University of Zurich[UZH]

INFORMATIK-VERTIEFUNG – Communication Systems Group, Prof. Dr. Burkhard Stiller

Comparative Study on Identity Management Methods Using Blockchain

Atif Ghulam Nabi
Zurich, Switzerland
Student ID: 15-709-116

Supervisor: Sina Rafati Niya, Thomas Bocek
Date of Submission: September 29, 2017

University of Zurich
Department of Informatics (IFI)
Binzmuhlestrasse 14, CH-8050 Zurich, Switzerland

ifi

Informatik-Vertiefung
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmuhlestrasse 14, CH-8050 Zurich Switzerland
URL: http://www.csg.uzh.ch/

Abstract

Blockchain technology is disrupting society by enabling new kinds of disintermediated digital platforms. The need for blockchain based identity management is particularly noticeable , we have faced identity management challenges for example security, privacy, and usability since the dawn of the Internet. Blockchain technology may offer a way to address this problem by delivering a secure solution without the need for a trusted, central authority. It can be used for creating an identity on the blockchain, making it easier to manage for individuals, giving them greater control over who has their personal information and how they access it. In this study, twenty three companies are studied by highlighting important parameters including their introduction, operations, advantages, use cases, design and challenges. From this research a comparison of all companies is conducted. Along with this study and comparison, best solution is discussed in terms of IoT devices integrating the blockchain technology.

Acknowledgments

I would like to express special thanks to my supervisors Dr. Thomas Bocek and Sina Rafati for their support. I also thank Prof. Dr. Burkhard Stiller, the head of the Communication Systems Group at the University of Zurich, for making this report possible.

Contents

Chapter 1

Introduction

Blockchain is a decentralized and public ledger, which has introduced tremendous changes during last few years with applicability on financial use cases (e.g. remittance) and nonfinancial use cases (e.g. documents). Blockchain-based systems provide the possibility for their users to insert their data in this distributed ledger. Users can trust the blockchain as it is leveraging consensus mechanisms to validate and gather the transactions in blocks[1].

Along with distributed ledger, blockchain is also considered as an open ledger where online transactions are recorded and users can connect, send and verify their transactions. In other words, it is a digitized system in order to account the records. These records are set of mathematical rules which are used to stop the illegitimate intrusion.

In order to include the data into the blockchain, users and nodes, which obtain an authorize-able address from blockchain, need to set up and communicate with smart contracts to send and retrieve data to/from blockchain [2].

Moreover, blockchain works on the following rules; it represents decentralized, transparent and secure systems. Decentralized can also be called user to user or peer to peer operation without involving any central hub or authority. Transparency means the data is being embedded in the network publicly. Security offers the encryption technology supporting public and private keys. For example, in bitcoin, public key represents the userâs address and private key act as a password to access the transaction.

Here are few advantages and disadvantages regarding the blockchain[3]. They are good to consider while developing blockchain based applications. It is also important to note that blockchain is facilitating the society/ human beings in many ways due to its advantages. Its disadvantages represent the lack of certain feature

Advanatges of blockchain are:

1. Blockchains are able to reshape the market by reduction in security risks. Also, it offers a trustworthy system, where a block is unable to alter once record is placed on the network. Protection of transactions is fully supported.
2. By using blockchain technology, no third party is required. So, it offers less number of peopleâs involvement to maintain the working of a business model or financial applications.
3. Blockchain technology is very helpful to overcome the issues like money laundering and fraud cases because it facilitates the users with more transparency. Transparency means user can monitor the recorded information on blockchain network.
4. Due to blockchain not only services are automated but also the follow-up is quite easy. For example, it is easy to keep track of the money sent via bitcoin.

Few disadvantages of blockchain are also given below:

1. As it is new technology which needs to replace the existing one. So, it always brings a fear to replace the existing technology.
2. Blockchain based technologies are suffering from less support from government and legal authorities
3. There is a need to make blockchain technology more effective against illegal authorities such as terrorism or drugs dealing, to make the blockchain more secure so that user can trust these services.
4. Blockchain requires more efforts for research in academia and business applications in the industry, so that stability can be achieved by high automation.

One of the prominent frameworks for developing smart contracts is Solidity[4] which is supported by Ethereum group [5]. Ethereum is an open-source platform developed by a group of researchers and programmers, in 2015. The programming languages used to develop this software are C++, Go and Rust. It works on Windows, Linux, MacOs, POSIX and Raspbian platforms. This tool can facilitate the number of use cases such as smart contracts, finance, Internet of Things (IoT) and business models [6].

1.1 Motivation

An emerging use case of blockchain-based systems in academia and industry is the integration of IoT (Internet of Things) and blockchain-based approaches. The collected data from IoT sensors scattered all around the world with a vast variety of kinds and functionality can be accessed by blockchain clients with completely distributed and public accessibility with an absolute and undeniable credibility[7]. On the other hand, identity

management is another use case of blockchain with a high number of proposed use cases and applications (Mesr. In this study, our focus will be on the identity management applications and already proposed solutions. Open and unresolved issues will be discussed regarding this area. Mainly, a comprehensive comparative analysis will be conducted.

1.2 Description of Work

In this comparative study, the relationship of blockchain and identity management system is focused. This study covers the problem to be solved, the discussion of the design choices, set of arguments on the final design choice and a list of solved and open issues. The question and goals we are going to target in this study are listed down

1. How blockchain networks operate, including the mining and consensus processes?
2. How blockchain-based applications integrated and set up in the Ethereum blockchain?
3. Presenting an analytical study on existing identity management applications and solutions which are proposing a blockchain-based solution, which could not be replaced with other regular (non-blockchain- based) approaches.
4. Define advantages and disadvantages of hired methods in all studied products per each use case with specified metrics and facilities?

Chapter 2

Related Work

Blockchain is an emerging technology. In the recent years, it is not only used for financial use cases but also targeting almost every main field revolving around a human life. It can be business, health, gaming, government system, software/ electrical engineering and many more.

Blockchain with identity management: An approach for identity management system which is implemented by using blockchain is a new trend. Here, blockchain is used to store and retrieve the user ID. In order to contact the user, block can be retrieved and validated. Also, it is made secure and encrypted by implementing blockchain internally and externally; internally for accessing the list and externally to follow the identities [9]

Blockchain with IoT: Blockchain is inspiring IoT areas where efforts are being made to implement the blockchain technology. Like the data creation, storage and transfer is tried to carry out with blockchain technology. To make it possible, a study has been conducted by hosting two environments; fog and cloud platforms. It is discussed and analyzed that fog yields better results in this study [10] . In another research study, the efforts are made to make IoT system more secure and privacy oriented by using decentralized blockchain methodology. The reason to provide the blockchain based security in order to remove the inefficiency of the existing methods which are not enough to cope with the high energy consumption and the large overhead. The applicability of this proposed approach is demonstrated through smart home based case study. This paper claims to present the idea of blockchain in smart homes for the first time[11].

In addition, researchers have focused on the providing optimized blockchain for the IoT devices which includes the low overhead and less delay. For this purpose, a hierarchical model is proposed which integrates the centralized immutable ledger for low level for IoT and decentralized public blockchain for the security/ trust[11]. Similarly, in another study, attention is paid to the security issues regarding IoT. The importance of integration of IoT with blockchain is described by comparing the centralized security methods. Also, the issues by neglecting this integration are also highlighted [12]. M. Amirtha Krishnan et al [13] presented file sharing by using blockchain in IoT. By doing so, live file transfer can be

observed. As well as, file can be tracked easily using IoT layer. The main advantages were observed by using the proposed methodology are in terms of authenticity and efficiency.

Another contribution in the area of blockchain and IoT is made by the authors in [14]. It is observed that blockchain provides decentralized and peer-to-peer security for the data, while smart contracts are used to automate the more than one complex processes. IoT helps in the interaction of the internet with the physical world using blockchain technology [14]. In another paper, the presented approach contributes in three main phases. Firstly, the IoT components are shifted to the edge hosts from the clouds. Secondly, IoT components which are software oriented are converted into virtual resources to assist the design and maintenance easily. Thirdly, permission based blockchain are being supported for the IoT virtual resources [15]. The research in the area of IoT and business models is carried in which the IoT e-business model is designed. All important aspects of business are considered such as entity, commodity and transaction[16]. Moreover, in order to make IoT e-business decentralized/peer-to-peer, blockchain is used. The proposed methodology is verified with the experiments.

Blockchain with other areas: Despite of being used in digital identity and IoT, blockchain is touching other areas such as health, finance, networking and gaming. In other words, as different organizations are paying attention to the shared and distributed ledgers, way to different use cases are opened. Different use cases with blockchain are discussed below giving insight to the reader.

Finance: Initially, the blockchain was implemented for financial area in order to handle the transactions of digital currency i.e. bitcoin. This would benefit the user in terms of secure, digital and shared technology. In the research study [17], the focus is on blockchain sustainability in the future in banks (banks are taken as a use case for this study). Also, the risk and opportunities regarding the payment methods using blockchain is considered. Different questions are raised against different areas; organizational issues, competitive environment issues and technology design issues. In order to make these transactions in finance more efficient, blockchains are resilient [18].

Health: New dimension of health industry is explored with the help of blockchain. Several issues are discussed which can be eliminated by using blockchain. One of the examples is to directly handle the issues of counterfeit medicines. As drugs comes up with timestamp indicating when and where the drug was produced and how long it can be used. The information is stored on the blockchain network [19]. In another research paper, health industry using blockchain is addressed. Authors tried to maintain a record of EMRâs using blockchain which is easy to locate and access. A prototype of âMedRecâ is developed and it is analyzed for the customers and medicine providers for record flexibility [20].

Networking: Blockchain technology can also be used in networking area. Such as decentralized blockchain technology is used in centralized VANETs (Vehicular Ad-hoc NETworking). To make it applicable, Ethereum blockchain platform is used. Many other

traffic and vehicle related applications are also used (e.g. traffic regulation and vehicle insurance application) [21].

2.1 COMAPNIES

There are many other interesting areas leveraging the blockchain technology. I will explore relevant use cases by studying already developed solutions for identity management and authentication. Additionally, the main contribution of this report is to study the 23 companies. The details of these companies are as follows

2.1.1 2WAY.IO

Introduction: 2WAY.IO is software company whose founder and CEO is Tim Pastoor. It uses the identifi protocol to provide the decentralized digital identities. It is mainly used for the identity and reputation systems [22]. There are different types of identities such as legal identity (e.g. Driving License, Passport, National identity card) and social identity (e.g. Facebook, Twitter, Skype). All such legal or social identities are mainly supported by centralized systems. For example, Facebook account created by a user represents his social centralized identity. Whenever a user sends a message to the receiver via Facebook, this message is encrypted at sender side and decrypted at receiverâs side. So, the Facebook service as a centralized authority, can decrypt the message anytime. When we use online services, we basically always rely on other people to handle our private communications and store our sensitive data. By doing so, we voluntarily give away control over our personal data. This centralization of identities is abandoned using 2WAY.IO which aims to provide decentralized identity systems reducing data breaches by enhancing security and privacy of users.

How it operates: 2WAY.IO is developing a purely peer-to-peer base layer protocol for trust (identity reputation), to add the missing layer of trust to the Internet. Integration of identifi and identity management ensures the authentication of services being offered to the customers. For this purpose, a digital ID is created for the user which acts as a digital watermark. 2WAY.IO is built on the Eris and NXT platform [23]. The underlying protocol on which this platform works is identifi . It was developed by the Martti Malmi or Sirius. It is capable of creating an electronic trust network that can be used by both human and machines[24].

The software(identifi) itself is fork of bitcoin daemon, so it uses the same sort of networking mechanisms (the way you connect with other network peers or information is flooded to other peers), command line interface, JSON RPC API, public key cryptography. So, for the large part, it works same as the bitcoin network. It does not use mining, proof or work scheme, objective logic i.e. consensus. The major difference is, there is no blockchain.

It actually works on the consensus mechanism which involves the subjectivity. Subjectivity means when data is flooded to the peers, and peers may establish different opinions on

data, then we can utilize those opinions from peers in order to develop our own way of identity[24].

