IBIMA Publishing
Journal of Software & Systems Development
http://ibimapublishing.com/articles/JSSD/2018/370695/
Vol. 2018 (2018), Article ID 370695, 14 pages
DOI: 10.5171/2018.370695

Research Article

Zenith Certifier: A Framework to Authenticate Academic Verifications Using Tangle

Abdul Wahab, Mahad Barlas and Waqas Mahmood

Faculty of Computer Science, Institute of Business Administration, Karachi, Pakistan

Correspondence should be addressed to: Mahad Barlas; mahadbarlas@gmail.com

Received date: 9 October 2017; Accepted date: 26 November 2017; Published date: 24 May 2018

Academic Editor: Mohammad Faisal

Abstract

The Blockchain technology has witnessed a boost in adaptability with respect to its application especially in distributed public ledgers dealing in the financial and academic sectors. However, the major drawbacks of this technology cause hindrance for sustaining in a longer run. Which is why applications solely built on Blockchain might also witness a decrease in their adaptability. Tangle, on the other hand, provides a more suitable and reliable system which also addresses the drawbacks of Blockchain.In this paper, we propose a framework to authenticate academic degrees and certificates built on Tangle so that the intermediate and middle parties which verify the transaction or data are eliminated, having a decentralized control with complete visibility to all the actors involved in the system. Additionally, Tangle provides a quantum resistant security mechanism and a highly scalable architecture.

Keywords: Blockchain; Tangle; Digital Certificate; Academic Verification

Introduction

Every industry is experiencing digital transformations and disruptive technologies that are emerging to fulfill the current business processes with a new dimension. Likewise, the education industry is also witnessing solutions to digitalize degrees and certifications to make it easier for the institutions and the employers to authenticate those documents with minimal effort. Moreover, since all records are precious in nature, therefore, they should be stored permanently without being ever altered. BlockCert, an application built on Blockchain caters these needs and proposes a solution to make it easier to validate the academic documents. However, the drawbacks of Blockchain make it difficult to implement it in the developing countries.

Cite this Article as: Abdul Wahab, Mahad Barlas and Waqas Mahmood (2018), " Zenith Certifier: A Framework to Authenticate Academic Verifications Using Tangle ", Journal of Software & Systems Development, Vol. 2018 (2018), Article ID 370695, DOI: 10.5171/2018.370695

In this paper, we propose our solution; Zenith Certifier, which would enable the academic industry to publish documents and facilitate the employers using Tangle.

This paper is organized as follows: In Section II, we state the background and challenges of Blockchain and Tangle. In Section III, we focus on the current state of the art of this technology and its drawbacks respectively. In Section IV, we present the Zenith Certifier framework. Furthermore, in Section V, we provide our critical analysis. Finally, in Section VI, we conclude the paper and also provide the future scope.

Challenges

In this competitive world, competition has put each person in a race of getting as many degrees and certificates as possible, this has led to a more advanced but complicated environment. With several degrees and certificates, one has to go through the process of verification and attestation a couple of times until all the prior documents are formally attested by the concerned regulatory / authority. Mostly, such cases are witnessed in the underdeveloped countries where paper-based degrees/certificates are common. Following are the most common problems which are experienced in such paper-based certificate system:

- The probability of fraudulence is very high as numerous certificates are issued by several different institutions. These certificates are always at risk of being challenged for their authenticity as fake physical documents are easily producible.
- Using paper-based certificates is always difficult to preserve and use in later stages of life. When applying for a new job or for pursuing a higher degree, these certificates are needed to be provided which becomes a challenge, given that the chances of losing such physical documents are much higher. Two of the major challenges in this current process are; the long time it consumes and the high risk of losing the original documents during the attestation process. Thus, the process is modeled in such a way that each attestation has to go through the same set of activities.
- The regulators do not maintain any database on their own and always rely on the institute itself for the verification of the documents. Hence, there is a lack of ownership by the central authority.

