school of continuing studies | YORK UNIVERSITÉ UNIVERSITY

Final Project Report

Business plan for – 'Verifik': A full-scale Credential and Certificate Verification system on the Ethereum blockchain

Verifik®

CSBC1020: Blockchain Applications for Industry

Submitted to:
Wai Kan Victor Li

Submitted by:
Gazi Mohammed Ashab Hossain

Student no. 219019231

Submitted on:

28.11.2021

Introduction

The name of this project is *'Verifik'* and it is a verification system for individual-specific certifications or credentials. These credentials can include individual identification documents, academic credentials, career credentials, financial certifications, and medical certifications.

It is a blockchain-based system where sensitive data like the credentials mentioned above have metadata about them stored on chain and are accessible only through smart-contracts; and therefore providing the ultimate security and safety. Essentially providing the opportunity of effortless access to all of the crucial information for an individual and the permitted participants to by sharing their unique *hash-key*. This *hash-key* is unique and generated by SHA256 encryption function.

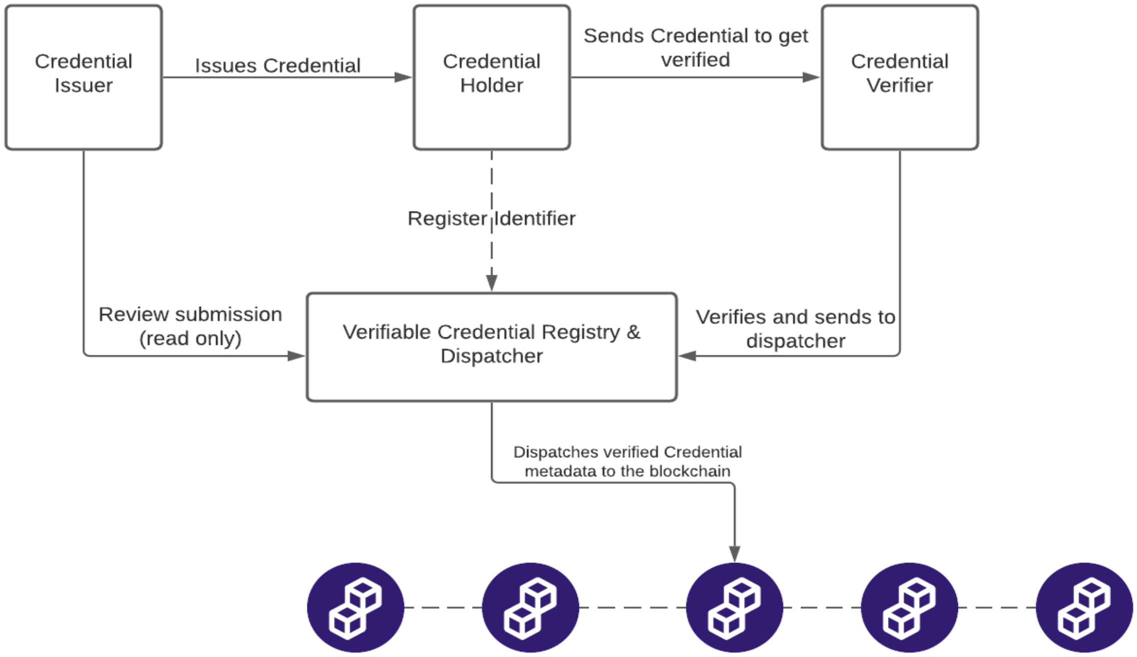

Credential Issuer
Issues Credential
Credential Holder
Sends Credential to get verified
Credential Verifier
Register Identifier
Review submission (read only)
Verifiable Credential Registry & Dispatcher
Verifies and sends to dispatcher
Dispatches verified Credential metadata to the blockchain

***Figure 1*: Basic information flow about verification and storage of credentials, and different roles on the network**

Talking about the issue of corruptible records: A Real-World Problem

In a constantly changing world of technology and innovation, every possible aspect of life is being virtualized and digitalized. This has greatly assisted us in being assertive in our *gradual progression* towards the future. However, in a world of internet identities and with the overflow of innovation, it has become easier than ever for malicious actors to contaminate and corrupt records and credentials for selfish gains. If an individual's identity, achievements and credentials are tampered with and rendered unusable, then it would cause tremendous repercussions for them. These qualifications give us an understanding of who we are and what we can become as a part of society. The burning question here is, how do we attain our goals and contribute to the overall progression of the society if our basic credentials are so **outrageously** vulnerable?