We can try to understand the working principle of the identifi protocol and subjective consensus by looking at more examples. For instance, the definition of a good barber is a subjective matter, it may be affordable price for someone, nearby for other person and another person considers it good for haircut styles. So, consensus of good barber can be denied by another person in the network, which means consensus can be true or false. In contrast to 2WAY.IO, bitcoin supports objective records of truth (a global record of transactions) about the previous transactions for transparency to make sure if the coin has not been spent before or not, but in case of 2WAY.IO, it is more about subjective logic, because the majority of people will never agree on the statement of an identity is true or false [24].

I can, for example, say that blue is a nice color, you can deny it. I can say you are a good person, researcher or car salesman, but somebody else can deny this information. Thatâs why objective consensus mechanism does not work in identifi as it works in bitcoin network, so the consensus mechanism in identifi is purely subjective. Similarly, if I can verify that your facebook account belongs to you, but somebody X can deny that, so the people in network of X will trust that itâs not true. There can be many other examples to explain it. [24]

Identifi is used to create the public identities. Its main features are as follows;

- It is used to keep the contacts and trusted identities up to date.
- It finds out the viewpoint of the people or organization said by other persons in the network.
- It shows the data or content only from the trusted parties.
- Identifi is peer-to-peer open source identity and reputation database.

If you store anything with in own database e.g. on your node, you simply connect it with other peers on the network to start flooding information to peers and if the other nodes on the network trust you they can sign the public key of your node, and from that moment on, they can verify any information that you are sending. Thereby, they choose to store information in their own database.

Itâs a broader concept than giving rating on eBay, Uber, Airbnb etc. A user can verify or deny certain statements to connections who belongs to another identity. When you look at PGP, a web of trust, a great example is OTC or bitcoin, so basically you create a keeper. In identifi, you choose to sign a public key of a user X with your own private key, to make a first degree connection. So, any information you store on your node and then decide to publish it to the world. It will also be sent to X, and if he chooses to store any data that you flooded towards him and he can verify it by signature i.e. by looking at the public key to verify that itâs in his own web of trust so itâs trusted key and these messages will be stored in his own node.

There are three types of messages that you can send over the network using identifi protocol:

1. You can simple static messages e.g. add URL to LinkedIn, you can send bitcoin address, you live in this country or have this age etc.
2. The other type, you deny or refuse to some connections, e.g. if someone creates a Facebook account on your name and a user X sees that its not you by looking at your public key. He can simply deny it, saying its not correct.
3. You can send rating to a connection, e.g. if he is a good barber, a good researcher so you give him 8 out of 10 or add your remarks in rating.

If you are receiving hundreds or thousands of messages and you donât want them to save on your node, as a solution, you can flood this information to data saving nodes in the network which may charge you a little amount to fetch this information again in the future. If you donât want to save the information on your node and you donât know whatâs the rating of a barber, you can check the public key of barber to see if someone in your web of trust has recommended this barber. You can search a nearby barber on the internet, and identifi will show you if some of connections has put remarks on the barber.

There are also other protocols out there e.g. blockchain id protocol, key base mostly for PGP etc.

Advantages: Few advantages of 2WAY.IO are as follows.

1. 2WAY.IO is applicable to the identification, authentication and reputation problems.
2. This software is open source, so extensions can be made to facilitate the further capabilities of block chain regarding identity solutions.
3. There is no need of trusted third party due to supporting cryptography and APIs.
4. In 2WAY.IO public and private keys are used. By using 2WAY.IO, the need of physical documents (e.g. Passport or license) will eventually be disappeared. For example, if you want to send some identity document to an organization, the document may not contain watermark or other features, so it is hard to recognize a persons identity if security features will disappear. You will not be able to verify that itâs a copy or photoshoped image.
5. Not only public and private keys are used but secured communication channel is used for identity management. If we send a document over a communication channel in a conventional way, it can be intercepted by a man in the middle attack.
6. It reduces the risks of saving sensitive or confidential data of users on the centralized information silos. In 2WAY.IO, even if somebody gets your public key, he wont be able to access your confidential information. He may only know that a citizen in a country and has age for example 18.

Use cases: This software can be used in many applications. Few targeted domains are 1) authentication systems, 2) communication systems, 3) smart contracts and 4) Internet of Things (IoT). 5) Web developers can develop the secure front end applications which facilitate both developers and users to execute the back ends (e.g. super nodes), 6) Financial services etc.[24].

Design: This software is able to convert the public nodes into private nodes. This is possible by adding an extra permission layer (Amit, 2016). Private nodes obtained by this transformation can be used to connect the information and communication channels. Design involves the privacy design and security design. Furthermore, security by design is the primary task which offers the secured data storage with the help of secured communication channels. These both design approaches are user in control which means user has the authority to control the application and can operate without any tradeoff between security and UX.

Limits: It is available for LINUX operating system. The limitation of this software is the unavailability of the 2WAY.IO in windows and mobile applications. Another limitation is the no record saving. This means every time, user has to show his/her identity and it is checked by accessing the private key at another end. Sometimes, it is valuable but it is also undesirable [24].

Recent and future tasks of 2WAY.IO: The efforts are made to make digital identity decentralized which open new directions. It simulates the development of the identifi protocol. It is currently establishing the documentation, developing a forum or a platform which helps the developers to share their idea and perform discussion on various aspects for identiti and blockchain (Pastoor, 2015). Moreover, it is building custom solutions which are less risky and cost efficient.

2.1.2 Atencoin

Introduction: Aten Coin is simply a digital coin which is used to be known as first generation digital currency based on blockchain. Blockchain is a distributed public ledger which keeps the record of every transaction in a network of blocks. Aten Coin was introduced by the National Aten Coin (NAC) foundation. This foundation aims to provide the blockchain based technologies and digital currency leveraging identity management and authentication [8]. Aten Coin is decentralized and users control the value of the Aten Coin. The only part of the Aten Coin that is centralized are its compliance features. Aten Coin is considered a fast and more secure digital currency e.g. to reduce money laundering, as compared to bitcoin[25]. Also the additional features of Aten Coin make it different and more applicable. For example, it completely overcomes the identity theft and suspicious activities. The Aten Coin database is compared with this list to prevent unethical people from using Aten Coin. The Aten Coin database is compared with many

other government criminal and sanctions lists. For any suspicious activity, reports can be submitted to the US final crime enforcement networks.

Advantage: Few advantages of Aten Coin [26] are mentioned below:

1. It guarantees to reduce money laundering problems as it knows its wallet users by knowing their decentralized identities.
2. Aten Coin is faster because average time it takes for first confirmation is 33 seconds while other digital currencies takes 300 seconds or 5 minutes for first confirmation of transaction.
3. The use of Aten Coin builds the security, trust, credibility and confidence among the people using it around the globe.
4. Aten Coin has no international transaction fees. Also, it has lower transaction fees for sending person to person.
5. The value of Aten Coin is not determined by the government as it is decentralized so, while having economic issues at government level doesnt affect the Aten Coin users.
6. Aten Coin is traceable and trackable in case of any suspicious activity and money can be obtained. Also, it is theft resistant.

Algorithms: The algorithm which is implemented on Aten Coin is X11. It is less susceptible to the 51Use cases: Users of Aten Coin can be banks, regulators, merchants, exchange, capitalist, organization, financial institutes or communities. In other words, it can be used by everyone who wants to spend their electronic money around the globe.

Limits: Its source code is not available yet. Aten Coin is used by big entities such as merchants and regulators but there is a need to increase the use of Aten Coin at marketplaces for example for buying a cup of coffee. It is only available in limited countries. It has no support for all the countries in the world.

Design: In order to get the Aten Coin, user has to follow two steps. First step is to get the Aten Coin wallet then user can buy the Aten Coin. In Aten Coin wallet, your email address, login and password is required. After creating an account, verification is required. The verification of the identity is carried out via driving license or passport. Also, webcam should be connected to the computer. Aten Coin takes 14 days to validate the identity. If the identity is not validated, account will be automatically deactivated. Aten wallet offers two main functionalities such as sending a transaction and mining the Aten Coin. By using the wallet address, Aten Coin can be received.

Comparison: The comparison of Aten Coin with other digital currencies is as follows. Atencoin is more fast, more secure and knows identity[26].

2.1.3 Blockauth

Introduction: BlockAuth enables users to own and operate their own identity registrar that allows them to submit their information for verification[8]

There are many services that need a secure user authentication system who also need to be assured of the authenticity of every user. Authenticity isn't just verification that a user is who they claim they are, it's verification of the facts that the user chooses to assert about themselves. A user can make any claim about themselves from their gender, age, financial class, visa status, or citizenship. The verification providers in the BlockAuth network will verify any information possible to vouch for those assertions on behalf of that user[27].

BlockAuthmakes a network of OpenID/OAuth login providers that uses a combination of machine-learning and human validation to verify the personal information of its users. These services will allow Bitcoin sites to outsource their Know Your Customer requirements and background checks to BlockAuth service[28].

BlockAuth has forked an existing OpenID Connect Provider software package and is making the necessary improvements to extend the metadata written into the standard to include additional data that can be passed along to any services that are configured to listen to them[27].

OpenID Connect is an interoperable authentication protocol based on the OAuth 2.0 family of specifications. It uses straightforward REST/JSON message flows with a design goal of making simple things simple and complicated things possible. It is uniquely easy for developers to integrate, compared to any preceding Identity protocol[29].

BlockAuth is creating a system so users can pick an Identity Registrar and verify their personal information. The Identity Registrars work hard to verify that each account is a real person and that every bit of information they assert is true[30].

The need of blockAuth arises when user claims its identity via name, age, gender, visa status or citizenship. The problem is, each time user has to identify himself/ herself in order to use multiple sites. In Figure 2.1, user interactivity with different sites is shown. If one user wants to create account at more than one site such as Facebook, LinkedInor Skype, the identity verification additional information is required for all these sites separately. Moreover, these sites need to perform the identity verification by themselves. If some personal information of a user changes, it will be required update it on all places. It turns out to be difficult, expensive and time consuming process.

BlockAuth allows websites to let users log in using an industry standard method without having to get their personal information, while still being secure in knowing that they can contact the user and that they're real and unique people [30].

BlockAuth aims to build an infrastructure to power a new generation of Authentication Providers to allow businesses to utilize Zero Knowledge Identity Verification. Goal is to

1.jpg 1.jpg

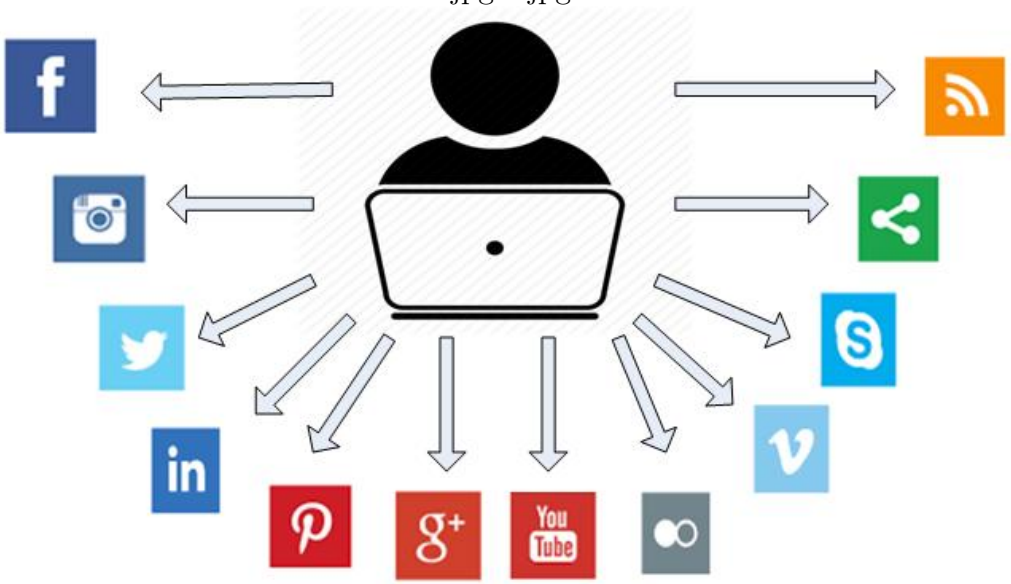

Figure 2.1: User interaction with multiple social application

allow users to prove their identity to an identity provider once and not have to prove it again to any websites that accepted the BlockAuth compatible logins. Benefits to business partners included guarantees that users were real people, unique, and meet any legal requirements to use the service[28].