Contrary to this paper-based approach the developed countries use various information management systems to cater the needs of certificate issuance and verification. However, they too face certain challenges which are as follows:

- Each region follows its own standard which creates hindrance at the time of creating an equivalency of a certificate issued from a different region of the globe. Likewise, the distinct systems face integration issues where such problems related to certificate format are encountered.
- A single point of failure within an institute's database can make the whole system malfunction since there would be no way to recover the original records with complete integrity. Additionally, since the data is centralized, there are numerous chances of being compromised at the hands of hackers.

The adaptation is yet always a major milestone once a technology has been introduced. Multiple factors such as cost, space, geography, and mindset are needed to be considered before a technology can be implemented. Currently, the developed countries use many different types of solutions depending on the size of the institute i.e. ERP, small-scale web and desktop based systems. Among ERP, PeopleSoft and other local solutions are very common, they are tailored to the needs of the institutions but they are very costly. Fedena is another web-based small-scale management system for schools and colleges. It is relatively affordable for small institutions but provides the least customization.

The recent development in this domain is a Blockchain based system, which is a distributed ledger known as BlockCert (Blockcert Organization, 2017). It proposes a brilliant architecture and open source code for the early adopter to experience its model. But since its architecture is built upon Blockchain, the risks associated with this technology have a high impact on the core application. Many institutions in the developed region have migrated to distributed solutions as they avoid a single point of failure and centralization of data, but the cost of migrations and operating such systems are very high.

These above issues highlight the need for a system that is both affordable for an underdeveloped country and acceptable by a developed country. The success of the solution will be compared against cost, scalability, and security, where our goal will be to minimize the cost and maximize the scalability and security. Tangle, a distributed technology, fulfills these promises as it provides a platform for secure, distributed and affordable solution (Popov, 2016).

Literature Review

The prior section of this research paper discusses the background and the challenges that the education industry experiences. This section discusses the current state of the art technologies which are being used to cater its requirements or have the potential to be used to design a system which can encounter all the major challenges. The Blockchain has been in the market for a couple of years now which function on the distributed ledger architecture. Various frameworks have also been developed using the principles of Blockchain with slight variations such as Private Chain and Ethereum. BlockCert is the most recent solution inheriting the scalability and performance issues of the Blockchain, which is the underlying technology of the system. We will critically analyze the impact and severity of these issues. We would then introduce and analyze Tangle, a recent innovation, which is considered a much better technology than Blockchain because of the features it has which outweighs the drawbacks of Blockchain.

Blockchain

Blockchain has been gaining popularity especially after its adoption by the famous application of cryptocurrency model, Bitcoin (Frank van de Ven, 2017). It has shown a lot of potentials for transforming business processes completely by linking all the concerned actors through a smart contract. Many researchers from all over the world have presented their ideas for implementing Blockchain in various business processes. Scenarios like global passports, healthcare management, warranty management and education are certain domains where a lot of research has been in progress (Blockcert Organization, 2017). However, it has various disadvantages as well which have been discussed in the sections below.

Major Issues

Following are some of the issues identified by different authorities and researchers related to building a technology solution using Blockchain:

Legality: Although more and more countries have started to recognize Bitcoin as a decentralized currency, there are still serious concerns about its legality in USA, Iceland and other countries. Due to its decentralized nature, it cannot be regularized by any authority which makes it very likely to be used for money laundering and illegal purchase of illicit goods (BTC Media LLC, n.d.). India and China have cracked down many illegal activities using Bitcoin-Blockchain. Countries including Canada and

Israel are still uncertain of its adoption (Cawrey, 2014).

If the authorities decide to shut down their network, all the framework and programs built on the top of it will be affected and may terminate because the transaction of any sort in Blockchain involves Bitcoin. A developing country usually follows the rules and policies laid out by the developed player of the financial market, so it is very risky to adopt Bitcoin-Blockchain based system.

Resource Intensive: The Blockchain has increased in resources and complexity over the time. The size of the ledger is also growing proportionally, which requires you to free up space in GBs (Malanov, 2017). The developing countries would require the infrastructure to setup the system which might turn out to be very costly for them.

