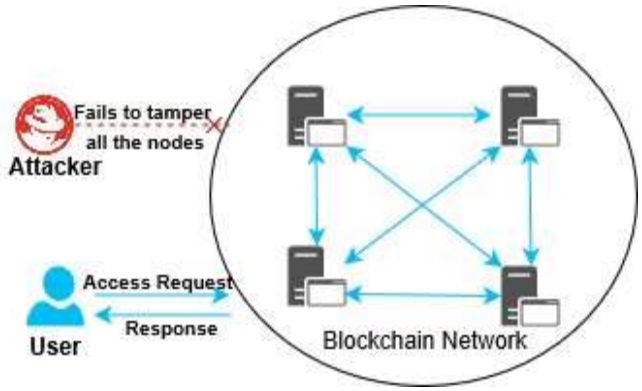


Fig. 2 Tampering in Blockchain Network

Paper Organization. The rest flow of this paper is as follows: Related work is presented in Section II, section III gives a brief introduction about Blockchain Technology and its characteristics, section IV describes about public/private key cryptography with an example, section V defines the concept of Blockcerts, section VI gives the idea about certification process using Blockchain technology and Blockcerts application and section VII contains the conclusion of this paper.

II. RELATED WORK

With the advancement in the field of Blockchain Technology, researchers have proposed many survey papers based on the advantages of this technology in several fields like Privacy & Identity, Security Services, Verification, Tampering and other survey-based on Blockchain include Healthcare, Cryptocurrency, etc.

A. Conceptual Blockchain-Based Surveys

Tara Salman, Maede Zolanvari and Aiman Erbad [4] present various security services like confidentiality, integrity, availability, and authentication. In their survey, they explain how the Blockchain-based system is more preferable to a traditional centralized system in the context of services. Shixiong Yao, Jing Chen, and Kun He [6] define how to preserve the privacy using the Blockchain approach in which they explain to store the necessary information (name, hash value, and other related operation) in blockchain and it utilizes another secondary storage for detailed information about certificates. And also, to deal with an unclear query regarding certificate status, thus preserving the privacy.

Nitin Kumavat, Swapnil Mengade, Dishant Desai [3] describes to tackle the problem of fake certificate and verify the authenticity of certificates. In their survey, they describe the manual process of verifying the certificate. And they are solving this problem by storing digital certificates in Blockchain which makes the verification task easier and there are fewer chances of producing a fake certificate.

Maharshi Shah, Priyanka Kumar [7] gives the theoretical concept about an unmodifiable digital birth certificate. In their survey, they use PKI (public key infrastructure) to validate the integrity of the certificate.

B. Differentiating our research work from related work

This paper describes the model in which we are using the concept of Blockcerts to build the application which will generate the Birth/Death certificate based on the information stored in the blockchain. Furthermore, the verification of the certificate will be done by using the concept of public/private key cryptography. The generated certificate will be stored in the blockchain as a new transaction. The stored certificate can be easily validated and retrieved whenever required. This is how we will remove the problem of a fake and missing certificate.

III. BACKGROUND OF BLOCKCHAIN TECHNOLOGY AND ITS CHARACTERISTICS

Blockchain was developed in 2008 [8] by an anonymous person commonly known as Satoshi Nakamoto to deal with the digital transaction. The first application of blockchain was bitcoin cryptocurrency which becomes the first blockchain-based digital currency [9]. The main idea behind the implementation of digital currency is to make the transaction secure. It is a shared, distributed, a decentralized database consists of the growing chain of records called ‘Blocks’. These Blocks are connected through a cryptographic technique securely. Each block having a hash value of the previous block along with its hash value as shown in fig.3. Also, contain a timestamp and several valid transactional details in form of Merkle Tree as shown in fig.4.

The creation of a new block in a current growing blockchain is known as mining. The various mining technique includes Proof of Work (PoW), Proof of Stake (PoS), Proof of space (PoSpace), Proof of Importance (PoI), Measure of Trust (MoT), Minimum Block Hash and Practical Byzantine Fault Tolerance [4].

Proof of work is a reward-based mining technique that is used by most of the application of blockchain like bitcoin. In this technique, the miner will have to solve the high computational mathematical puzzle and should be agreed by all the miners before adding a new block in the blockchain. As a result, the miner will be rewarded [10].