This software package also lets users log in and enter their information, choose what they want verified, manage their account, and use additional features such as the micropayment system and privacy enhancement options that the Identity Provider wishes to operate.

Competitive Advantage: There are several companies that offer verification services but they tend to just facilitate specific verification techniques. By not placing the ownership of the results in the users ownership, those services charge different sites and services the same costs for repeated verifications. This is why BlockAuth is different from the existing services. The user has the ownership of the results of their authenticity verifications and can use that verification with any site that asks for it[27].

How it operates: Instead of having every merchant doing their own KYC / AML and user authentication, the BlockAuth solution is to have a marketplace where specialized Identity Registrars work to authenticate individual pieces of information. For example, one Registrar may specialize in authenticating phone numbers, another at authenticating addresses, and yet another at authenticating passports each without knowledge of the other information relevant to the person they are authorizing[31].

In BlockAuth system, the information provided is checked in terms of accuracy/correctness. It takes any kind of information that users want to be able to provide and verify it through a mixture of automated and manual processes. It allows the user to enter any personal information for identity verification e.g., identity information, location information, contact information, social media profiles etc. A franchise partner, licensed by the BlockAuth

with monthly membership fee in terms of tokens, will do the validation process. If a verification service has a high rate of incorrect verifications, BlockAuth might commission a spot audit of a percentage of that work in order to determine if the franchise partner should lose their license or be asked to stop verifying the category of information that they are showing a deficiency in[27].

The initial design asks for common bits of information such as name, gender, age, social media links, location etc. from the user. The BlockAuth systems are designed to allow any information that users assert about themselves to be checked for authenticity if there is a verification partner willing to perform the checks. This allows for the system to grow to meet the needs of websites such as a forum for Air Conditioner repair only allowing licensed AC repairmen or an investment platform that only allows accredited investors to participate[27].

The BlockAuth company operates with a token for decentralized decisions in the organization, the price of the tokens changes based on the volume of coins that are purchased with bitcoins[31].

In receiving the tokens, the partners maintain a stake in the operations and direction of the BlockAuth organization. The more tokens they hold, the more powerful their voice is. BlockAuth generated a total of 20,996,011 tokens for angel investors, accredited investors, developers and for public[27].

Advantages: Here are the few advantages of BlockAuth that distinguish it from other centralized services or applications:

1. There are also lots of industries that are expected to benefit from login ID provider services that are able to ensure that users are real human beings and that their submitted information has been verified[28].

2. There are also lots of industries that are expected to benefit from login ID provider services that are able to ensure that users are real human beings and that their submitted information has been verified[28].

3. The services that the BlockAuth providers will provide have tangible benefits from an extensive variety of industries from cryptocurrency exchanges to message boards to dating sites[27].

4. It will reduce the cost of repeated requests for identity verification with ownership of results.

5. It is an open source platform that believes in software movement.

Use cases: BlockAuth can be used in different domains. These are 1) cryptography exchanges 2) message boards 3) dating sites 4) demographic restriction 5) Microloans and micropayments. 6) Online communities or social networks[28].

Design: The BlockAuth system is built on the new OpenID Connect standard which is a combination of Open ID and OAuth systems that are popular for log in systems and API connections[31]. BlockAuth has forked an existing OpenID Connect provider software package and is making the necessary improvements to extend the metadata written into the standard to include additional data that can be passed along to any services that are configured to listen to them. BlockAuth hasaltered the software package to work with MongoDB in order to allow for proper storage of user information that fits our extended and flexible schema.

Technology Platform: [32]

1. OpenID Connect Platforms(s)
2. Anvil Connect (Coffeescript with Redis storage)
3. PHPOIDC (PHP with Doctrine ORM that supports several relational DB's)
4. Ideal DB Server
5. MongoDB RethinkDB
6. Message Queue Service: RabbitMQ
7. Front-end framework: Laravel
8. Containters: Docker
9. Orchestration Engine: Puppetlabs

BlockAuth plans torun it on cloud application platforms, like Google AppEngine or Elastic Beanstalk, in order to make it so our franchise partners can operate it with less of a need to hire system administrators to handle the difficulties of growth and server resources[27].

Privacy and Security: BlockAuth is designed in such a way that privacy and security is fully controlled by user. It is in userâs hand what information should be shared to public. Security of the user is very important to BlockAuth. For this purpose, messages are encrypted. There are two level of encryption. If a user demands high level security which means information is kept private, then multi parts encryption is applied. Multiple parties are required to decrypt the messages. If the user requires the messages to be displayed after approval, then encryption in a form is made. It will not disclose the information[27].

Challenges:

1. The BlockAuth project relies on building acceptance from a number of existing open source communities and integrating into a variety of libraries (while not insurmountable getting consensus on the BlockAuth approach will take time)[31].
2. The BlockAuth project will have competition from other KYC / AML providers who choose not to list their projects on the BlockAuth marketplace (though this may be mitigated by lower or no fees for the BlockAuth marketplace)[31].

3. Another open issue of BlockAuth is that team is making effort to shift the software to MangoDB to store the user information in database to accommodate the large number of users[27].

2.1.4 Bitnation

Introduction: Bitnation is the world's first operational decentralized borderless nation, based on blockchain technology. Bitnation provides the same services as traditional governments provide which includes legal services (ID System, Dispute Resolution, Marriage, Divorce, Corporate Incorporation, Birth and Death Certificates, Child Care Contracts), insurance services (Healthcare Insurance, Unemployment Insurance, Pension), social services (Education), diplomacy services (Advocacy, Direct Crisis Negotiations) and security services (Protection, Law and Contract Enforcement)[33].

The need to develop virtual chain on Governance 2.0 is based on observations of the following general patterns of human behavior [34].

- The majority of people do want various degrees of governance services; some want more and some want less, or none at all
- The majority of people want an easy choice of governance service providers - e.g., an end-to-end solution instead of having to choose between every single service provider themselves. Aggregation of services is a key part of the solution.
- Many people do not wish to leave their geographical area because of their attachment to their family, friends, work situation, and culture. Relocation should not be a requirement to choose your governance service provider.

The existing blockchain technology, along with others still emerging, enables governance 2.0 in its function of being a cryptographically secure public ledger [34]. Bitnation was founded in July, 2014 by Susanne Tarkowski Tempelhof [35]. After two months, in October, Bitnation did the first blockchain marriage, then the first Blockchain world citizenship, together with Chris Ellis from World Crypto News (WCN), was introduced. Not only marriage certificates and world citizenships were provided but in April 2015 it created the first land titles and the first birth certificate on the Blockchain. In November 2015, Estonia announced its cooperation with Bitnation to create a blockchain based public notary solution allowing anyone from the world to digitally notarize documents on the Blockchain[35]

BITNATION use a model of smart contract based Liquid Holacracy based on the philosophy of Holon, which means "something that is simultaneously a whole and a part", and mimics the way swarm like systems emerge in nature. BITNATION has upgraded the initial implementation of Holocracy into Liquid Holocracy, to increase the speed and autonomy of descision making processes, and the agency of individuals and holons[36]. Bitnation uses governance model, comprised of different entities with various degrees of autonomy: Core, Holons, Citizens, Laws, The Archipelago.

Core: The core is the lead of the holocracy, a small group of dedicated citizens, who are able to set the general framework, and make swift decisions. Generally, the founders and/or core developers. A new core can be created at any time, and the holons and citizens can choose to follow the new core. The responsibility of core is to manage the key infrastructure, including funds, wallets, domain names, general political positioning, core development priorities, etc[36]

Holons: Holons are parts within the Decentralized Borderless Voluntary Nation (DBVN), with various degree of autonomy, at various times. Holons are used to perform the operations. Any citizen can start their own holon, for profit or non-for profit, without any central approval. Citizens suggest Holons, and others can choose to finance them or work on them. The holons benefits from the DBVN resources and infrastructure[36].

Citizens: Citizens opt in or out on a voluntary basis, and can be part of several nations, or none at all. Citizens should contribute in some way, either through work, computing power or in other ways, to the nation. Citizens should have read the constitution, and signed off on the principles. Being a citizen means receiving dividend from the profit of the nation, and being part in building the nation. Itâs not required to be a citizen to use Bitnations services. Each citizen is subject to the reputation system, which serves as an incentive for good behavior. Bitnation accepts homo sapiens, as well as artificial intelligence (AI) agents as citizen [36].

Laws: Bitnation follows a Polylegal system, meaning people are free to choose the code of law of their preference, whether thatâs common law, sharia law, civil law, pashtunwali, or whatever it may be. People are also free to create new individual laws, or new codes of law. Laws can be refereed to, or coded into agreements. Laws are subject to reputation as well, and people reviewing law are equally subject to reputation of being good or bad at reviewing laws[36].

The Archipelago: The Archipelago is a loose federation of different virtual nations, allies, embassies, ambassadors who pledge to assist each other when possible, and desirable[36].

How it operates: Bitnation offers the same services as those provided by traditional governments, but in a geographically unbound way. Any individual from around the world can become a citizen of Bitnation by signing on to the constitution. Cryptoequity can be bought on cryptocurrency exchanges, or earned by contributing with work. The first version of the ID required users to prove their existence at a certain time by taking a picture with the latest Bitcoin merkle root, or the hash of all the hashes of all the transactions in a block. Then the picture is inserted into an ID template and the documents are signed with PGP keys. Later forms of identification have been simplified, in the current Bitnation World Citizenship ID, as well as the Refugee Emergency ID [35].

The ID created on bitnation acts as deterrent or reputation. It means that every individual needs reputation to perform the business deals. The absence of reputation is hindered from performing the many contracts such as marriage on bitnation. Decentralization involves in the Bitnation is the process of redistributing or dispersing functions, powers, people or things away from a central location or authority. In the realm of a DBVN, decentralization translates into both technological and human decentralization - through striving for P2P (Peer-to-Peer) technology, modular interfaces, API (Applications Programming Interface)

layers, and forkable (duplicated) code. This means that every user can become its own node and transform the platform to their opwn liking[34].

The blockchain transactional database has the basic record-keeping properties required of a governance system. Once the information is online, it exists forever on the network, preserved in millions of individual nodes. The blockchain has a rigorous verification process that is virtually impossible to crack once the network reaches a certain critical mass. It can record births, marriages, deaths, property ownership, business contracts and a variety of other records traditionally created and held by governments. The identities of individuals on the network can be established definitively through their unique âsignaturesâ, and in turn, those individuals can sign and verify transactions (e.g. the attending physician at your birth or the official recording your wedding). Instead of a government official acting as notary or other trusted third party verifier, the consensus of the blockchain now takes on that role [34].

In essence, vision of bitnation is to make the choice of governance service providers for individual users as easy as choosing to join a social network (Facebook, LinkedIn, Twitter, etc). Users can choose several of them or choose none. Users will also be able to create their own DBVN through forking the Bitnation source code[34].

Advantages: The following advantages in bitnation makes it acceptable globally

1. Bitnation provides secure nation; bitnationâs user can live their lives without getting security risks. It handles the crisis management 24/7.
2. Bitnation gives the option for living a life of your own choice, anyone can live as communist commune like kibbutz or capitalist city like Hong Kong or combination of two.
3. Bitnation will not sell the data of citizens or customers to any entity, under any circumstances. It strives for client side technology, encryption, and pseudo anonymity.
4. Bitnation doesnât judge or select based on the color of your skin, ethnicity, religion, country of origin.
5. Bitnation honor the Non-Aggression Principe (NAP) moral framework. Bitnation stand unified against any and all forms of coercion, whether itâs through violence, or the implied threat of violence.
6. Bitnation users can send and receive any amount of money instantly by using crypto currency, at anytime, anywhere in the world. Users have full control of their money, even on bank holidays. Bitcoin users can also protect their money with backup and encryption. [37]

Use cases: It will facilitate the state governments and organizations to be more cheap and secure. Bitnation is currently working in 1) insurance like structures, 2) e-resident systems, 3) refugee emergency response and 4) Decentralized Borderless Voluntary Nation (DBVN).

In November 2015, the virtual nation started the Bitnation Refugee Emergency Response (BRER) program in response to the refugee crises. This project provided an identification system called Blockchain Emergency ID (BE-ID). The BE-ID allowed a person to receive an ID recorded on the blockchain for those who cannot get other identification documents. With this ID, people were able to receive social assistance and financial services. The ID form generated a QR code which could be used with a cellphone to apply for a Bitcoin Visa Card which could be used throughout Europe and the UK without a bank account. The cards allowed the refugees to accept transfers and donations from anywhere in the world, through a Bitcoin public address[35].Additional services were also added including a map and a forum to track lost family members, safe locations and dangerous locations.