The average time for a transaction to enter into the network is approximately 10 minutes, and it is common to wait for an hour before a transaction appears on the ledger. The increasing competition among the mining pools has increased the complexity of mining a transaction by 400% in last few months, and only a few huge mining pools dominate the mining market (Cawrey, 2014). The reason for increased complexity is the competition among the mining pools, to beat each other they invest heavily in hardware and software to increase mining speed, which in turn raises the complexity to maintain the transaction time near to 10 minutes. The problem lies when a large portion of these mining pools withdraws from mining, the transaction may take up to several hours to be mined since the majority of the miners do not have that infrastructure for mining within average 10 minutes. Altogether, this can affect the overall throughput of the system.

Statistics show that the majority of the mining networks are based in China and control more than 50% of the mining network. This polarization in control over the network not only brings in danger of the political centralization but also gives these pools the power to exploit the authenticity of the data (Malanov, 2017). This could lead to a potential loophole for generating fake academic credentials and will make the whole system vulnerable.

Obsolete Security: The Blockchain has several security issues, despite the efforts of the community to make it stable and secure. The major challenges, such as Double Spending, 51% Attack, Selfish Mining and Time-jacking Attacks, are common to most of the cryptocurrencies (Chinmay & Munindra, 2014). One major threat to the Blockchain is its incapability to resist a large-scale quantum attack. Nowadays, quantum computers are emerging rapidly; hence, the survival of Blockchain apparently is at stake (Marchenkova, 2015).

Increasing Transaction Fee: Every transaction in Blockchain is carried out with a fee, which ranges drastically. Due to the high volume of transactions and limited resources, the miner prioritizes the transaction on the basis of high transaction fee (Schroeder, 2017). The developing countries can barely afford to pay the variable transaction fee to register academic artifacts in the system. This inconsistent behavior makes this system financially unreliable and the developing countries might not be able to afford it.

One such example of a developing country can be taken of Pakistan, where people have to get their degrees attested from the central regulator; The Higher Education Commission (HEC), which requires all the prior original educational documents to be submitted for each and every attestation. This is applicable even when an applicant has already got prior degrees attested and wishes to attest the new ones, the requirement to submit all the previous original documents remains unaltered.

Hence, by looking at all the aforementioned points it seems difficult to build an education system based solely on the Blockchain technology. This is why BlockCert is difficult to implement in the developing countries.

Other Variants of the Blockchain

Private Chain

Private Chain is much like shared databases as they have permission-based architecture and accessibility to a limited audience. It is widely accepted by the financial institutions where the data must be accessible to only allowed personnel, also called the whitelisted users (Pilkington, 2016). The permission architecture also compromises the security as the authorized user is allowed to insert new records into the system.

This appears to be a poor fit for our approach where security and accessibility are top priority. Our system will be accessible by students, also known as recipients, who if gained the unauthorized access or under the influence of the management, can put fake records.

Ethereum

Ethereum is a decentralized cryptocurrency which has its own built-in currency named Ether. The smart contracts are programmable and they rely on the Blockchain which is considered to be an evolved version of Bitcoin (Delmolino, et al., 2015). It is a public Blockchain which still carries the limitations of Blockchain, as discussed in the previous sections. It is relatively simpler and highly programmable (Anon., n.d.). These features make it more prone to hacking and less robust in nature, thus making it less secure (Jagers, 2016).

Private Chain is still a nascent technology and requires further maturity. The smart contracts and Ether are easily programmable, that makes it simple but vulnerable to programming mistakes of both natures, intentional and unintentional. That is someone can exploit the behavior of the chain or create a backdoor if one wants to exploit it intentionally.

Tangle

Another architecture existing in the same domain of Internet of Things (IoT) is Tangle which is a distributed ledger technology built on Directed Acyclic Graph (DAG) (Popov, 2016). It is the most demanding evolution of the existing technology as it addresses the potential drawbacks of Blockchain-based variants.

Application

The major application of Tangle is IOTA which is termed as the next generation of cryptocurrency. It provides a no-fee transaction model for conducting micropayments in IoT. The number of upcoming devices associated with IoT is increasing exponentially and it is estimated to reach 50 billion by the next decade (Evans, 2011). IOTA has the potential to seamlessly conduct the micropayments across these devices without compromising on the product design.