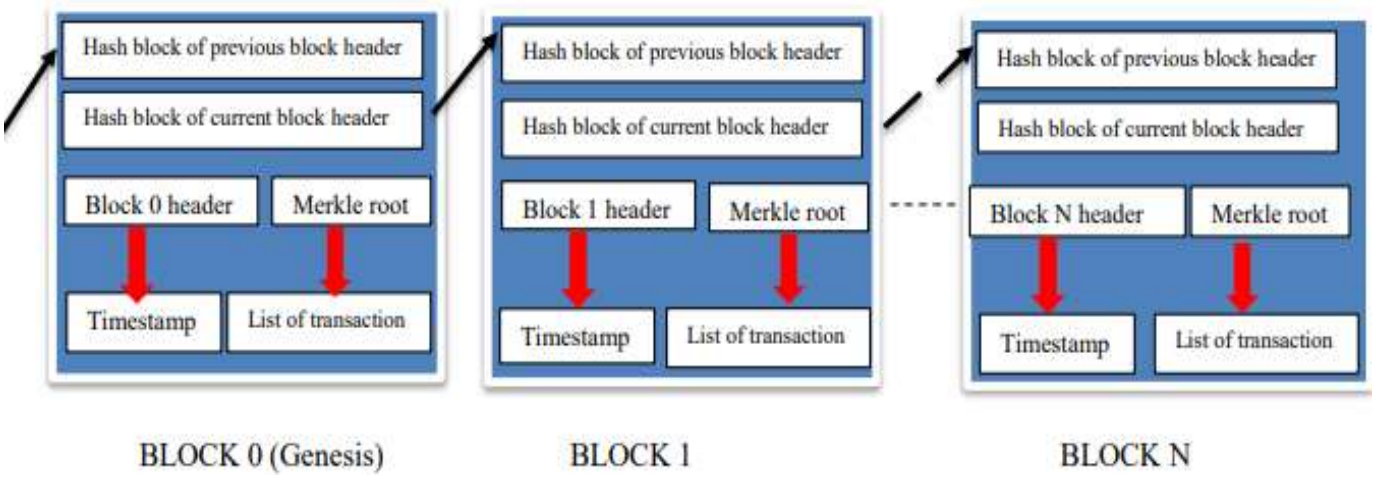


Fig. 3 Structure of Blockchain

Proof of Stake is not a reward-based mining technique. This technique is used by Ethereum. In this technique, we do not need to solve a mathematical puzzle-like in PoW. Thus, PoS saves computational energy. In PoS, the miner who will add a new block will be selected at random basis depending upon their stake(wealth). More the stake a particular miner has more will be the chances to be chosen [11].

Proof of Space is also not based on rewards. PoSpace is almost similar to PoW. The only difference, PoW uses computation power and PoSpace uses storage. Now, the miner does not need to have high computational power, they just need to allocate storage for mining purpose. Comparatively PoSpace require low cost than PoW [12].

Minimum Hash Block is a mining technique that is used in the implementation of an extended version of bitcoin. In this technique, the miner will be selected based on the minimum hash value in the complete blockchain [13].

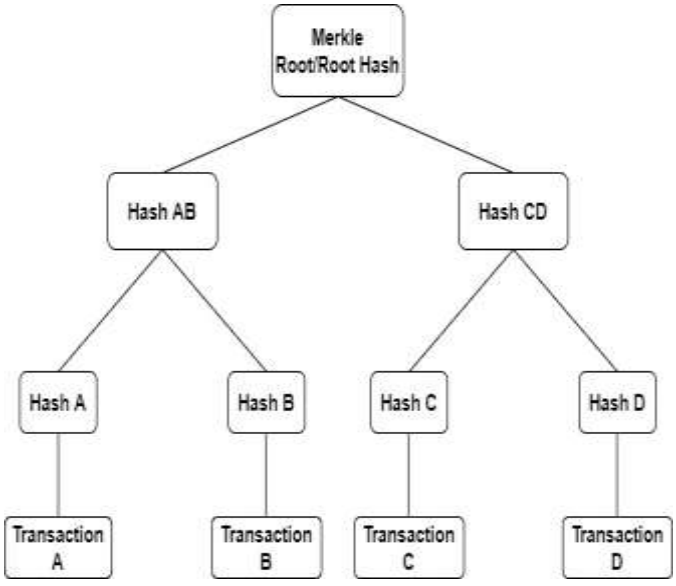


Fig. 4: An Example of Merkle Tree

Comparison: In Table 1, there is a comparison between all the mining techniques which is based on Assets required, their application and rewards.