Design: Pangea is Bitnationâs polycentric decentralized Jurisdiction, on which Virtual Nations can be built, agreements among Citizens (and between Citizens and service providers) made, and disputes resolved. Pangea is also an incentive network which can be used to host a range of future governance services for Virtual Nations as DApps and bots. The Pangea Software is a Decentralized Opt-In Jurisdiction where Citizens can conduct peer-to-peer arbitration and create their own Nations[].

Until a better language is mainstream available, Smart Contracts will be written in Solidity. Ethereum is the first blockchain to be integrated with Pangea, for the purpose of creating Smart Contracts. Bitcoin will be integrated as soon as the Rootstock protocol - which is also using Solidity - has been publicly launched and tested on the market. The recently launched Tezos decentralised ledger is another potential alternative, as well as future chains like Tauchain, EOS and post-blockchain technologies like Tangle and Bitlattice. As other more secure alternative contract languages and blockchains emerge, they can be integrated too. (Tempelhof, Pangea Jurisdiction, 2017)

Challenges: Bitnation is looking for further improvements in its network such as socio political environment and advancement of true global peace. So far, the platform's services are limited and interest is negligible. Bitnation embassies are thus limited in the services they can provide. An asylum seeker could ostensibly come and stay at Schloss Heinrichshorst, but international protection couldn't be guaranteed.

Still in a largely experimental phase, only one couple has signed up to be married through their online platform. Bitnation has nearly 4,000 citizens flung across the globe, though the majority and its spokesperson are based in Europe which represent the limitation of the company[39].

Adaptation challenges consist in the initial educational process of advertising blockchain technology as a secure public ledger, and second will be in regional and cultural adaption[34].

2.1.5 Block Verify

Introduction: Block Verify was founded by Pavlo Tanasyuk in October 2014 [40]. Block Verify provides the anti-counterfeit solution. The use of blockchain technology in order

to improve the anti-counterfeit solutions in different domains such as pharmaceuticals is available through Block Verify application. Block Verify has also targeted the area of supply chain in order to identify the counterfeits goods. Supply-chain is a process of creating goods from raw material to the finished products. It has multiple players or actors such as supplier, vendors, partners and distributors as shown in Figure 2.2.

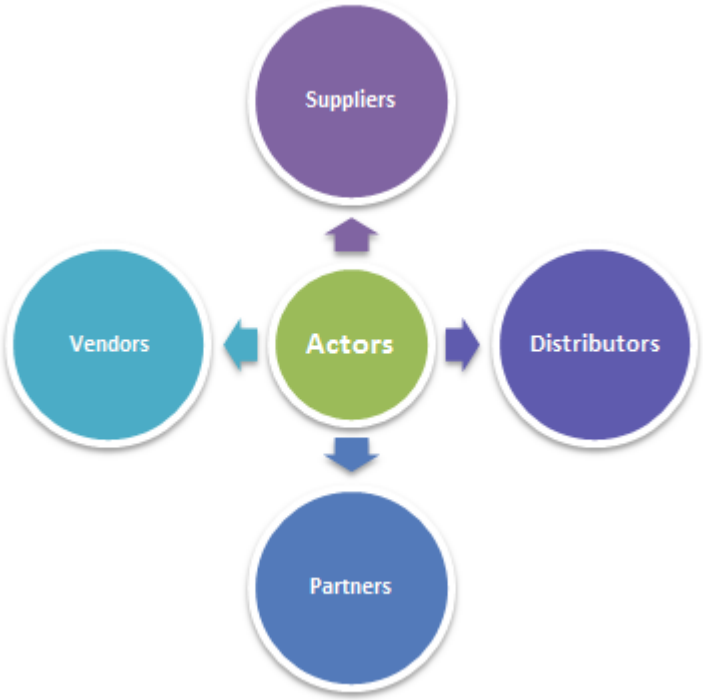

Figure 2.2: Actors of Supply chain

The need to introduce Block Verify arises due to the following question

1. What if workers in the field and consumers at the time of purchase could scan a QR code on the box and know immediately that their product was authentic?

The US Food and Drug Administration (FDA) wrote in 2013 that more than a third of anti-malaria drugs available in Sub-Saharan Africa and Southeast Asia are counterfeit or substandard. Fake malaria and tuberculosis drugs cause about 700,000 deaths per year, according to the UN in 2012. [41]. This is what Block Verify wants to make possible by using the bitcoin blockchain, âthe most trusted immutable data store in existence[41].

These services/functionalities are being offered to the user of Block Verify [42]

1. Identify counterfeits: Helps users/professionals with their many problems over identifying counterfeit goods.

2. Non duplicable: Blockchain offers a transparent environment where it is impossible to duplicate products.

3. Companies verify: Companies can create their own register of products, and monitor the supply chains.

4. Global solution: Block Verify creates a truly global solution for connected world.

In short, London-based startup Block Verify aims to use the blockchain to authenticate a wide range of high-value goods (ranging from mobile phones to diamonds) to simplify sales tracking and product verification[45].

How it operates: Consumers need not to be worried about the possibility of duplicate product identification numbers any more than they have to worry about Bitcoin double spending, because the system will be âtoo sophisticated for that.â Eventually, any type of product will be verifiable through Block Verifyâs service, including name brand clothing, electronic tablets, and precious jewelry. The system will also be able to discover diverted goods, stolen merchandise, and fraudulent transactions[41].

Improving anti-counterfeit measures can only be achieved by using a decentralized, scalable and tamper-proof solution. Block Verify will make use of a private blockchain, a highly scalable transparent protocol, in order to assign every manufactured product as an asset. All of these assets will then be added to this blockchain and assigned a unique identification number called hash.

The Block Verify team will use a private blockchain simultaneously with the Bitcoin blockchain, which they will use as a ledger to hash certain data to secure [their] own chain. They will give every product its own permanent record on their blockchain, making manipulation of private keys impossible, says Tanasyuk. The system is designed to protect everyone at each point in the supply chain, creating a trustful system of transparency[41].

Block Verify system relies on two blockchains working together. An internal blockchain will be maintained by Block Verify, that will store pertinent information on licensed products. Bitcoins blockchain will be utilized for confirmation of events and actions related to the internal chain maintained by Block Verify. We are not hashing the full history of ownership into bitcoin blockchain, but using our own private blockchain. We use bitcoin as a trustless environment to confirm important events within our own chain[44]

The blockchain will verify these hashes in order to determine whether or not the item in question is legitimate or counterfeit. Whether its a handbag, a tablet, or more importantly â a medicine, any and every item in the world will be verified through the blockchain. And this is where this major of technologys strength comes into play: anyone in the world can access the blockchain without any restrictions, and conduct their own item verification[45].

The blockchain technology applied to supply-chain management addresses the issues of counterfeit by enhancing the transparency and security and solving the problem of trust. In particular, by using the blockchain technology to trace back the journey of an item

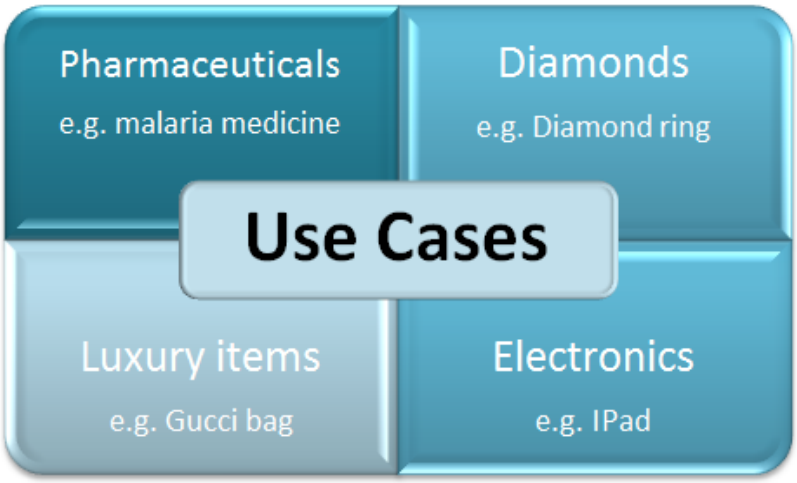

Figure 2.3: Use case of Block Verify

through the supply chain, Block Verify assigns a unique code to a product, which can be tracked on the distributed ledger (the blockchain) and monitored at all stages along the value chain by all parties involved in the transactions. This enables the identification of diverted products, stolen merchandise, fraudulent transactions and counterfeit goods. Block Verify can be applied to management of the supply chain of high-value items, including pharmaceuticals, luxury goods, diamonds and electronics [46]. **Advantages**:

The advantages linked with Block Verify are given below

1. The brands are protected with embedded anti-counterfeit mechanism by using Block Verify.
2. With Block Verify, we can pay the accurate amount of the product which was not possible before due to absence of transparency in supply chains. The buyer can track back the purchased product to its raw material without any difficulty.
3. Block Verify facilitates the customer in identifying the price, date, location, quality and state of the product[42].
4. Block Verify is creating the ability to identify items that are diverted and not suitable for a particular location [47]
5. The blockchain prevents malicious individuals or groups from creating duplicate item records[45].

Use cases: The four targeted domains are pharmaceuticals, electronics, diamonds and luxury items depicted in Figure 2.3.

In pharmaceuticals, the authenticity of products is ensured. By using the block verify, the economic damage is hindered which cost the hundreds of thousands of lives every year.

For this purpose, scanning of QR code is done [43]. In electronics, customers are delivered the original products. In diamonds, the trust in increased by certifying the diamonds and preventing the frauds. In luxury items, quality is assured by working close to the luxury manufacturers.

Design: Block Verify has introduced the way we produce, market, purchase and consumes our good with distributed ledger i.e. blockchain. It has added transparency, security and traceability. Moreover, each product in Block Verify is validated and recorded which makes it anti corrupted and history of verified products can be accessible to the customer.

The design of Block Verify is represented in Figure 2.4 and it is as follows;

1. The productâs authenticity is ensured at first step.

2. In second step, it verifies that product is not in possession already. So, it offers no counterfeit or replicate. Also, it can verify the diversion of the product from its original destination. It helps in tracking the products from stolen merchandise [42]. Supply chain is verified and we can make it transparent to the extent we want it to be.

3. In last step, the product is labeled. So that customer can check the genuineness of product. Product labeling is done with the help of Block Verify tag that can be Qr code, 2D barcode, nfC and other methods[48]. Unique codes cannot be duplicated.

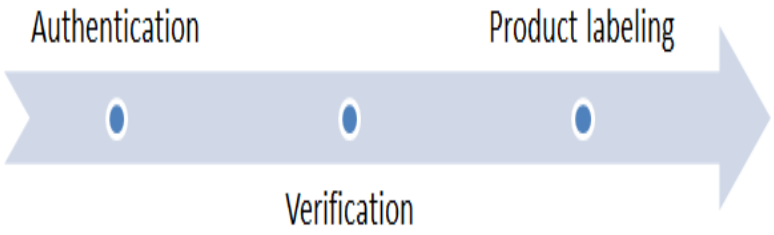

Figure 2.4: Steps of Block Verify

This whole concept relies solely on a trustful platform in the form of the blockchain, which not only holds all of the vital information, but is also given absolute trust by Block Verify. Absolute trust is achieved by putting information on both the private and the Bitcoin blockchain, providing a transparent database to the level that is needed[45].

Challenges: With every emerging technology, hidden or visible obstacles are always present which can prevent the blockchain technology for adoptions. These parameters can be extreme cost, organizational resistance and management conflicts among the partners. Mostly organizations shy to change the large software systems such as supply chain organizations with Block Verify[49].

2.1.6 Cambridge Blockkchain LLC

Introduction: Cambridge Blockchain was founded in 2015 by CEO Matthew Commons. Other founders are Alex Oberhauser and Alok Bhargava. The company is based in Cambridge, USA. Cambridge Blockchain provides digital identity enterprise software for financial institutions such as multinational banks[50]. The need to develop Cambridge blockchain arises to facilitate the blockchain technology in identity management which is decentralized. The problems with centralized compliance databases are here; 1) Centrlaization offers the struggle to meet the conflicting priorities 2) Centralization results in duplication of the same identity checks across institutions and severe impacts to customer experience and operating costs[51].