Following the footsteps of age old paper based storage of credentials and having only one physical copy that is verifiable, it sounds almost like an invitation for the records to be stolen/tampered with. Additionally, with the advent of digitalization nowadays, the issue of corrupted records has become more prominent. Besides credentials being corrupted, it is also easier to target an individual and theoretically destroy their lives. Someone's credentials can be used to commit fraudulent activities, or they can be altered to frame/accuse them of something they aren't aware of, and disproving it would be difficult because their credentials had been tampered with.

Let's look at some real world examples. In the US, between 2016 and 2020, credential theft has caused a total of 3 million to 5 million USD in losses due to fraud and other illicit activities (as shown in figure 2). This is becoming more of a problem each year and there is an urgent requirement to address this issue before it's too late.

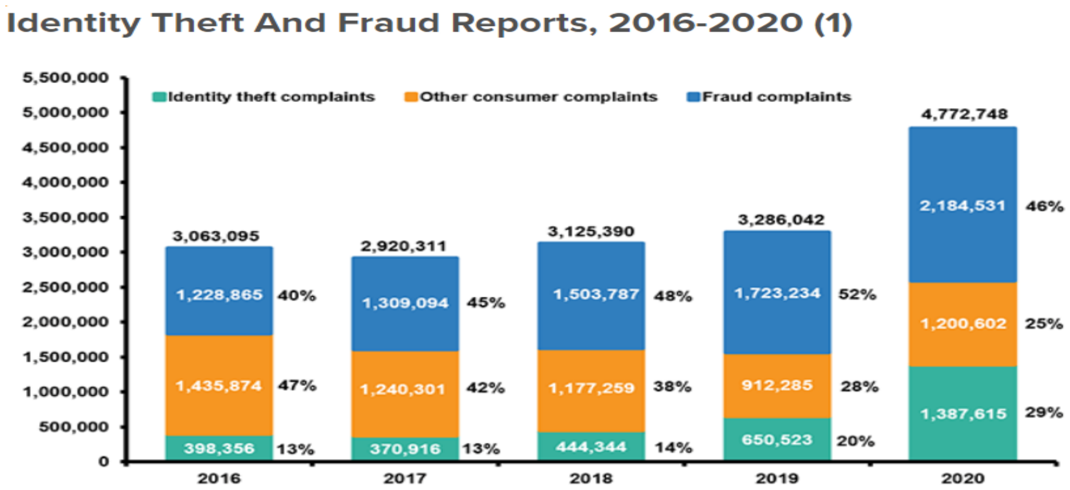
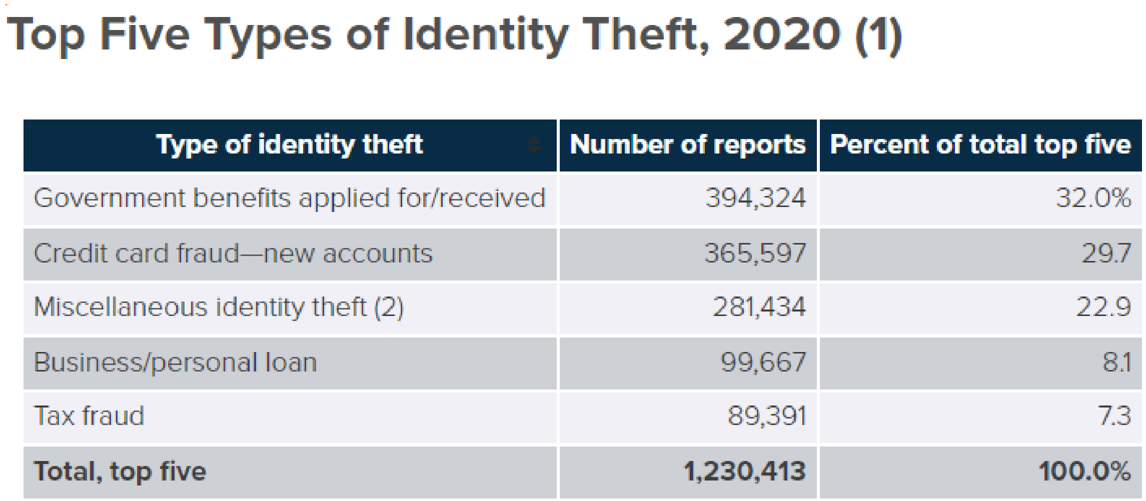


Figure 2: **ID theft and fraud statistics in the US (2016-2020)**



Top Five Types of Identity Theft, 2020 (1)

Type of identity theft	Number of reports	Percent of total top five
Government benefits applied for/received	394,324	32.0%
Credit card fraud—new accounts	365,597	29.7
Miscellaneous identity theft (2)	281,434	22.9
Business/personal loan	99,667	8.1
Tax fraud	89,391	7.3
Total, top five	**1,230,413**	**100.0%**

Figure 3: **Top 5 types of credential theft in the US in 2020**

Source

From figure 3, we can see that theft of Government benefits, Credit Card Frauds, Business Loans, Tax fraud etc. has been listed. These identity thefts are caused due to altered/corrupted credentials of an individual, apart from the general callousness that accounts for a very little percentage of these frauds.