Features

The underlying technology, Directed Acyclic Graph, is a distinct architecture that enables it to retain all the features of the Blockchain, distributed ledger, and secure transaction, without using the block-based strategy. Instead, it is based on a graph-based data structure with nodes or vertices representing each transaction, keeping the salient features of the technology, which are ideal for our use case (Popov, 2016).

Zero Transaction Fee: IOTA-Tangle evolves the current consensus in every way. Zero fee transaction works in a way that every participant of the network does some computational work, verifying any other two transactions, in order to insert a transaction to the network (Popov, 2016). In this way, it eradicates the concept of mining pool and transaction fee. Unlike Bitcoin, the difficulty of verifying a transaction is very low but highly secured which enables a device with even limited computational power to perform the required mathematical work. This resolves the hefty and inconsistent transaction fee issue caused by Bitcoin.

Decentralized Control: In IOTA-Tangle every participant acts as a miner and validates two other transactions each time they add one to the network. This makes the mining power decentralized as compared to other distributed technologies where centralized control is inevitable, hence compromising the entire system.

Quantum Resistant Security: Unlike the preceding distributed technology, IOTA-Tangle uses a quantum resistant cryptography algorithm (Popov, 2016). From a security perspective, it is inevitable that hardware will soon break the classic cryptographic techniques. IOTA-Tangle has already prepared for the upcoming quantum advancement and has the ability to resist future advancements even with the current architecture.

Legality: Since this technology does not favor mining pools and obsolete security, it is very likely to be accepted officially in all countries. So far IOTA-Tangle is under legal boundaries that make it favorable for implementing different solutions, especially for the early adopters.

Scalable Throughput: In IOTA-Tangle every participant, who makes the transaction contributes actively unlike Bitcoin where one has to wait for the transaction to be verified by a miner which could take unpredictable time. The IOTA-Tangle allows the work to be done as soon as the required mathematical work is performed. Therefore, it is highly scalable and can process much larger throughput as all primary actors act as miners (Malanov, 2017).

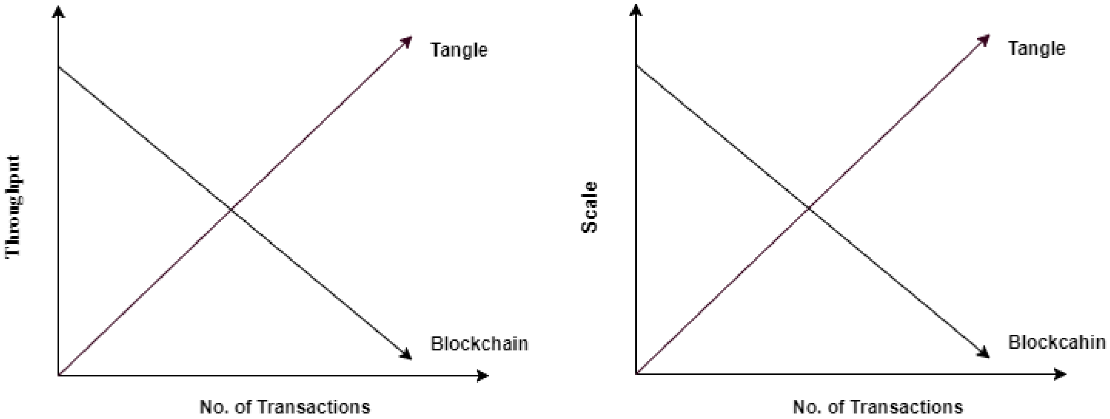


Fig. 1: Comparison of Blockchain with Tangle

The above graph shows that Tangle has an increasing throughput with a number of transactions as each user who wishes to perform a transaction verifies two other transactions. Furthermore, Tangle is highly scalable as compared to Blockchain which is why it is the most demanding evolution of the existing technology of distributed ledger as it addresses the potential drawbacks of Blockchain-based variants.

Table 1 drawn below sums up the pointers discussed above for all the four technologies

Table 1: Comparison of Different Distributed Technologies

	Tangle	Blockchain	Ethereum	Private chain
Quantum Proof	Yes	No	No	No
Feeless Architecture	Yes	No	No	Yes
Scalable	Yes	No	No	No
Throughput	High	Low	Average	Low
Smart Contract Support	Yes*	No	Yes	No

*as per the current plan of IOTA

Proposed Solution

The previous sections of this research paper explain why Tangle is preferred over other technologies for developing a unified education system across the globe. In this section, we will discuss the architecture and various aspects of the Zenith Certifier. Every digital certificate produced by the system will be called a **ZCert**.