The proposed solution known as Cambridge Blockchain has following qualities[51]

- With Cambridge Blockchain, global privacy requirements are met.
- Elimination of redundant compliances is facilitated.
- End user experiences are improved.
- It provides lower costs to its customers as compared to other identity management applications.

How it operates: Cambridge Blockchain not only solves the problem of enabling strong digital identities at a global scale but also provides individuals control over their identity data. This platform facilitates client control of their own personal data in a single, unified version through a virtual container called a Personal Data Service (PDS). Using the PDS, a user can do the following task[51];

1. Pre-approve automated rules that allow financial institutions to access the data.
2. Ensure that each division is working with the most updated version of the data.
3. Confirm that the data is identical to what has been checked by another trusted party. The shared blockchain ledger does not contain any personal data, but rather cryptographic proofs that can attest to the validity of personal data (and who has signed it) along with an auditable and trusted tracking of changes.

Cambridge Blockchainâs identity blockchain solves this quandary by combining blockchain technology with a Personal Data Service (PDS). The PDS concept was developed by ID3âs Open Mustard Seed to permit individuals to collect and share data in a secure, transparent and accountable way through encapsulated data management. The goal of this new blockchain-linked PDS system is to meet both privacy and KYC requirements in the same system through the selective release of personal information to only authorized counterparties on a controlled, as-needed basis [52].

The LuxTrustâs (a leading European Trust Services Provider) current certified services such as authentication, signature and document management are combined with blockchain-based enterprise software. As a result of this collaboration Cambridge Blockchain will deliver the future of digital identity for Europe and beyond[53].

Cambridge Blockchain will facilitate a tool for validating secure digital identity documents, processing electronic signatures, and recording transactions. Since this is a new blockchain, it begins with a Genesis Block. All subsequent data entries in the blockchain must reference this genesis block through a chain of strong cryptographic proofs. Any attempt at manipulation of blockchain data will break the chain of proofs, making it effectively impossible to alter records without detection[54].

This architecture permits integration with any public or private blockchain system, allowing system participants to validate identity information about counterparties in a selective and context-aware fashion. It aims to be most respected identity platform for blockchain transactions.

Advantages:

1. Cambridge Blockchain distributed architecture resolves the competing challenges of transparency and privacy, resulting in faster customer on boarding, lower costs, and enhanced compliance through a single, trusted and consistent view of customer reference data. [50].

2. Cambridge blockchain provides the reliably and flexibly managed leading to seamless transactions, operational efficiencies and strong privacy.

3. âWorking with Cambridge Blockchain allows to augment the scope of identities, including any attributes, and will enable users to share personal data fully respecting the increasingly stringent European regulatory framework. It is used to fill gaps in compliance, security and trust needed to accelerate digital, personalized and automated services across Europe and worldwide.

Use cases: The use cases of Cambridge Blockchain are listed below

1. Banks: The banks wind up in a position in which they spend time and resources conducting what are essentially redundant checks on customer identity[55].

2. Financial institutions: Applications will cover rapid onboarding and know-your-customer checks for financial service providers.

3. Medical and internet of things: Broad range of personal data sources such as health records and Internet of Things (IoT) devices are also facilitated by Cambridge Blockchain

4. Insurance like bonds: Cambridge Blockchain reduces time and cost for bond issuance (Commons, 2016).

5. Wealth Passport: Streamline digital identity checks for global private wealth managers[56].
6. Identity network: Bank funded entity for the customer ownership of personal identity data[56].

Design: In Cambridge Blockchain, smart contracts are digitally signed documents that govern how such data may be released, powered by an engine to run the smart contract code. Cryptographic proofs of all information are stored on an identity blockchain shared by all system participants, says Matthew Commons, CEO of Cambridge Blockchain. The resulting system allows the selective release of personal information to only authorized counterparties on a controlled, as-needed basis[57].

The platform will instill state-of-the-art privacy by design principles outlined in the General Data Protection Regulaxdtion (GDPR) to provide quick on boarding, attribute, consent management and compliance services for natural persons, legal entities and devices with full transparency and auditability of transactions. Data and privacy policies are established through a single comprehensive system, accessible via user-friendly mobile and web applications[53].

Challenges: Permissionless, open blockchain architectures such as bitcoin or Ethereum typically achieve privacy through anonymity (or pseudonymity, with identification only via a public-private key pair). While censorship resistant, these blockchains are often incompatible with financial institutions regulatory requirements for customer identification. On the other hand, many permissioned blockchain designs for financial markets envision that all participants are explicitly identified, with key pairs tracing back to known individuals or entities. This traceability aids regulatory compliance and audit work, but often comes at the expense of privacy. This is problematic because even if the specific details of trades are encrypted, market participants may be harmed by the revelation of trading activity levels and counterparties. Conventional blockchain designs may thus put financial institutions in a quandary, with the impossibility of meeting both KYC and customer privacy requirements within the same system architecture[52].

2.1.7 Civic

Introduction: Civic was developed by Vinny Lingham (CEO) and Jonathan Smith (CTO). Civic is building on trust and it is used to create an Identity Protection Network where consumers could signup for free identity theft protection services and, in the process, allow Civic to verify and authenticate who they are. This strategy has helped us build and create systems for ID Verification that will be the underpinning of creating Digital Identities for everyone.

Civic application looks and works like a digital wallet, but instead of money, it secures personal information, while allowing users to selectively share it. The Civic app offers a variety of ID-aware services, from password-free website logins to storing important data like healthcare records[58] . Also, Civic uses a smartphone fingerprint scanner to authenticate users. The information can then be shared directly with companies and individuals, which can confirm the data by referring to Bitcoin's blockchain. [58]. Furthermore, an

example of Civicâs applicability is Government can use the Civic platform and issue the passport or license directly to the Civic user.

Civic was introduced as a decentralized counterpart to existing social identity applications like Facebook. Civic works on these following principles;

1. The difference of Civic and other centralized identity providers is that Civic will enable users to prove their uniqueness â without sharing that information with a website.
2. Civic works by leveraging blockchain-linked private keys, which are stored on consumers mobile devices.
3. Civic technology provides an user attestation service that would serve as a layer between someone seeking to establish certain information about a person and that end user[59].
4. Toward this goal, Civic will offer three levels of access: anonymous or private, where no information is shared, then two levels with which users can selectively make certain data available [59]
5. Instead of information being exchanged, a website that wanted to know if someone was 18-years-old, could verify that this was true against hashes on a blockchain, in this case bitcoin, that are verified by Civics technology[59].

How it operates: The identity transaction is a voluntary information exchange between the user and the Identity Requester, with the Civic Secure Identity Platform (SIP) securely sharing validated data. The process is initiated by an individual downloading the Civic App, establishing an account, and verifying their identity thereby becoming a Civic user as shown in Figure 2.5 below.

The requirements of this verification process are set by the Identity Requester. Civic unique product offering allows real-time authentication of identity data verified by Civic or a Civic Identity Partner, such as a government entity, financial institution or employer[60].

How Civic Verifies Data: Once identity data is provided by a user, Civic uses multiple identity validation service providers to verify submitted data against phone, credit, social media, and other public records. By combining multiple reputable sources with fraud detection algorithms, manual auditing, and our own internal decision engine, Civic maintains a high pass rate for legitimate users while mitigating the risks of fraudulent behavior. Civic pushes the verified identity data to the user's Civic App and attestations to the blockchain[60].

How Third Parties Verify Data: Leveraging the Civic Secure Identity Platform APIs or SDKs, a Civic Identity Partner with Civic technologies may provide users with verified identity data (including pushing verified data to the Civic app and attestations to the blockchain). Since the Identity Requestor still defines the requirements for identity validation, Civic can work with a range of Identity Partners to establish various levels of trust, including strong multi-factor authentication across multiple Identity Partners[60].

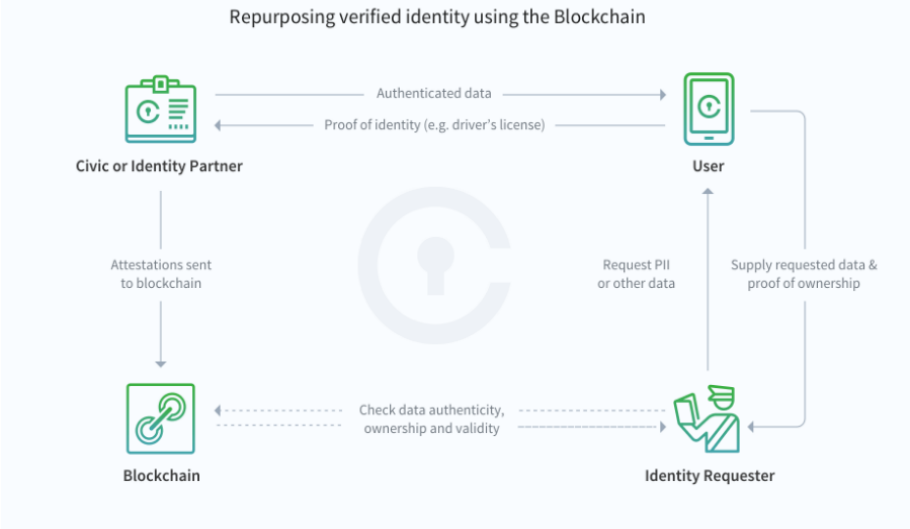

Figure 2.5: Architecture of Civic

Civic Identity Partner Examples: A government agency is able to directly push authenticated identity data to the Civic app and be the authenticating authority, resulting in trust and acceptance similar to physical forms of identity, e.g. driver license or passport. Civicâ architecture establishes greater trust and confidence since Civic cannot be forced by another party to revoke the verified identity data. A financial institution issues verified identity data to their customers for improved internal and external customer experience, e.g. using real-time authenticated identity data for secure travel requirements such as boarding a flight. Since the verified data is shared directly with their customers, Civic does not see or store their sensitive data. This verified data is accessible to the member for real-time authentication through a biometric verification, e.g. fingerprint, 3D facial recognition, heartbeat, etc.[60].

Civic never has access to any user private keys as stored on the public blockchain. Civic only receives hashes of the identity data along with a blockchain address to store the hash. Identity data is stored fully encrypted on the userâs device. Since hashes of the identity data are undecryptable by design, neither Civic nor the blockchain is vulnerable to exposing identity data. The Civic platform is therefore not a valuable target for hackers due to strong encryption and decentralization of the data[60].

Authentication: An Identity Requester can request verified identity data from a member with the Civic app in a variety of technologies. This includes Bluetooth low energy, QR code and near field communications, to name a few. Prior to approving the request, additional biometrics can be required to verify the user is sending their identity data, e.g. 3D facial recognition, voice[60].

After the user approves the request to send the Identity Requester verified identity data, a key to hash of the data and an address on the blockchain, the Partner generates

1. A hash with the Civic SDK,

2. The identity data
3. User provided key

The Partner then independently conducts a real-time authentication with data at the user provided address on the blockchain. By determining the level of trust for the identity data with the public identifier on the blockchain (e.g. USPS, Civic, State Department). Comparing the hash received from the user to the hash on the blockchain, ensuring the data is the same. Verifying the data has not been revoked, or no longer valid[60].

Advantages: Following are the advantages of civic application [60]

1. The need of username, password, third party and hardware tokens is diminished. Secure identities are created using Civic and can be used worldwide.
2. Traditional identity monitoring services typically charge a monthly fee to monitor your credit report and alert you when there have been changes. Civic is totally opposite, it is free of charge application for its consumers.
3. The fully encrypted data on the userâs device is an advantage which is difficult to decrypt.
4. No Proprietary Software or Infrastructure is used in Civic. Civic uses the public blockchain. This means that Identity Requesters do not have to invest large amount of money to set up the technology infrastructure to support the Civic Identity Platform solution.
5. Identity data is revocable by the authenticating authority. For example, if a member changes their last name, then the former/invalid last name data is revoked on the blockchain by the authenticating authority.
6. Identity data is encrypted and stored in the Civic App on Member mobile devices.
7. With third-party authenticated identity data, Civic cannot be compelled by a foreign government or criminal organization to invalidate identity data.
8. Users store and share their own identity anywhere in the world. Their data is accessible anywhere in the US, Europe, Africa or Asia.
9. Civic Technology uses the power of the blockchain to ensure the highest quality privacy and security for your business.