It is important to note that these stats are only concerning the US. If we look at the global impact of credential-theft, the issue escalates tenfold.

A Necessary Solution

Companies/institutions across every industry that want to *genuinely* tackle and eliminate fraud, exacerbate risk, and relieve bureaucratic and administrative burdens concerning exchange of sensitive content, are leaning toward the use of blockchain technology to do so. Using blockchain to issue and verify official credentials and applying integrated content and a process management approach to it will only solidify the robustness of the chain.

Why use blockchain?

1. **Prevention of fraud**
   - Blockchain offers an immutable log of records. It is mathematically impossible to bypass the cryptographic signatures, making it implausible to impersonate someone else and commit fraud.
2. **Improved Efficiency**
   - Having all of the actors as active participants on the network, credential issuance and verification for any blockchain-anchored records without a third party improves efficiency massively.
3. **Increased Security**
   - After the records have been sent to a block, a user can rest assured knowing that his/her records are now unchangeable, tamper-proof and independent—meaning the security of the records are fortified.
4. **Ownership provided and verified**
   - An individual's records are their own and nobody else's. On a blockchain, this can be enforced by implementing private *hashkeys* for each record.
5. **Global reach**
   - your records can be accessible from anywhere in the world on a public blockchain, if the key is known. This way the records can be retrieved and verified without any geographic restrictions.
6. **Promoting Authenticity**
   - With authentic and easily accessible records, their authenticity can be advocated from anywhere in the world, increasing awareness of an individual's brand.
7. **A self-sufficient architecture**
   - In most public blockchains, the actors and stakeholders are incentivized economically to preserve the integrity of the network. For credential verification, an incentive (monetary or non-monetary) could be introduced to further amplify the security measures.

     Using a blockchain system to store and verify credential data and other sensitive information by taking advantage of the distributed ledger system seems to be the most sensible path for tackling the issue of corruptible records.

Blockchain of Choice

For preservation of content sensitive records, the blockchain of choice requires a robust and tamper-proof system. For the *'Verifik'* system, the blockchain would be built upon the solution '*Blockcerts*', which is also the building block for *'Hyland Credentials'* who have acquired *'Learning Machine'*, a startup whose previous design partner was MIT. The objective of '*Learning Machine'* was to migrate important student records of the institution and place them on a blockchain.

Introducing Blockcerts:

- Blockcerts is an open standard for building applications that issue and verify blockchain based official records. These may include certificates of any kind pertaining to a certain individual.
- Blockcerts consists of open-source libraries, tools, and mobile applications for a decentralized, recipient-centric ecosystem, enabling trustless verification through blockchain technologies.
- It is committed to the self-sovereign identity of all participants, and provides the user control of their credentials and claims through easy to use tools such as a certificate wallet. Blockcerts offers complete availability of records that is distributed in the network, without single points of failure.
- Blockcerts contains components for creating, issuing, viewing, and verifying credentials across any blockchain, which ensures interoperability.
- The governance framework of Blockcerts allows no outside interference with the data already stored in the network.

Blockcerts was initially built on the technical standard to work across any blockchain. In 2016, it started with the Bitcoin blockchain and then soon expanded to Ethereum blockchain. It has a native token called the BCERT token to help govern the infrastructure. Blockcert's open standard verification focuses on verifying student credentials for an institution primarily.

BlockCerts
Trust.Truth.Transparency

We can look at figure 4 to understand Blockcerts workflow:

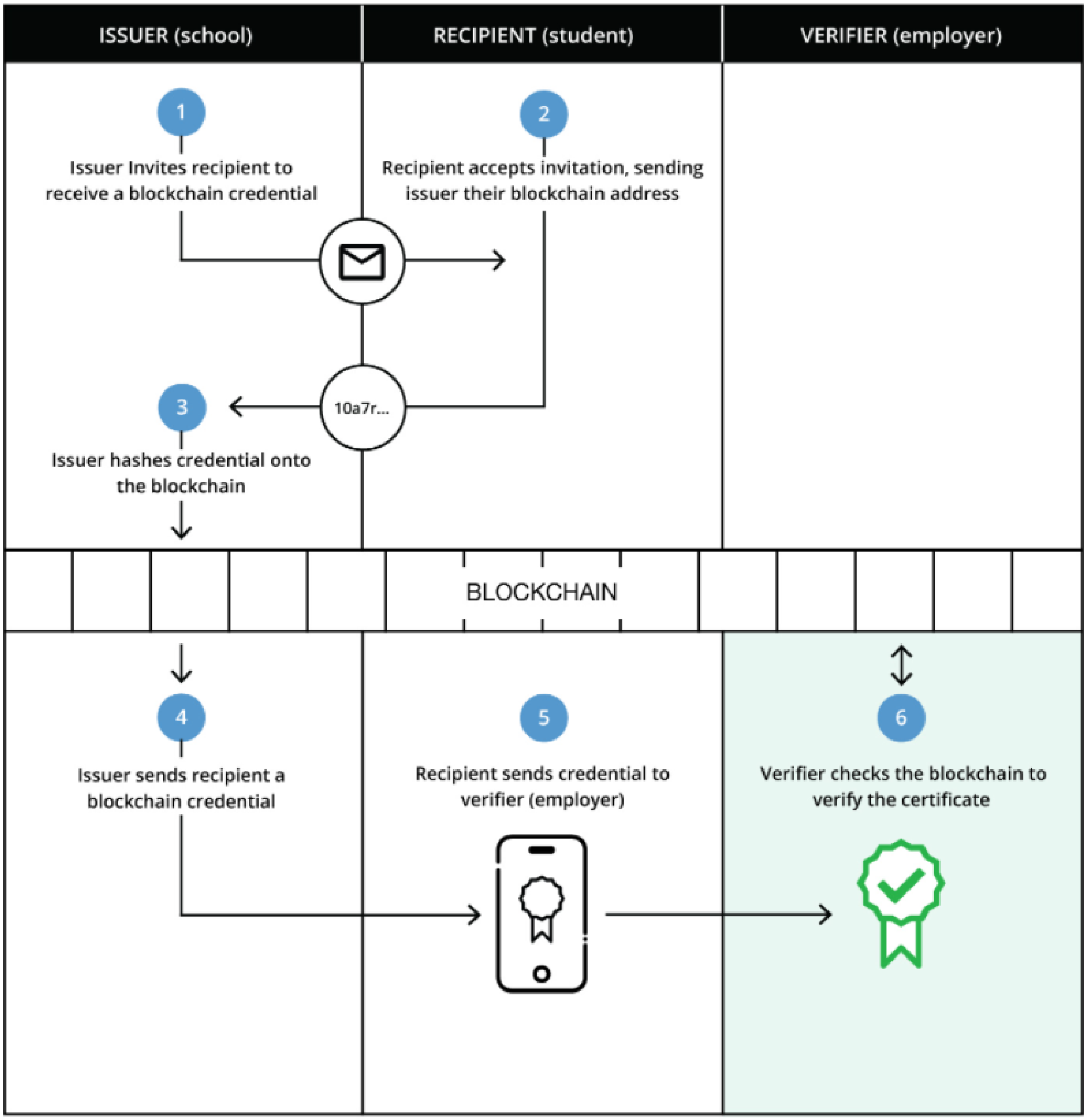

ISSUER (school)
RECIPIENT (student)
VERIFIER (employer)
1
Issuer Invites recipient to receive a blockchain credential
2
Recipient accepts invitation, sending issuer their blockchain address
10a7r...
3
Issuer hashes credential onto the blockchain
BLOCKCHAIN
4
Issuer sends recipient a blockchain credential
5
Recipient sends credential to verifier (employer)
6
Verifier checks the blockchain to verify the certificate

Figure 4: Blockcerts workflow

Source

As such, the '*Verifik*' system would be deployed on Ethereum and built upon the Blockcerts solution. As Blockcerts lays the groundwork for academic credential verification, a similar framework can be adopted in 'Verifik' system to extend the system to include all sorts of necessary verifications for an individual (i.e. jobs, medical records, credit scores, identification etc.) which is the ultimate goal of this project.

Specifying Primary Participants of the Network

In a credential verification system, the primary participants are the credential holders, the issuers and the verifiers. All these participants are part of the same network functioning in cooperation with each other.

Credential Holder: A holder is the user to whom a certificate is issued. It can be one or more individuals or a corporation even, depending on what sort of certificate has been issued. The whole system works to protect a holders' interests pertaining to their credentials. Their roles include:

- Registering on the network to get unique pair of digital keys
- Signing the provided certificate with their private *hashkey*
- Storing their private key safely (such as in a wallet)
- Presenting their certificate to the verifier/inspector

Credential Issuer: Issuers are the institutions that provide the holder(s) with the certificate. Issuers can be schools, universities, colleges, corporations or companies, businesses or banks, the DMV, hospitals, and even governments. Their roles are:

- Registering on the network to receive unique ID
- Verifying credential holder identity
- Signing holder certificate with unique Issuer ID
- Issuing the signed credential
- In absence of a Verifier, acting as the Verifier