S.No	Mining Technique	Assets Required	Application	Reward-based
1.	Proof of Work	High computational Power	Bitcoin	Yes
2.	Proof of Stake	Wealth or Stake	Ethereum	No
3.	Proof of Space	High Storage	SpaceMint	Yes
4.	Proof of Importance	Node Importance	Nem	Yes
5.	Measure of Trust	Trust Value	Not implemented	Yes
6.	Minimum hash block	Minimum Hash Value	Bitcoin (modified)	Yes

TABLE I
Comparison between Different Mining Techniques

A. Characteristics of Blockchain

The blockchain technology has the following key characteristics:

- **Decentralized Technology:** In centralized transactions model, all the transaction needs to be permitted by the single central body whereas in blockchain network the transactions are performed in Peer-to-Peer manner that's mean two nodes communicate directly with each other [16] as shown in Fig. 1 and Fig.2.
- **Cannot be corrupted:** In blockchain network there are several nodes and each node have a replica of the valid ledger. The new transaction can only be added when the majority of the nodes will be agreed on that

transaction. In this way, we can achieve a corruption free network and avoid invalid transactions [16].

- **Distributed Ledger:** In the blockchain network, all the resources are distributed among all sites of the blockchain, there is no single central database to store the resources [17].
- **Enhance Security:** Each block in the blockchain have a hash value and also contains the hash value of the previous block, if an attacker wants to tamper the block then he has to tamper all the block which is quite impossible. Another aspect of enhancing security in the blockchain is asymmetric cryptography.
- **Consensus:** In the blockchain network the set of nodes are responsible for the addition of new block in the blockchain, these set of nodes are selected based on various consensus algorithm such as PoW, PoS, MoT, etc. As explained in Table 1 [18].

IV. PUBLIC/PRIVATE KEY CRYPTOGRAPHY IN BLOCKCHAIN

Cryptography is a method of securing data confidentiality from unauthorized persons. For cryptography, we have to perform the following operation: Encryption and Decryption. Blockchain uses public key cryptography techniques to secure transactions, preserve user privacy and maintains data integrity. The public key cryptography uses two types of key: a public key and private key. A public key is distributed publicly over a network and can be used by anyone in the network whereas the private key is kept confidential by the user. Every user has its pair of keys (Public key and its corresponding Private key) [14].

Encryption in Blockchain Technology

Encryption is a technique in which the normal text is transformed into an unreadable form. In Blockchain, we use a hashing encryption algorithm to encrypt the information. So, if any malicious user tries to access the information then the information will be of no use as the information is in the encrypted form. The hashing encryption algorithm uses the public key to encrypt the information that can only be decrypted using the corresponding private key. The most common applications of blockchain technology are Bitcoin and Ethereum which are using SHA256 and KECCAK256 encryption algorithm respectively [14].

Digital Signature

The digital signature is used to verify the authenticity of a digital document. It is used to prove that the specific information belongs to the sender who has made the digital signature [16]. It involves two parts, the signing part, and the verification part. In signing part, the sender will sign the document using its private key. The digitally signed document will be broadcasted over the whole blockchain network which is accessible by everyone. In the second part, the receiver can verify a digitally signed document by using the sender's public key [16].

Decryption in Blockchain Technology

Decryption is a technique in which encrypted information is taken and converted into its original form by using a corresponding private key.

Let's take an example of Public/Private key cryptography as shown in Fig. 5. In this figure, Jack wants to send a digital document to John. So, Jack will use John's public key to encrypt the digital document and digitally sign the document by using its private key. Then Jack sends a digitally signed and encrypted document to John over the blockchain network. In between, no one can read the document because it is in the encrypted form. Now, John will use its private key to decrypt the encrypted document and validate the same document by using Jack's public key.