Use cases: The information is secured on user's device (and backed up to whatever backup provider you use for your phone), user can use this information to do any of the following: [61]

1. Open new accounts with banks other institutions, or just websites apps.

2. Passwordless-entry into websites and apps built-in 2-factor authentication
3. Private signups to sites and apps (they can let you signup without taking ANY personal information)
4. Store your cryptographic keys and any other personal information, like health records, etc.

Civic is applicable to the various domains. These major domains are [60]

1. Financial: Civic does not support the fraudulent activities in financial organizations/ financial institutes. Civic is used to verify the identity data and it provides multi-factor authentication with simple user experience.
2. E-commerce: Reduce the impact of data breach by not storing user Personally Identifiable Information (PII) with credit card data. Avoid identity fraud with a Civic verified identity.
3. Medical: Allow Civic members to securely store and instantly share authenticated medical records from their device with the Civic application.
4. Crypto currency: Secure new account creation using Civic verified identity for KYC. Multi-factor authentication for web and mobile apps.
5. E-signature: Better user experience with more options to establish various levels of trust in the identity of a signer of a document
6. Social: Secure account creation that offers varying levels of privacy to your users, including anonymity or verified demographic attributes.

Civic aims to become the trusted third party source for securing and verifying your identity. Civic is building partnerships with banks, credit card companies, online lenders, wireless and cable providers, employee verification services - in fact, any institution that uses your identity[60].

This system is made possible through Civic's Identity Protection Network, which will be a network of businesses who collect usersâ personal data, including their Social Security Number (SSN). This network could include members like banks, financial services, healthcare organizations or any other company that asks for your SSN. Consumers will be alerted when their SSN is used by a Civic partner[62].

Design: Civic is working offline and online. This application is available on smart phones. Civic has its own protocol called ChainAuth. The protocol is a new alternative to OAuth, which is used by thousands of companies including Google, Facebook, Microsoft and Twitter. OAuth is an open standard for access delegation, most commonly used as a way to allow internet users to grant websites and applications access to their personal information, without handing over their passwords. Using Bitcoins blockchain as the only third party, ChainAuth is a far more private solution, according to Civic[58]. Users

personal information is never stored on the blockchain, but we utilize the cryptographic infrastructure to ensure that the data on your device is never changed or compromised[61].

Data is encrypted on the device and to access this data biometrics is used. The validity of the data is ensured by hashed identity and flags. If a stranger is using civic personal account, alerts are generated and send via email and mobile applications. This will alert the user against identity theft[60].

An individual downloads the Civic App and completes an Identity Validation Process customized to the Civic Business Customer requirements. This process verifies PII to ensure ownership of the identity with enough data to establish the level of trust required by the Civic Business Customer. In other words, more PII may be collected to establish a high level of trust, e.g. scanning of passport, drivers license and social security number, while only minimal PII, e.g., only email and mobile phone number, may be collected for new users when the Civic Business Customer only wants to verify the user is real and unique.

After validation, the user is now considered a Civic Member with authenticated identity data secured in the Civic App on the userâs device, not stored by Civic. The Civic Member may share this previously authenticated identity data with Civic Business Customers, businesses that enter into a partnership with Civic. Civic Business Customers leverage our blockchain technology for real-time authentication of Civic Member identity data[60].

Civic also offers additional features to help protect your identity such as

1. Identity Monitoring Alerts: Civic's fraud notifications help keep your identity safe. Through credit bureau alerts, Civic empower you to take control of your identity
2. 24/7 US-Based Fraud Support: Whether you need help setting up your Civic Membership or assistance after discovering potential fraud in your name, Civic offers US-based support services when you need it most. Through Civic's partner network, you have access to experienced identity fraud investigators to help guide you and recover any funds you might have lost
3. Civic has an important feature to pay theft recovery to its customers.

Challenges: This application aims to develop new features such as stolen funds replacements, data beach notification, black market monitoring and secure ID authentication application. The details of these challenges are given below; [60]

- Stolen funds replacement: This new feature will allow Civic to refund stolen funds back to you (up to your set limit amount), even if we are unable to recover your funds during the course of working with an identity fraud investigator.
- Data breach notifications: Civic will be keeping a closer eye on the ever increasing number of data breaches happening around the globe. As Civic identifies new breaches, we will send out a customer wide alert, allowing you to take action if needed.

- Black market monitoring: Civic's technology keeps an eye on the dark web where hackers buy and sell identities for fraudulent use. By monitoring these sites for your name, Civic can be the early warning system you need to stop identity theft before it happens.

- Secure ID authentication problem: Your Civic Membership gives you access to our expanded Civic Business Customer network. Get access to features like automatic account creation and secure private login to access websites securely without cumbersome two-factor authentication

2.1.8 Credits

Introduction: The founders of Credits are Eric Benz, Nick Williamson and it was founded in November 1, 2014 .Credits is a blockchain platform provider offering a Platform-as-a-Service (PaaS) with tools for building secure and scalable blockchains to power enterprise applications. The Credits framework is purpose-built to be seamlessly and securely interoperable with other legacy systems and blockchain providers. As an infrastructure provider, Credits is able to leverage the growing use and investment in blockchain technology across all sectors and applications.

Credits platform enables enterprises to quickly and easily build robust blockchains that address the challenges of establishing provenance, authentication and reconciliation faced by many industries. The platform allows to create encrypted digital identities to substitute dozens of usernames and passwords while offering greater security features would save enterprises, institutions, governments and customers, time, energy and money. A golden record for identity which would work not only at a bank level but across the globe in all electronic environments[8]. The Credits Blockchain is a disruptive technology platform that uses strong cryptography and a distributed messaging protocol to create a shared trusted ledger between trading counterparties. Credits is a hybrid platform that facilitates interoperability between private and public chains[63].

How it operates: The following components are used in Credits in order to perform different operations.

Credits Core: As any blockchain - the Credits blockchain consists of Blocks. And every block contains transactions that happened since the previous block created. Unlike other blockchains, the Credits blockchain also contains States, which are snapshots of the contents of the blockchain created after each block is appended to the blockchain[63].

Blockchain State: While still being a blockchain, Credits Core blockchain starts with the state and not a block. The State, or state of the world, is simply just a key-value map of data. Credits Core has one global state object, that is comprised of many different models. The Dapp models are effectively data models and are used to define the data structure that is supposed to go into specific substate, and also provide an FQDN (fully qualified domain name) that will be used to reference that part of the state. There can be multiple different models in the global state, and it can contain arbitrary values, all

that is important is that every key in the state is a string. An example of a traditional state as shown:[63]

”works.credits.loans”:

”Bob”: 200,

”Dave”: 200

,

”works.credits.balances”:

”Alice”: 100,

”Carol”: 100

In the example above there is a works.credits.balances model and a works.credits.loans model. Each model has to have an FQDN key and may have entries inside it. You can define as many models as you need inside the global state. Inside the model you can have an arbitrary number of key-value pairs. Usually, Core addresses are used as the keys in a model but this doesnât always need to be the case, as the keys nature depends on applicationâs business logic. The model is ordered by insertion order and the whole global state is hashed to provide a state hash. The initial state of the world may be referenced as Genesis State, but normally itâs called just state 0 [63].

Blockchain Block: Essentially a block is just a collection of transactions. Blocks are formed by taking valid unconfirmed transactions from the internal transactions pool and making a block that contains these transactions. Once the block is formed it is distributed in the network and nodes can decide to vote and commit to this block. A block also contains information on the previous state of the world that it is built on. By referencing the previous state, a node can take the block, check that it is starting in the same place as the creator of the block, apply the transactions and calculate the next state. Assuming all nodes are following the same logic â all nodes will compute identical next state. If that is not the case â network partitioning will occur, and this edge case is discussed a little later [63].

Blockchain Structure: Building from states and blocks the chain is formed. Because Credits blockchain has intermediate states itâs not a direct link from block to block, instead, a block is formed from the current state, and then the application of that block to current state forms the next state [63]. Imagine starting at the following state 0:

”works.credits.balances”:

”Alice”: 100,

”Bob”: 0

And there is a transaction that moves 50 credits from Alice to Bob. This transaction can apply to state 0, so it is formed into a block that builds upon state 0 [63].

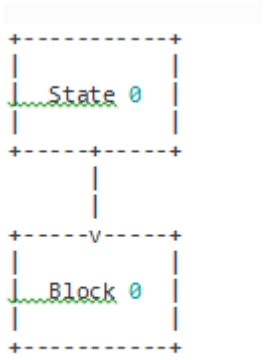

Figure 2.6: State 0

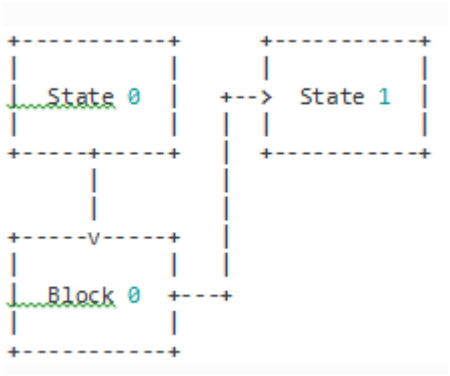

Figure 2.7: State 1

The block is then distributed between the nodes and references the state it is built on. Once the network agrees to make this block the next one in the chain each node applies transactions in this block to state 0 to produce the next state [63].

The new state 1 looks like the following: (Credits)

”balance”:

”Alice”: 50,

”Bob”: 50

A new transaction is formed and posted to the blockchain, this transaction moves the remaining 50 from Alice to Bob. Another new block is formed looking like such: [63]

The process continues and block 1 will be applied to state 1, forming the next full state.

Leaving it with a final state of: ”balance”:

”Alice”: 0,

”Bob”: 100

From here onwards other transactions can happen, further mutating global state and adding new blocks to the chain. The process will run indefinitely as long as there is a

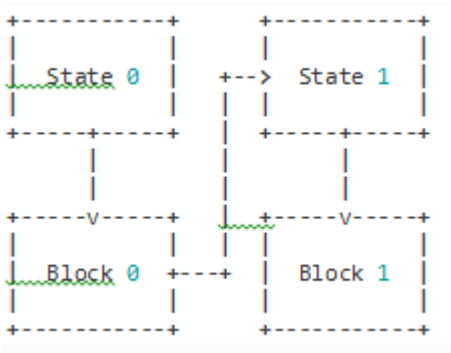

Figure 2.8: Next state

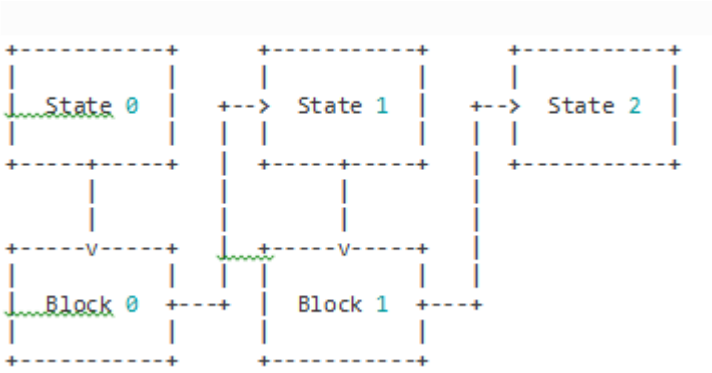

Figure 2.9: Block 1

quorum of nodes in the network to agree on blocks and new valid transactions are coming in. [63]

Credits Core Consensus: Credits Core consensus is a leaderless two-phase commit algorithm with variable voting power. This means that each and every DLT (Distributed Ledger Technology) network participant is equal in its rights to gather transactions from the unconfirmed transactions pool and form a block, and they are free to vote on the blocks that make the most sense according to current block validation rules. Also, votes may have different weights though according to voting power distribution for a given network. Essentially Credits Core consensus is a variant of Proof of Stake algorithm [63].

Consensus example sequence: Assume a network of three nodes, A B and C. Network starts at height 0, no blocks exist yet and the current state of the network is state 0 [63].

1. Node A receives a valid transaction from a client through HTTP gateway.
2. Node A verifies the transaction and onboards it, adding it to the unconfirmed transactions pool.
3. Node A recognizes new transaction in the pool and tries to form a block
4. Node A forms a block proposal and sends it out to other nodes in the network.
5. Nodes B and C receive the block proposal and verify the proposed block for validity.