Overview

Zenith Certifier will be one of the implementations of the Tangle for academic and professional records management. It allows the Recipient to share the academic and professional credentials with the surety that it is authentic and coming from a trustable source also known as the Issuer.

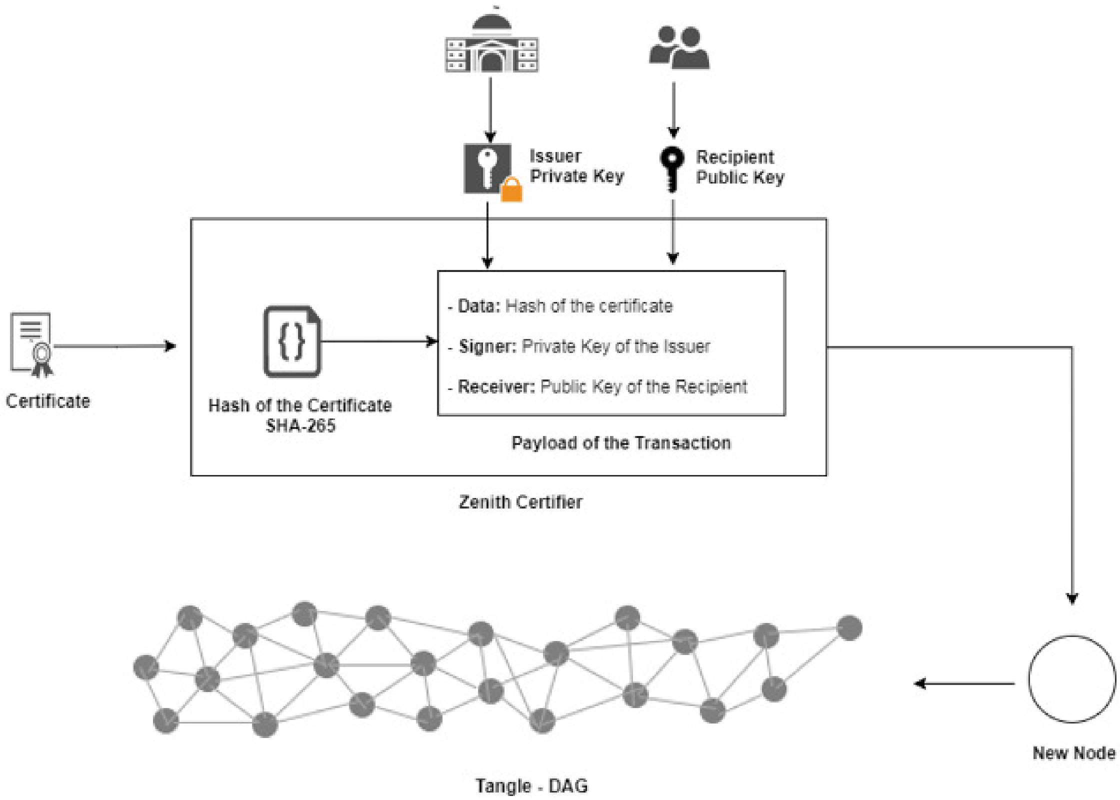

Issuer
Private Key
Recipient
Public Key
Certificate
Hash of the Certificate
SHA-265
- Data: Hash of the certificate
- Signer: Private Key of the Issuer
- Receiver: Public Key of the Recipient
Payload of the Transaction
Zenith Certifier
Tangle - DAG
New Node

Fig. 2: Use Case Diagram of Issuing a Certificate

Our solution comprises the following four basic steps:

Apply: The Recipient user acts as an applicant and applies for getting a digitally signed academic transaction issued against his or her certification on the system.