V. BLOCKCERTS

A. Foundation of Blockcerts

The concept of Blockcerts initiated by the MIT media lab. MIT media lab is a research laboratory at the Massachusetts Institute of Technology [19]. A team of researchers at MIT media lab gives the concept of Blockcerts during their research project led by Philipp Schmidt and Juliana Nazare along with many other professors. They collaborated with Learning Machine which is a software company at Cambridge to develop Blockcerts [20]. The need to introduce Blockcerts was to provide the student with a way of storing and verifying their credentials securely. Blockcerts also allow employers of the company to instantly validate the credentials of the student to prove their skills and proprietary.

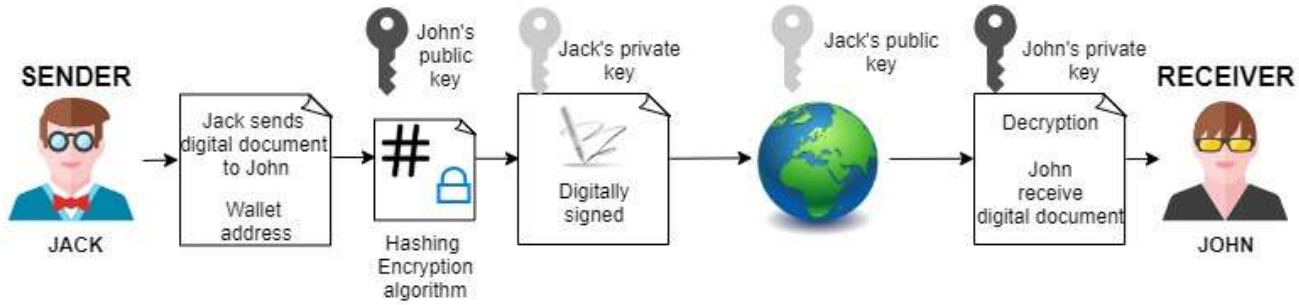


Fig. 5: An example of public/private key cryptography

Blockcerts can also be considered as metamorphic technology for those who have lost their credentials in some kind of disaster (can be a natural disaster, a situation of war). Due to these kinds of disasters, we have a situation of credentials missing, in that case, we are dependent on our universities which may don't exist or do not store our credentials for a longer time [21]. Hence, Blockcerts can help to get rid of these problems.

"I don't believe in one central body having ownership over the digital record of people's learning,"

- Philipp Schmidt [21].

Initially, the Blockcerts was taken as an experiment in which 619 MIT students can receive their diploma in digital form. Students were guided in such a way, to download Blockcerts Application and add MIT as an issuer.

"Before graduation, MIT sends the students an invite e-mail, which says 'Hey, go download the Blockcerts Wallet app, accept the pass phrase, and add MIT as an issuer,'"

-Chris Jagers [21].

After the course completion, MIT sends an email containing a digital certificate and ask the students to upload the certificate into Blockcerts application. Then the application sends that certificate to all the nodes in the blockchain. Moreover, blocks containing information about certificates created and verified by nodes. After that, the blocks are added to the existing blockchain which can be accessed by the student using its private key [21] as explained in fig.5.

B. Working of Blockcerts and its components

Blockcerts is an open infrastructure for the generation and validation of blockchain-based credentials. Blockcerts can be used to issue many kinds of certificates and identity documents in Government or Private sectors.

Components of Blockcerts

There are four components of Blockcerts which include Issuer, Certificate, Verifier and Blockcerts wallet application as discussed below [20]:

- **Issuer:** Issuer can be a university, governmental authority or any other organization that will issue or create a certificate by using recipient public key and digitally sign the certificate by using their private key.
- **Certificate:** Certificates are nothing but a digitally signed document that contains proof of an individual's skills and achievements.
- **Verifier:** Verifier can be anyone who will verify that the certificate has not tampered, issued by the particular authority and issued to a particular recipient
- **Wallet Application:** This is a platform where the recipient can securely store their certificate and can easily share it with anyone.

Working of Blockcerts

As we have discussed above the components of Blockcerts, all the components have their work in the process of certification. Let's take an overview of generating a birth certificate in which we have Government Authority (GA) as issuer, a recipient and a verifier as shown in fig.6.