6. Nodes B and C confirm block validity and start voting on the block. This is the process of voting, phase one of the consensus algorithm. At this point only one block proposal exists, so all votes are given to this block.

7. Votes are exchanged and if one block reaches the quorum of Voting Power backing â it is now avoted block. The phase one is done.

8. When the node receives enough votes on a block and thus finds out that the block was voted, the node goes into phase two of the consensus algorithm â committing to the block

9. Once the selected block has received quorum Voting Power backing - it is considered committed to be the next block in the chain. Phase two is done.

10. Every node receiving the block with enough committing VP attached to it adds this block to the chain and persists it on whatever storage is used with that particular node.

11. The process can start over from scratch if there are new transactions in the pool. In a more complex real life situation, there will be multiple transactions forming block proposals on different nodes and nodes will exchange and vote on proposals until one of the proposals reaches the quorum [63].

The consensus algorithm depends on several things: [63]

a. There has to be a required quorum defined. The current default is at least 51

b. There has to be voting power available in the system, and whoever is executing the votes using it â has to have access to the corresponding private keys. This is discussed in more details inVoting section.

c. There has to be a connection between nodes that will allow propagating the blocks and votes. Given these conditions are met - the consensus algorithm will function correctly.

Voting and Voting Power: Voting in Credits Core consensus is strongly tied to Voting Power (VP). VP is one or more arbitrary integer values assigned addresses on the blockchain. These values are stored in the blockchainState and represent the weight of votes allocated to each of these addresses [63].

”credits.voting.model.voting”:

”19joM8wBG7bAmBypMj23DBmmjGmqfxL4Bj”: 100,

”14RixTSeLtit5GJoDKdEJ23ob74vcvcFvv”: 100

Example above is a subset of the blockchain state showing two addresses with 100 of voting power assigned to each. The VP figure itself assigned to each address is of little importance, what matters is the relative weight of VP of each address to the total VP declared [63].

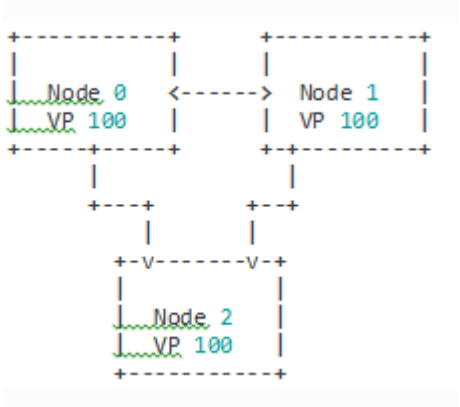

Figure 2.10: VP figure

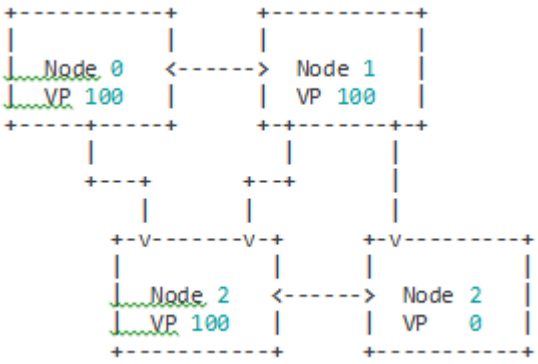

Figure 2.11: VP figure 2

To use this voting power, i.e. cast a vote one must have in possession the private key corresponding to the address VP is assigned to be able to prove the ownership. By default, every node of the Credits DLT network holds a private key to one of the VP addresses and casts votes with it, and VP itself is split equally between all parties. However it is totally possible practically to create new addresses and assign VP to them, imbalance the system by giving some addresses more VP than others or strip out VP completely from some addresses (set to 0 or delete address)[63].

In the edge case when VP is completely absent, so the VP model contains no addresses with none-zero VP values; DLT will stall and wont be able to progress, i.e. confirm new blocks. So in the simplest default case VP is distributed equally between addresses attached to each node of the DLT network [63].

In this example each node has VP value of 100 and votes for blocks using this VP. A more advanced case:

In here three nodes still have same 100 VP, while one other node has no VP at all. This node cannot vote on the blocks going into the blockchain but has full visibility of the blockchain contents and can confirm its validity[63].

Partitioning: Forking is not possible in Credits Core, but the Credits network can go into the partitioned state. Partitioning is a situation where the quorum cannot be reached

in a part of the network because either the network connectivity is impaired and nodes cannot propagate the votes on new blocks or the nodes cannot agree on the rules of the network and do not cast votes on blocks that they assume invalid [63].

In both of these scenarios the Voting Power required to choose and commit to new block becomes unavailable to part or the whole network, and the affected part of the network stalls, i.e. cannot continue to grow the chain. Since not enough VP is available to progress the chain and vote on blocks â no minority chain will form, the forking or chain reorganization will not happen at any circumstance and any data that was voted and committed to the chain before the partitioning will be not affected.In this case, if only a minority of the networkâs VP is affected and the majority is still both in agreement and has enough VP available to form a quorum â the majority of the network will continue to operate normally. The partitioning situation will likely to require manual intervention to identify and address the root of the problem, whether it is a connectivity issue, consensus disagreement or anything else. (Credits)

Use case: The Credits Blockchain is a disruptive technology platform that uses strong cryptography and a distributed messaging protocol to create a shared trusted ledger between trading counter-parties.

Design: Credits was designed initially for 'Know Your Customer' (KYC) applications, Credits developed, pragmatically, into a cloud platform that took the donkey work out of hosting specific applications using blockchains. Itâs a model that makes Credits an enabler that can work across and between applications, including those from large enterprises and smaller firms alike.

2.1.9 CredyCo

Introduction: CredyCo is document verification 'software as a service' (SaaS) founded by Venny Lingham in 2014. It is located in Canada. The company describes the service as using "a smart contracts and identity technology built on top of the blockchain to ensure the credibility and irrefutability of all statements". For example, firms will be able to record their financial and growth metrics securely, allowing investors to more efficiently assess companies credibility and thereby potentially shortening the closure time and increasing the number of successful deals[64].

At the core of companys proprietary technology stack lie Trustatom ID, a mobile privacy-respecting identity and credentials application. Seamlessly integrated with other APIs Trustatom provides, Trustatom ID helps businesses reliably identify and verify their customers, as well as improve the security of their customers by using cryptographic signatures for authorizations [65].

Built on Trustatom's technology, CredyCo significantly reduces the complexity of the manual due diligence process through the use of timestamped and mathematically irrefutable, signed statements on KPIs (Key Performance Indicators), reports, milestones and other information[66].

Trustatom ID is the heart of the company's proprietary technology. The company describes it as a âmobile privacy-respecting identity and credentials applicationâ, helping businesses automate 'know your customer' practices and allowing their customers to authorize transactions with cryptographic signatures [64].

In short, CredyCo claims to facilitate the authenticity of the user in smart contracts using blockchain technology. The problem with centralized identities is that it is so easy to create Pseudo Twitter accounts, fake Facebook profiles and anonymous chat room IDs when it comes to assuming the personalities of others.

Advantages: Here is the advantage of CredyCo 1. Credyco uses Trustatom ID which helps businesses to reliably identify and verify their customers, as well as improve the security of their customers by using cryptographic signatures for authorizations.

Use Cases: CredyCo can be used in industrial use cases such as establishing and transferring property rights.

2.1.10 Cryptid

Introduction: Masley and partner Dakota Baber created Cryptid to be used as both a demonstrative web application as well as a stand-alone windows program, making the source code available at Github. A smartphone application already exists to verify other peoplesâ IDs from Cryptid.xyz. All of the software for this is finished now and ready for businesses to start using[68].

Cryptid is a new open source identity system. Itâs a low-cost, extremely flexible ID-issuing and verifying program that can be useful for organizations of all sizes. It is using Factom [It stores the world's data on a decentralized system. Using blockchain technology for smart contracts, digital assets and database integrity] to place encrypted identity data on a blockchain, this lightweight program allows for a variety in the types of ID card or token used[68].

Cryptid is the next generation of identification. Current identification methods such as state issued driver's licenses are insecure and easily tampered. Cryptid eliminates the possibility of counterfeit identification by adding factors of identification and encryption that is backed by a distributed, global network[69].

There are many dozens of access control and ID card-issuing programs for sale to businesses today, and far more proprietary programs that governments and the largest corporations use. No matter if they allow control over devices like door locks and badge scanners, all of them have a central database that holds personal data, and many of them issues ID cards of some kind. The larger and more secure these databases grow, the more expensive they become. The largest require their own co-located datacenters, complete with armed guards and their own access control systems. This centralized paradigm is

forever subject to hacking, downtime, software licensing fees and upgrades, huge energy costs, hardware limitations, networking restrictions, technical support, IT training, and more. Todayâs systems, it seems, are far from perfect[68].

Because the identity records, including a small photo and fingerprint file, are no larger than a few hundred kilobytes, Cryptidâs team was able to use Factom to store entire records onto a blockchain, which is timestamped on the bitcoin blockchain too. There is neither local nor administrator server that needs to be run for others to access; all data is decentralized and accessible anywhere on the planet[68].

By utilizing the power of the blockchain, no one authority holds access to your identity. Instead the data is distributed across many computers, which prevents corruption and makes it nearly impossible for your identity data to be tampered. Conventional identification methods rely on a central authority such as a state government in order to assure your identity, making them vulnerable to hacking and corruption[69].

Cryptid uses three factor authentication to assure you who you are. Traditional identification methods only require one factor of authentication which is the card that you have. Cryptid gives you the ability to use all three. The unique identifier is something you have, the password is something you know and your fingerprint is something you are[69].

Since Cryptid doesn't require a physical identification card to prove your identity, Cryptid allow you to cut costs by allowing your identification media to be almost anything from a smart phone to a generic piece of paper – anything that can store a QR code[69].

How it operates: Here are the operations of the Cryptid [69]

1. Fill out the form: To begin with, Cryptid takes the data provided in the form and package it into a compact format readable by system and generate Cryptid identification data.

2. Encrypted and Signed: All of data is encrypted with the provided password. It is important that you do not forget this password as there is no way to recover it. We also have a password of our own (a private key) that is used to sign the data to prevent any counterfeit identification data.

3. Uploaded to the Blockchain: This is the last step in which your data will be on Cryptid. It will now be permanently transferred to the blockchain. This means your data cannot be manipulated by any authority or person, not even the Cryptid Company.

4. Get your ID location: You are then given a unique identification number that points to your information on the block chain and can be stored on almost anything from magnetic stripes to QR codes. We currently use QR codes to store this on our standard issue identification cards.

Utilizing existing standards, such as ISO 19794-2 for our fingerprint templates and AAMVA (American Association of Motor Vehicle Administrators) and ANSI personal information

format standards, Cryptid system can be integrated with existing software and hardware (fingerprint scanners). Current version of Cryptid uses Factom as its blockchain backend. For encryption, Cryptid use AES-512-CBC for data encryption and RSA-4096 for signing and verification[70].

By using private keys and a 3 factor authentication system, Cryptid can prevent any possibility of counterfeits or fake IDs. Instead of renting large, dedicated servers and hiring security personnel to protect databases, Cryptid can place any member registry on the blockchain, creating an unhackable system with 100

Advantages: The advantages of Cryptid are as follows

1. From a security standpoint, there are many benefits to be gained from using this system over legacy solutions. Chief among these would be the cost savings from decentralization, so there would be no need for a datacenter or even a dedicated server at all, with the blockchain holding all of that information. Identification can be verified anywhere the internet is, no matter the state of the administratorâs server[68].

2. Blockchain systems can take advantage of multi-signature bitcoin addresses, so no single authority will hold the access to anyone's identity. Being open source means that no one can put a backdoor hack into it. Passwords can be tied to cards too, on top of typical factors like photos and fingerprints, offering an impressive additional layer of protection for users[68].

3. Flexibility is also a major plus point, because the user-side data does not necessarily have to be saved to a photo ID card. This info can be stored on anything that can keep a few kilobytes of information, anything that can store a QR code, representing just private key and a password. Even hidden tokens inside jewelry or an app on smartphone could hold ID card in this way[68].

4. The biggest advantage of Cryptid is its complete identity security. With Cryptid, identity theft is a thing of the past. A thief no longer needs only to steal your wallet to masquerade as their victim's identity. [70]

5. The open nature of Cryptid allows it to be more widely adopted, adapted for security and integrated into unique systems.