Issue: The Institute acts as the Issuer and verifies the request by issuing a digital certificate. Furthermore, the issuer inputs the digital certificate and public key of the recipient to the Zenith Certifier as illustrated in Fig 2. The Issuer also provides its private key to the system while inputting the digital certificate. This certificate has to be uploaded in Portable Document Format (PDF) which is first converted to an irreversible hash by using SHA-256 encryption (Handschuh, 2004). This hash is then passed to the transaction maker to develop the transaction payload. Since the hash is irreversible, it reduces the privacy concern of putting your credential on the Tangle.

Sign: The transaction develops the payload that contains the certificate hash and public key of the recipient. It is signed by using the private key of the issuer as illustrated in Fig 2. The public key in the transaction tells the ownership of the recipient, and being signed by the private key, guarantees the authenticity of the certificate.

Broadcast: The institute broadcasts the transaction to the Tangle. As part of the process, it verifies the other two transactions to add them to the ledger. After the transaction is added, a transaction number (Tangle address) would be provided to the recipient for reference.

Actors of the System

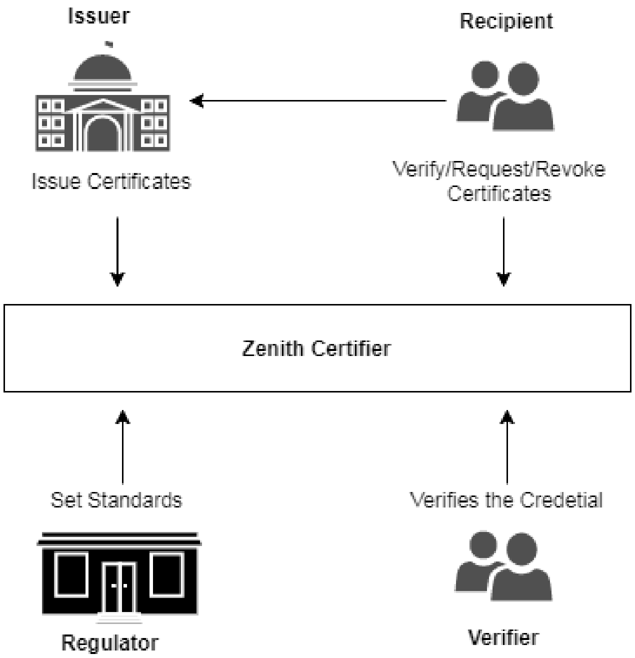


Fig. 3: Actors Involved in Zenith Certifier

There are four main actors that will interact with the system which are as follows:

1) Issuer: Universities and institutions play the role of the Issuer. Their goal would be to issue academic certificates to the students which are registered on Tangle in a digital format. These certificates will reflect their achievements, skills and personal academic records.

2) Recipient: This would be the students or applicants who would receive their digital certificates corresponding to their public key. They would also have a provision to request a new certificate and revoke an existing certificate from the issuer as illustrated in Fig 3.

3) Regulator: This would be the regulatory bodies which would verify and set standards within the system to map the actual business process. Every region follows a different grading system and it would be the role of the regulator to apply and evaluate these standards on the system. The regulator would further coordinate with different accreditation bodies to implement the standards.

4) Verifier: Verifier could be anyone who is interested to verify the authenticity of a given digital certificate such as institutes or employers. They can provide the public key and certificate of the recipient to verify if it is authentic or not.

Certificate is merely the standard document on which the trust for verification can be gained. The role of the verifier is comprised of verifying the credibility of a certificate, its issuer and to whom it was issued.

Wallet is a safe where one can store credentials. Both issuer and recipient can use their respective wallets to avoid losing their set of public and private keys.

Architecture

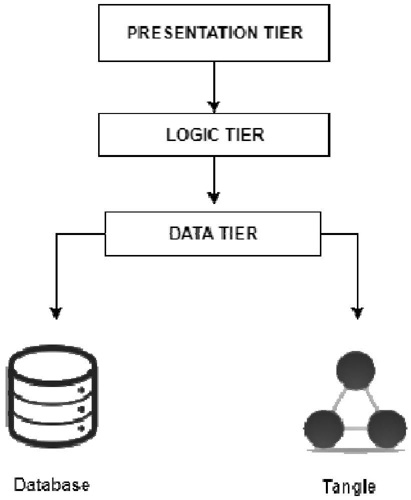


Fig. 4: Three-Tier System Architecture

Our solution would be based on a three-tier architecture to enforce scalability and persistence. Fig 4 illustrates the logical separation of the tiers. Each tier would have their different role as explained below.