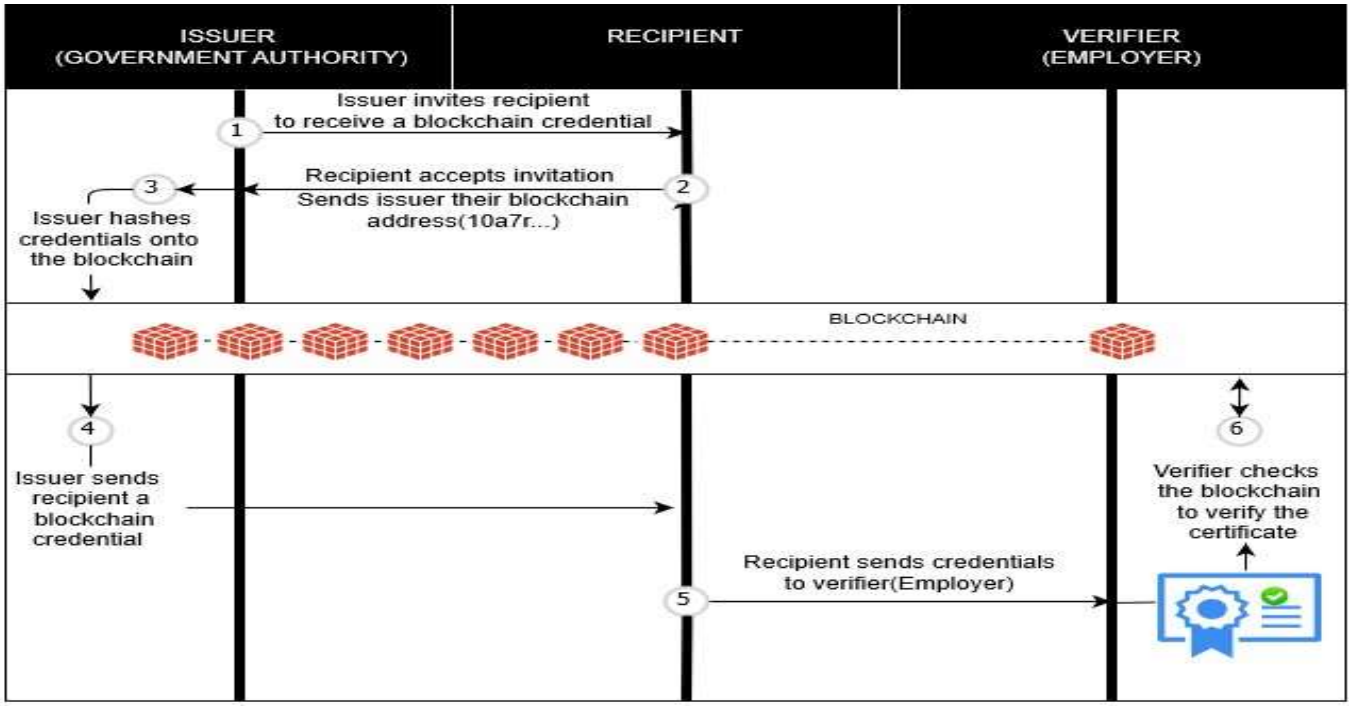


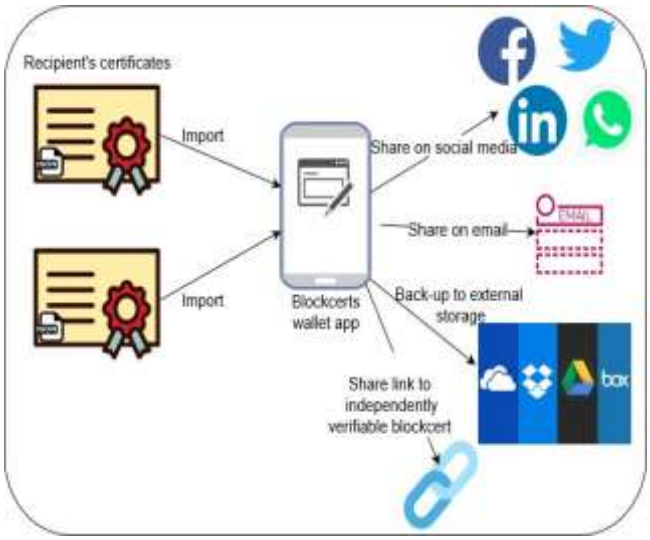
Fig. 6: Workflow of Blockcerts [5]