Credential Verifier/Inspector: For such a system, the verifiers have crucial responsibilities. The verifiers are required to verify the certificates and credentials from issuers or holders. Verifiers could be the same entities as Issuers. Alternatively, it is also possible to have a group of validator entities whose duties only consist of verifying the certificates sent their way. The verification process could also be delegated to a third-party, but it is not commendable as it might amplify the potential risks against the system. Verifiers' roles are:

- Request and receive proof of credential from the credential-holder
- Verify signs from Issuer and Holder
- Grant access to the decentralized network (store the metadata)

Incentivizing the participants:

In a cryptocurrency environment, incentivizing the participants (monetary or otherwise) is an ideal way to maintain the integrity of the network. In a credential-verification system, incentives could be introduced to further fortify the infrastructure of the system. Incentives could be non-monetary as well. Below are a few possible incentivizing techniques:

- Incentives in this system would be provided through an internal scarce currency called *'VFIK'*
- **For Verifiers/Inspectors,** it is sensible to have some sort of incentive—as the verifiers play a crucial part. A rogue verifier entity could destroy the whole equilibrium, therefore it is essential to incentivize them to get the utmost out of the system *and* for better scalability.
- A governance token would be distributed to selective participants (Issuers and verifiers) to have distributed control of the protocol.
- Holders will be attributed a small number of tokens each time they use the system to verify a claim.
- Issuers get *VFIK* tokens each time some credential is issued through them.
- For **issuers** and **holders**, earning *VFIK* would be enhancing their brands; the more tokens you have, the more your brand value is. These tokens cannot be monetized, rather it will be used to rank participants-- It will work in a way initially to incentivize various central institutions to join the network. (Under the assumption that the tokens increase brand value)
- Finally, for an **Inspector** entity, *VFIK* could be offered as a reward token. It could work like this: An inspector accumulates 2000 tokens- meaning they have successfully verified at least 2000 claims. Like in a video game, they can exchange their tokens for a tally system where you can apply for a raise; as it only makes sense if you gain more expertise in a field, you should be paid more as well. Or, they can trade their tokens on a decentralized exchange at the running rate-only after it has been legally accepted to have an exchange value.
- A penalty system is also possible this way, where participants are penalized for wrongful issuance/verification.

Incentivizing the participants with tokens is one of the basic protocols that keep a crypto-environment honest and robust. Applying token incentives in *Verifik* system would enhance the security and integrity of the system tenfold.

Smart Contract Integration- Every transaction done on the blockchain (storage and retrieval of verified credentials) is done through implementing a smart contract; that includes the metadata of the record, the hashkeys and the block information. There is also a 'revocation' tool that can be integrated- it would enable a claim holder to revoke access to their data when required

A Self-Sovereign Identity(SSI) but with extra steps

The idea of a full scale credential and certificate verification system is dependent on the application of a decentralized identity. It makes good on the promise that **'your data is yours only'**, and self-sovereign identity implies just that.

An SSI specifies that a Decentralized Identification or a **DID** is to be issued to each claimer-in this case a holder of the verifiable credentials. In *Verifik* system, an *DID*-like hash key is given to each participant after registration on the system. A self-sovereign verifiable claims structure works like this:

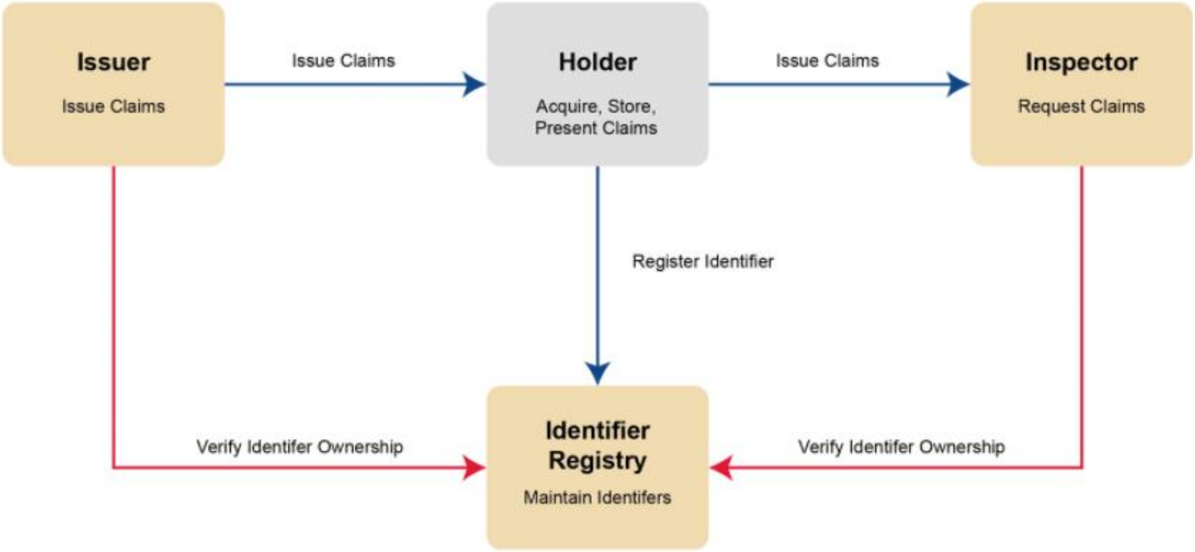


Figure 5: Verifiable claims workflow – SSI

Source

Here, the Issuer, Holder, and Inspector have similar roles as the 'Credential Issuer', 'Credential Holder' and 'Credential Verifier' respectively; as shown in the *Verifik* information flow. The 'Claim' is assumed as the credential to be verified. Here, the holder is always the subject of claims, as opposed to SSI system where even the issuer can have claims. The holder's credential is of the utmost importance in this system. Another difference is the Issuers sometimes can act as verifiers (e.g. when the issuer is an academic institution) in *Verifik* system, but not in SSI verifiable claims.

Ensuring Data Privacy in Verifik

Selective Disclosure:

In selective disclosure, you can generate proof from a few attributes from a credential. E.G. someone has to prove their address from an ID card but is not okay with sharing their address which is printed with the ID; in this case they can select that they only want to disclose their age and not their address from the credential.

Zero Knowledge Proof (ZKP):

In ZKP, you can prove the attribute from a credential without actually ever revealing the value.
From the example above of the ID card, someone can still prove that they're over 18 without revealing their Date of Birth with the help of Zero Knowledge Proof.

A ZKP is a unique method of authentication that, through the use of cryptography, allows someone to prove to another entity that they know certain information or meet certain requirements, **without** having to disclose any of the actual information that supports said proof.

What does it mean for this system?

A ZKP system would be designed into the verification system—in order to avoid exposure of sensitive data and to provide proof ownership with the usage of encryption key pairs and hashkeys; without ever revealing the real credential- as in, this system should theoretically able to prove that your Taxes are paid for the next fiscal year without you having to send a copy over of your tax papers.

If a ZKP system can be properly engrained into the protocol, it would minimize the risk of private data leakage greatly. It would enable data and scope minimization.

In other words, the minimum data/metadata required to accomplish the task will be retrieved from the credentials.

Limitations and predicted hurdles:

Every progressive venture forward naturally will accumulate enough opposition to be considered proactively. In the case of a decentralized credential verification system, there will undoubtedly some hurdles that will pop up upon testing and implementation. Some of the potential predictable issues are:

- **Personal responsibility for data:** Since your data is *yours only*, it is also implied that your data security is your problem as well. Expunging third parties means taking on more responsibilities about your own data. Most people are not equipped enough to deal with this issue on their own.
- **Initial limited operability:** Initially the system will run into operability issues, as a system like this can only flourish if *majority* of the population are participating. Because of course, decentralized ledgers cannot be dealt with in the same way as paper-based ledgers, there will be potential hesitancy to adapt.
- **Data management costs:** If your data is your own responsibility, it means to manage and maintain your data, you would have to invest a given amount of time and resources towards it, something that wasn't required before, as the third parties would take care of these issues. This would cause extra data management costs.
- **Unwanted intermediaries:** Managing data will likely become a problem that can't be dealt with at a personal level, hence, a lot of intermediaries will arise to offer their services and take care of this problem. However, for a decentralized system like *Verifik*, third party intermediaries are not ideal. With time and more adoption, managing data will be more simplified and only then the requirement for intermediaries will subside.

The tradeoffs for widespread implementation of a system like Verifik are not negligible. But they are solvable and we should see them reduced in the long run. Governing participants will get the chance to assess these drawbacks and hence trigger a change in protocol using their governance tokens; it would create a user friendly and open minded environment, which always helps to overcome difficult issues.

Plans to utilize funding

To achieve our goal of an efficient and well-produced product, sufficient amount of research and time for development is crucial, besides the required budget. The budget allotment and detailed timeline of the project development is given below:

Project timeline: 1 year

Budget distribution:

Category	Description	Allotment %
Development and Research	A specific amount of budget will be spent on research so that due diligence is done and the product is completely functional	20%
Human Resources	A team consisting of developers, testers, and interns will have to be hired. More details about technical personnel later	27.5%
Initial Cloud-Hosting	Hosting the database of credentials on a cloud-database requires purchasing the domain name at the specified database	7.5%
Testing	Test & trial of the project and proper automation with a Wallet app included	10%

Marketing	To encourage more people/institutions to participate, proper advertisement is needed	20%
Legal Fees	Legal issues will predictably occur when implementing the system, like tokenization and reward system	15%
		100%

Team hiring strategies:

Technical Research Analyst:

One experienced technical research analyst is needed to perform due research and suggest the best fit for the technology.