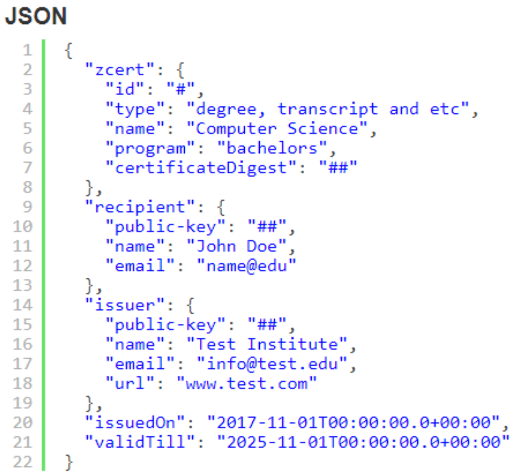
Presentation Tier: The top tier is responsible for interacting with the users of the system. It would be in form of both; mobile apps and web-based system that would translate the task and result into something that the users can comprehend. It is the focal point for the actors of the system to perform their task by interacting with logic/business tier.

Logic Tier: The role of the logic layer is to process and execute all the commands from the presentation layer. It interacts with other applications, performs tasks and communicates with the data layer. Since our solution is a thin client, the logic is where all the processing will take place such as generating a hash of a certificate for issuing and verifying and managing user rights management for all actors.

Data Tier: The third and last layer is responsible for managing the data present in the system which includes performing the storing and retrieving operations. In our solution, it would have two data stores; one being Tangle for certificate storage and other would be a relational database for registering actors and managing system configurations.

Zcert Schema

This section focuses upon the schema of the file which would be used to store the data onto a node.



JSON

```
{
  "zcert": {
    "id": "#",
    "type": "degree, transcript and etc",
    "name": "Computer Science",
    "program": "bachelors",
    "certificateDigest": "##"
  },
  "recipient": {
    "public-key": "##",
    "name": "John Doe",
    "email": "name@edu"
  },
  "issuer": {
    "public-key": "##",
    "name": "Test Institute",
    "email": "info@test.edu",
    "url": "www.test.com"
  },
  "issuedOn": "2017-11-01T00:00:00.0+00:00",
  "validTill": "2025-11-01T00:00:00.0+00:00"
}
```

Fig. 5: ZCert Schema Example

The format shown in Fig 5 illustrates the certification schema that defines the standard of a ZCert. We have used JavaScript Object Notation (JSON) for storing the certificates on Tangle. This can also be shared over the network as a simple JSON file. The schema contains a "certificateDigest" field and some other optional and mandatory fields. The "certificateDigest" field contains the SHA-256 digest of the certificate. Secure Hash Algorithm (SHA) is a one-way complex cryptographic function widely used in different applications.

This JSON is posted on the Tangle as the part of the transaction. This contains the public data of both recipient and issuer for necessary identification. The ZCert object holds the information about the certificate name, type, and hash. This current schema is basic and will be furnished as the system scale.

Critical Analysis

The proposed solution would have benefits as well as several challenges during its implementation. Since the use case taken for this model is Pakistan's educational system, so certain governmental pressures would act as a reluctant force for this implementation. Furthermore, to implement this use case, a complete brute force technique would be applied for each and every higher education institute to accept this approach.

Additionally, the main challenge would be to input all the data of the past graduates; i.e. complete data migration. Multiple resources would be required for each student's data to be inputted into the system.

Technically, the complete solution is built on the top of Tangle, so any vulnerability in the underlying technology will be inherited in our system as well. Also, we are using other centralized databases for managing different meta-data and profiles of the actors on the system. We may need to scale and secure that resource as the adoption of the system increases.

Furthermore, a paradigm shift would be required for the recruiters who wish to hire candidates. Since they would be the ones who would use this system as the second-most concerned primary stakeholder. Finally, it would be a big challenge to make it secure at all levels. Since it provides an end-to-end deal so leaving even a single loophole would compromise the purpose of this proposed model.