ISSUING: GA will issue a digital certificate on blockchain for that, there will be the following steps:

- The GA will create a JSON file from the information provided to GA concerning certificate (which will contain recipient Name, DOB, name of the issuer, etc.).
- GA has its Blockchain address (pair of public /private key). The GA will Digitally Sign the certificate using its own Private Key. So, the point of origin can be verified and will encrypt the JSON created using an encryption algorithm (SHA-256).
- Now, GA will invite the recipient to receive the blockchain credential. The recipient will accept the invitation and will share its blockchain address.
- Then the GA will perform a blockchain transaction from their address to recipient address by using the recipient's public key and send the blockchain credentials to the recipient.
- The recipient will use its private key to decrypt the JSON file to read it.

VERIFYING: Here comes another component of Blockcerts which is verifier. The blockchain certificates are sharable as shown in fig-7. Let suppose the recipient shares the certificate along with transaction details to the third person, then that third person will play the role of the verifier. Now, the verifier will be able to verify the certificate provided by the recipient that the certificate present on the blockchain is the same or not. The verification can be done by uploading a JSON certificate on Blockcerts application.

Fig. 7: Shareability of blockchain-based certificate



VI. CERTIFICATION PROCESS USING BLOCKCHAIN TECHNOLOGY AND BLOCKCERTS APPLICATION

In figure 8, the working of blockchain is explained for the certification process. There are mainly six steps in the overall process of certification. In the first step, the user will provide the details and legit documents that are generally required in the process of birth/death certification respectively. In the second step, a block will be created which contains relevant information regarding the certificate. Now, this block will be broadcasted to every node in the blockchain. Then, in the fourth step, all the nodes will validate the details provided by the user in the first step. After validation new block is added to the existing verified blockchain. At last, the certification process is completed by using Blockcerts.

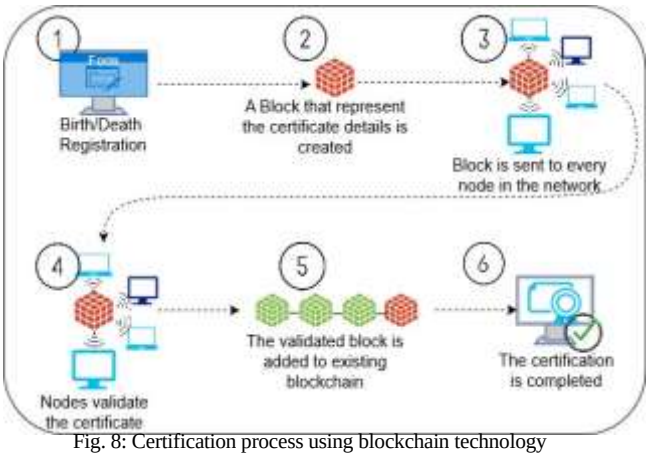


Fig. 8: Certification process using blockchain technology

VII. RESULT AND DISCUSSION

To generate the certificate based on Blockchain Technology, the user will be going to register their selves on our application built using Blockcerts, the generation of the certificate will be based on public/private key cryptography using hashing algorithms, which adds an amazing level of security in certificate generation.

The Blockchain-based certificate can be validated using Blockcerts application any time anywhere in the world which results in the decreasing of tempering of certificates. Hence numerous numbers of problems will be solved using this approach to generate the certificate.

VIII. CONCLUSION

In this paper, we presented a solution that will replace the conventional approach of birth/death certificate generation. We have used blockchain technology and Blockcerts in the process of birth/death certification and validation. The solution includes registration of birth/death, creation of JSON file (digital certificate), public-private key cryptography to achieve confidentiality using encryption and digital signature.

Moreover, the retrieval of certificates in case of certificate missing can be done easily. Furthermore, we have discussed the concept of Blockcerts, the shareability of certificate, working of blockchain technology in the process of certification. We have also discussed the key features of blockchain technology which will provide the new way of generating birth/death certificate and its validation.