Business Analyst:

One experienced business analyst to be a part of product design discussions, and integrate the business requirements into the design.

REST API developers:

At least 2 developers to handle the API calls made from the wallet and ensure their functionality with experience in web3 technologies.

App developers:

A team of 3 junior level or 2 high level developers to create and test a wallet app that will be integrated into the system.

Blockchain Developers and Interns:

To write and process smart contracts, a team of 2/3 blockchain developers and interns is needed with experience in web3 and solidity.js, node.js

Testers:

An Experienced automation tester that would help with testing out the framework to perform integration testing.

Similar Projects

There are a few other projects that have been built on the principle of identity/credential verification. Below are a few examples:

1. *Microsoft Azure AD verifiable credentials:* Still in its beta stages, Microsoft released this platform to digitally validate credentials that can be used in multiple scenarios.

   Microsoft

2. *Hyland Credentials:* Built on Blockcerts, Hyland credentials issue digital credentials in a blockchain secured format that is easily shareable and instantly verifiable anywhere in the world.

   Hyland

3. *TrustEd:* A system that implements blockchain technology to mitigate the problems faced in the process of academic credential verification and storage.

   TrustED

4. *DL creds:* Part of the DL Certify platform, it is a blockchain based credentials verification system.

   DL Creds
   Powered by DL Certify

5. *Snapcert:* Snapcert enables secure digitization, generation, authentication and sharing of any kind of academic certificates and creates a trusted ecosystem with all the secure records.

   SnapCert

So what makes 'Verifik' better? As it can be seen, these projects mostly work to solve the issue of academic credentials and certificates. For our system (Verifik), the idea of using this verification mechanism is being extended to any sort of verification that might be required i.e. academic certificates, financial certificates, driver's licenses, medical prescriptions etcetera. This makes the *Verifik* system much more scaled up and equipped for generalized purposes; as an extension to these verification systems usecases.

What could derail this project?

A lot of significant issues might arise during the development and implementation of this project. A few of them have been predicted below:

❖ **Government interference:**

A decentralized ledger means that there is no centralized control over any data; which usually many central governments/entities own. It might not sit right with them to lose control and they might interfere with the process, development, and implementation. Therefore, it is essential to build trust between the system and various central governments.

❖ **Attack on infrastructure:**

Any outside attack on the chain or the system by malicious actors might derail the project or seriously delay the development process. Thankfully, as one of the advantages of a decentralized system is that targeted attacks are improbable due to the distributed and randomized states of blockchain data. Although the blockchain doesn't store any of the sensitive data, just the metadata concerning the real data, the attackers might acquire the keys and then act like the owners of that data—this is where people have to be vigilant. Various incentives/penalties will also help repel attacks on the system.

❖ **Cloud Storage issues:**

As the original copies of the credentials are stored in a database (cloud databases, in this case) and only the metadata is distributed in a chain, the issue still remains that all the data is stored centrally and this opposes the principles of blockchain functionality. Even after applying distributed cloud systems (where data is stored in multiple random cloud addresses) this problem still could be prevalent. If this issue arises; it shouldn't be more than a superficial problem, as the real data can be accessed ONLY with the possession of private and public keys for a specific entity. In simple terms, even if the records are in a central database, the keys to access them will be on the chain and hence they will still possess the incorruptibility attribute.

- **Lack of wider adoption:**

As we can see from the limitations, generalized adoption of this system would require some effort that a lot of people might not think is warranted. If a small percentage of people don't agree on the protocols and safety requirements of the data, then it might mean more difficulty in implementation on a global scale; and that is required for us to fully take advantage of such a system that relies on immutability.

A disturbing aspect to consider

It is safe to assume that in 2021, all of us have been victims of the horrible ailment that is the COVID-19 pandemic. As explained in the statistics building up to this solution, due to the pandemic, people have started using their virtual identities (like email, Facebook, online vendor accounts) more and more. This has made scams easier and the flow of identity information is at the highest it has ever been. Identity theft has become a norm these days, and the system needs an overhaul. A system like *'Verifik'* can offer a solution to this problem, of course. But the larger concern here is the availability of personal data on the web. It is unnatural, to a great extent, and we should always be more careful of sharing too much information, especially without a decentralized system. Just food for thought.

Future plans:

-Implementation of Ethereum 2.0

-Migration to an independent blockchain (Permissioned-public)

-Adding relevant tools and plugins to meet future requirements.