Conclusion

Our proposed solution would address the defined problem statement of this research paper. Once the proposed framework is implemented, it would help all the actors involved in the smart contract to save time, and the chances of fake degrees and certifications would be minimized. Moreover, the process of authenticating academic certificates would be shortened.

Furthermore, higher education institutes would also have an easy access to confirm an applicant's past academic career without the need for approaching any particular institute for verifications individually. Employers can also take advantage of this system by simply using the generated hash to check and verify that the applicant's academic degrees and certifications are completely genuine or not. Furthermore, the institutes would be able to regenerate digital certificates from Zenith Certifier in future by utilizing the ZCert JSON data on each Tangle node to create a uniform distributable digital certificate.

References

1. Anon., n.d. *Ether.* [Online] Available at: https://www.ethereum.org/ether

2. Biggs, J., 2017. *Tech Crunch.* [Online] Available at: https://techcrunch.com/2014/10/31/your-next-passport-could-be-on-the-blockchain/

3. Blockcert Organization, 2017. *Blockcert.* [Online] Available at: https://www.blockcerts.org/guide/system-overview.html

4. Blockchain, 2017. *Blockchain.* [Online] Available at: https://blockchain.info/wallet/#/

5. BTC Media LLC, n.d. *Is Bitcoin Legal?.* [Online] Available at: https://bitcoinmagazine.com/guides/bitcoin-legal/

6. Cawrey, D., 2014. *The Five Biggest Threats Facing Bitcoin.* [Online] Available at: https://www.coindesk.com/five-biggest-threats-facing-bitcoin/

7. Chinmay, A. V. & Munindra, L., 2014. Security Concerns and Issues for Bitcoin. *International Journal of Computer Applications,* p. 3.

8. Delmolino, K. et al., 2015. *A Programmer's Guide to Ethereum and Serpent.* [Online] Available at: http://mc2-umd.github.io/ethereumlab/docs/serpent_tutorial.pdf

9. Evans, D., 2011. *The Internet of Things.* [Online] Available at: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
10. Frank van de Ven, J. B., 2017. [Online] Available at: https://www2.deloitte.com/nl/nl/pages/deloitte-digital/artikelen/warranty-solution-based-on-blockchain.html

11. Handschuh, H. G., 2004. *Security Analysis of SHA-256 and Sisters.* s.l., Springer, Berlin, Heidelberg.

12. Jagers, C., 2016. *The Blockchain Menu.* [Online] Available at: https://medium.com/learning-machine-blog/the-blockchain-menu-7cdaa4b657eb

13. Lab, M. M., 2016. *Block Cert.* [Online] Available at: tps://www.blockcerts.org/

14. Learning, M., 2016. *Blockcerts—An Open Infrastructure for Academic Credentials on the Blockchain.* [Online] Available at: https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for-

academic-credentials-on-the-blockchain-899a6b880b2f

15. Malanov, A., 2017. *Six myths about blockchain and Bitcoin: Debunking the effectiveness of the technology.* [Online] Available at: https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/

16. Marchenkova, A., 2015. *How secure will our data be in the post-quantum era?.* [Online] Available at: https://medium.com/quantum-bits/how-secure-will-our-data-be-in-the-post-quantum-era-6a7f444ce7d5

17. Nakamoto, S., 2008. Bitcoin A Peer-to-Peer Electronic Cash System. p. 9.

18. Pilkington, M., 2016. Blockchain Technology: Principles and Applications. *-,* p. 39.

19. Popov, S., 2016. *IOTA_Whitepaper.* [Online] Available at: https://iota.org/IOTA_Whitepaper.pdf

20. Schroeder, S., 2017. *Here's how to deal with those ridiculously high Bitcoin transaction fees.* [Online] Available at: http://mashable.com/2017/08/28/bitcoin-transaction-fees/#11V.b25A6kqX

21. Swanson, A., 2017. *The Next Big Thing.* [Online] Available at: http://www.scmp.com/tech/innovation/article/1852141/how-baidu-tencent-and-alibaba-are-leading-way-chinas-big-data