REFERENCES

[1] Swagata Yadavar, Disha Shetty, "Birth Certificates Are Citizenship Proof, Govt Says. But 38% Under-5 Children Don't Have One" ,[online] Available: https://www.indiaspend.com/birth-certificates-are-citizenship-proof-govt-says-but-38-under-5-children-dont-have-one/ (accessed January 6, 2020).

[2] WHO, "Civil registration: why counting births and deaths is important", [online] Available: https://www.who.int/news-room/fact-sheets/detail/civil-registration-why-counting-births-and-deaths-is-important/ (accessed November 20, 2019).

[3] Nitin Kumavat, Swapnil Mengade, Dishant Desai, Jesal Varolia," Certificate Verification System using Blockchain," IJRASET, Volume 7, pp. 53-57, Apr 2019.

[4] Tara Salman, Maeda Zolanvari, Aiman Erbad, Raj Jain, Mohammed Samaka" Security Services using Blockchain: A State of the Art Survey," IEEE, Volume 21, pp. 1-23, 2019.

[5] Blockcerts, "Blockcerts: Introduction", [online] Available: https://www.blockcerts.org/guide/ (accessed December 5, 2019).

[6] Shixiong Yao, Jing Chen, Kun He, Ruiying Du, Tianqing Zhu, and Xin Chen "PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management," IEEE Access, Vol. 7, pp. 6117-6128, 27 December 2018.

[7] Maharshi Shah, Priyanka Kumar "Tamper Proof Birth Certificate Using Blockchain Technology," IJRTE, Vol.7, pp. 95-98, February 2019.

[8] Wikipedia," Blockchain", [online] Available: https://en.wikipedia.org/wiki/Blockchain (accessed December 15, 2019).

[9] Peng Zhang, Jules White, Douglas C.Schmidt, Gunther Lenz, S.Trent Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," ELSEVIER, Vol. 16, pp. 267-278, 2018.

[10] Bitcoinwiki, "Proof of Work", [online] Available: https://en.bitcoin.it/wiki/Proof_of_work, (accessed December 25, 2019).

[11] Wikipedia, "Proof of Stake", [online] Available: https://en.wikipedia.org/wiki/Proof_of_stake, (accessed December 25, 2019).

[12] Wikipedia, "Proof of Space", [online] Available: https://en.wikipedia.org/wiki/Proof_of_space, (accessed December 27, 2019).

[13] G. Paul, P. Sarkar, and S. Mukherjee, "Towards a more democratic mining in bitcoins," in 10th International Conference on Information Systems Security (ICISS'14), Dec. 2014, pp. 185-203.

[14] Victor Lai, "INTRODUCTION TO CRYPTOGRAPHY IN BLOCKCHAIN TECHNOLOGY", [online] Available: https://crushcrypto.com/cryptography-in-blockchain/ (accessed December 27, 2019).

[15] Noe Elise, Longzhi Yang, Fei Chao, Yi Cao, "A Framework of blockchain-based secure and privacy-preserving E-government system," Springer US, pp. 1-11, 03 December 2018.

[16] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang, "Blockchain challenges and opportunities: a survey," Int, J, Web and Grid Services, Vol. 14, pp. 352-375, 2018.

[17] Wikipedia, "Distributed Ledger", [online] Available: https://en.wikipedia.org/wiki/Distributed_ledger, (accessed December 30, 2019).

[18] Hasib Anwar, "Basic Features of Blockchain Technology", [online] Available: https://101blockchains.com/introduction-to-blockchain-features/ (accessed December 31, 2019).

[19] Wikipedia, "MIT Media Lab", [online] Available: https://en.wikipedia.org/wiki/MIT_Media_Lab, (accessed January 2, 2020).

[20] Philipp Schmidt, "Blockcerts — An Open Infrastructure for Academic Credentials on the Blockchain", [online] Available: https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for-academic-credentials-on-the-blockchain-899a6b880b2f, (accessed January 2, 2020).

[21] Frankie Schembri, SM '18, "Digital diplomas Blockchain technology gives grads control over their academic credentials.", [online] Available: https://www.technologyreview.com/s/610818/digital-diplomas/, (accessed January 3, 2020).