Conclusion

Through this report, the whole system, architecture of *'Verifik'* system has been specified and a solution against corruptible data has been presented. To summarize the whole system,

- ✓ ***'Verifik'*** offers an instant **verification** system for any sort of credentials an entity can have.
- ✓ **Issuers** issue the credentials and **verifiers** verify them. The credentials belong to the holder.
- ✓ The system implements **SSI** and **digital key pairs** to ensure security of records. **Smart contracts** are utilized to dispatch the **metadata** to the blockchain.
- ✓ Applies **Selective Disclosure** and **Zero Knowledge Proof**
- ✓ Participants are incentivized with scarce tokens **VFIK** and governing tokens (Could be non-monetary as well)
- ✓ Based on the open-standard verification system called ***'Blockcerts'*** on ***Ethereum*** Blockchain
- ✓ Especially in a **pandemic-driven** environment like the current times, a system like *'Verifik'* could accomplish a lot against **credential-theft**.
- ✓ This system has the capability to **replace** paper-based identification and verification systems **globally**-simultaneously providing the highest **data security** technology can provide.

"Not your keys, not your coins nor your identity", states the famous crypto entrepreneur *Andreas Antonopoulos* -- This is the defining principle of this system. A full-scale decentralized verification system would succeed simply on the merit of security and transparency alone. With an incentive inclusive protocol and fortified smart-contracts, any verification can be achieved in minutes; saving us a ton of time.

After all, *time is the ultimate currency*.

References

[1] Course Modules of CSBC1020

[2] “Blockcerts timeline and growth.” [Online]. Available: https://blockcerts.com/media/1590/blockcertsplustimelineplusandplusgrowthplusedited.pdf. [Accessed: 28-Nov-2021].

[3] D. Crichton, “With MIT launched, learning machine raises seed to replace paper with Blockchain credentials,” *TechCrunch*, 07-May-2018. [Online]. Available: https://techcrunch.com/2018/05/07/learning-machine-credentials/. [Accessed: 28-Nov-2021].

[4] Hyland Newsroom, *Hyland acquires Blockchain-credentialing provider learning machine*, 05-Feb-2020. [Online]. Available: https://news.hyland.com/hyland-acquires-blockchain-credentialing-provider-learning-machine/. [Accessed: 28-Nov-2021].

[5] Hyland, “Hyland launches Hyland credentials for Higher Education,” *Hyland launches Hyland Credentials for Higher Education*, 13-Apr-2020. [Online]. Available: https://www.prnewswire.com/news-releases/hyland-launches-hyland-credentials-for-higher-education-301039484.html. [Accessed: 28-Nov-2021].

[6] ”Blockcerts: The open standard for blockchain ... - youtube.” [Online]. Available: https://www.youtube.com/watch?v=2drjOUeO-IA. [Accessed: 28-Nov-2021].

[7] “Introduction,” *Credential Status List 2017*. [Online]. Available: https://w3c-ccg.github.io/vc-csl2017/. [Accessed: 28-Nov-2021].

[8] D. Hardman, “A gentle introduction to verifiable credentials,” *Evernym*, 27-Oct-2021. [Online]. Available: https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/. [Accessed: 28-Nov-2021].

[9] “Self-sovereign identity: The Ultimate Beginners Guide!,” *Tykn*, 01-Oct-2021. [Online]. Available: https://tykn.tech/self-sovereign-identity/#Self-Sovereign_Identity_and_Blockchain. [Accessed: 28-Nov-2021].

[10] “Identity verification solutions - microsoft security,” *Identity verification solutions - Microsoft Security*. [Online]. Available: https://www.microsoft.com/en-ww/security/business/identity-access-management/verifiable-credentials. [Accessed: 28-Nov-2021].

[11] “Home,” *TrustED*. [Online]. Available: https://www.trusteducation.io/. [Accessed: 28-Nov-2021].

[12] “DL creds,” *DLT Labs*. [Online]. Available: https://www.dltlabs.com/platforms/certify/dl-creds. [Accessed: 28-Nov-2021].

[13] “Issue and verify academic credentials powered by Blockchain,” *SnapCert*, 05-Oct-2021. [Online]. Available: https://snapcert.io/. [Accessed: 28-Nov-2021].

[14] “Decentralized identity - bonus livestream session - youtube.” [Online]. Available: https://www.youtube.com/watch?v=ySHNB1za_SE. [Accessed: 28-Nov-2021].

[15] “Facts + statistics: Identity theft and cybercrime,” III. [Online]. Available: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Top%20Five%20Types%20of%20Identity%20Theft,%202020%20(1). [Accessed: 28-Nov-2021].