6. The use of the blockchain for immutable, effectively unhackable, identity storage is extremely novel[70].

Use Cases: It benefits a group or organization of any scale by allowing them implement a secure method of managing the verification of official members. Furthermore, in following areas Cryptid plays a vital role. The description is given below [70].

1. Rochester Institute of Technology Student Identification Cards RIT, like almost every other university uses a unique number stored on the magnetic stripe for authentication. RIT in particular uses ID cards for building access, dorm access and

billing. This is considered one factor of authentication and is easily susceptible to replay attack. All you need is a magnetic stripe encoder and a picture of their identification card and you have the same access as the card holder. The advantage of Cryptid in this scenario is invulnerability to replay attacks as well as additional factors of authentication.

2. United States Department of Defense Common Access Card The DOD CAC uses all three factors of authentication, however the issuance of the card is limited to only DOD employees and contractors. The DOD CAC also calls back to one central database (RAPIDS – which is vulnerable to potential data breach). The advantage of Cryptid in this scenario is the distributed nature of the block chain, further securing the data.

3. ICAO Machine Readable Travel Documents (Passports) Passports use two factors of authentication (something you have – the passport – and something you are – the fingerprint). However, like DOD CAC they also call back to a central database. They are also far more expensive to make as they require expensive EEPROM contactless chips to store and transmit data. The advantages of Cryptid here are low cost and again the distributed nature of the block chain.

Design: The front of a Cryptid card issued on Cryptid.xyz. The backside would have a fingerprint and a QR code displayed. If you want to edit anything on your card it would require making a new one, so disposing of old cards properly is important[68].

CryptIDs can be verified on our website(www.cryptid.xyz) simply scan an ID on your phone and enter your password. While Cryptid are not currently registering IDs directly through website, Cryptid can implement that for any client or organization who wishes to register their members. schools, businesses, or governments could use CryptID, using it to secure student IDs, standardized test scores, employee IDs, driver's licenses, or even social security numbers[71].

2.1.11 Evernym

Introduction: It was founded in 2013 by CEO, Timothy Ruff[72]. Evernym builds and operates Sovrin, an attribute-based open source global identity network for self-sovereign identity. It provides software, websites, blockchains, and distributed ledgers with a self-sovereign identity ledger that supports the continuum of the identity graph from anonymity to pseudonymity to proven legal identity[73].

We have too many usernames and passwords, too much ID theft and fraud, too many data breaches, too little control, too little privacy, and an unacceptable 3 billion people unbanked. But now there's an elegant solution, a way to take control. Evernym is building an attribute-based sovereign identity platform on a permissioned distributed ledger, a solution to the global identity problem that restores privacy and control where it belongs: you[74]. It provides following services to its users [75]

- Instantly and accurately verify the authenticity of claims made by any person, organization, or thing, without centralized databases.
- It is simply the most powerful, privacy-preserving technology in existence. It's time privacy made a comeback.
- Evernym is engineered for universal compatibility with both legacy and ledger-based identity protocols.

If anyone other than you can pull the plug or change the rules for your identity, it is not self-sovereign, it is siloed â even if it uses blockchain technology. Globally scalable self-sovereign identity requires an open source, decentralized network which no single entity owns or controls. Until the advent of distributed ledger technology (DLT) this was impossible.

Implemented properly, distributed ledger technology (DLT, referred to as blockchain) can remove reliance on centralized silos, enabling the revolutionary power of self-sovereignty. Moreover, DLT behaves similar to a traditional database where one entity retains pull the plug and change-the-rules authority. This model still has the fundamental problems of siloed identity, which created the identity mess in the first place.

How it operates: Sovrin is the worlds global public utility for trusted, self-sovereign identity. Like the Internet, it is not owned by anyone: everyone can use it and anyone can improve it.

1. Any person, organization, or thing can actually own their digital identity not just control it independent from any silo.
2. Any person, organization, or thing can instantly verify the authenticity of claims, including who (or what) something claims to be.
3. Complete control of how, what and when information is shared, without added risk of correlation and without creating troves of breachable data.

Sovrin utilizes Hyperledger Indy, an open source blockchain framework and one of the Hyperledger projects hosted by The Linux Foundation. Hyperledger Indys source code was originally developed and contributed by Evernym. Sovrin represents the leading edge of distributed ledger technology, with unique privacy, performance and security characteristics ideal for identity and not found in any other ledger.With Sovrin, trust is established using verifiable claims. A verifiable claim is exactly what it sounds like: a claim shared by any person, organization, or thing that can be instantly verified by the receiving party. **For Example**: The post office issues a verifiable claim to Alice attesting that her street

address is 123 Main Street.

Alice shares this claim with her credit union as part of opening a new account.

Figure 2.12: Step one

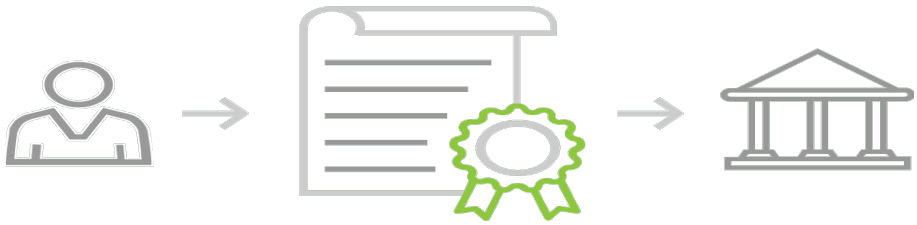

Figure 2.13: Step two

Without having any connection to or interaction with the post office, the credit union instantly and cryptographically verifies that Alice claim is signed by the post office and has not been revoked.

Alice now owns this proof-of-address claim and can use it anywhere she wants, as much as she wants, and now the credit union can trust that Alice address is 123 Main Street.

Leveraging the advanced capabilities of Sovrin, Evernyms platform offers developers, solutions providers and systems integrators the tools they need to break down data silos, onboard users more seamlessly, and make trust a key value proposition. Deployed standalone or tightly integrated into an existing offering, hosted on premise or on our secure cloud infrastructure, Evernyms smart agent software is the enterprise bridge to trusted peer interactions shown in the Figure 2.15 below.

Advantages: Here are the advantages of the Evernym [75]

1. Not restricted to specific data types, mechanisms, or contracts imposed by a central hub, anyone can present identity information of any type to anyone else in the world, and the recipient can unpack and verify it instantly, with no need for hundreds of complex APIs and commercial contracts.

2. Verifiable claims, along with all private data, are stored off-ledger by each self-sovereign identity owner, wherever the owner decides. No private information is ever stored on the ledger, in any form.

Figure 2.14: Step three

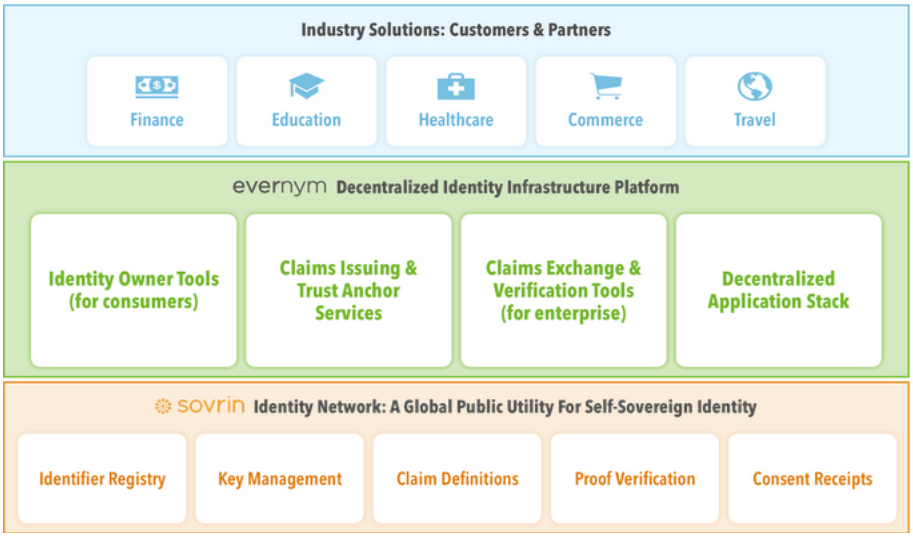

Figure 2.15: Architecture of Evernym

3. The combination of self-sovereign identity and verifiable claims enables highly advanced privacy-enhancing techniques, such as zero-knowledge proofs (for selective disclosure) and anonymous revocation, to be made available to the world.

4. It supports password less login and multifactor authentication with the cryptographic confidence of a user's Sovrin identity.

5. Dispense with burdensome online forms and lengthy manual reviews: let users provide instantly verified data about themselves on the web, on mobile and in person.

6. No more printing paper certificates and maintaining ancient files: issue digitally signed, cryptographically auditable academic and professional credentials which can be accepted anywhere.

7. Auditable consent records, selective disclosure. non-correlation. User control. Requirements in GDPR and PSD2, and key components of self-sovereign identity.

8. This multi-national leader in the financial services industry with 40 million customers tapped Evernym to simplify compliance while improving customer experience.

Use Cases: Use cases of Evernym are as follows[75]

1. Homeland Security: Evernym is currently researching, designing and building a Decentralized Key Management System (DKMS) under an SBIR research grant from the U.S. Department of Homeland Security Science Technology Directorate.
2. CU Ledger: For CU Ledger a national consortium representing the U.S. Credit Union industry Evernym will dramatically reduce fraud, increase security, and simplify compliance, all while improving the member experience.
3. iRespond: Global nonprofit iRespond is partnering with Evernym for privacy-respecting biometric identification for at-risk populations across the globe.
4. Financial Services Leader: This Fortune 500 financial services company believes their 10 million customers should own their own identity, and is working with us to accomplish exactly that.
5. Healthcare Initiative: Evernym is partnering on a nationwide initiative to provide all UK doctors with a digital passport and reputation system.

Design: Evernym is developing a sophisticated identity platform built on Sovrin. These tools and products are designed by the same team that created Sovrin to significantly ease the deployment and integration of self-sovereign identity infrastructure in many different industries.

Evernyms consumer app puts the individual at the center of their interactions. Built for security and ease of use, connect.me provides a place where individuals can manage their connections, keys and verifiable claims, giving them true control over their digital identity for the first time.

2.1.12 ExistenceID

Introduction: ExistenceID, a secure global identity storage and onboarding platform utilizing distributed ledger technology. Launched in February 2016, the Hong Kong-based digital identity startup is led by CEO (Chief Executive Officer) and co-founder Katherine Noall [76].

Two main things were happening before ExistenceID, people werent being given a safe place to hold identities that were being issued, and the data liability being placed on businesses was really heavy, said Noall, in an interview with One World Identity. ExistenceID is trying to solve both those problems.ExistenceID allows users to create a digital identity capsule âa bit like Dropbox, that enables people to store their documents, but has a much higher level of security said Noall. Each user account is completely self-authenticated for which ExistenceID doesnât hold login details and any of the data, it has zero knowledge. [76]

How it operates: Following steps are carried out to use ExistenceID [77]

1. Simply register an account (self-authenticated)
2. Save your identity documents to your account
3. Choose who and when to share your identity documents with
4. Add new documents to keep your identity alive ExistenceID believes in access, freedom and privacy. For this purpose, identity capsule is used. Identity capsule has following features [78]

- It is used for super safe keeping and sharing of valuable identity documents.
- A secure and private identity capsule for all of userâs identity documents, even the old ones.
- The capsule rates the total identity so user can prove that he/she is real. Only user can choose to whom and when share different parts of identity with.
- It is so private that ExistenceID has zero knowledge of users account.

The mechanism for reporting identity data stored inside a digital identity capsule operates independently, using the Bitcoin blockchain[76].

For example, in order to complete an online purchase, an ExistenceID user might receive a request from a retailer to verify their address. The user can then select the requested piece of identity data, in this case, address, and have it encrypted and encoded on the Bitcoin blockchain. The retailer would be granted access only to the data chosen for disclosure by the user, and nothing more [76]. Report the bit that individuals have agreed to report to the blockchain, and hash that in a way that itâs unidentifiable, and then use that for reporting, said Noall. Thats good because it canât be tampered[76].

Identity documents saved to a digital identity capsule are encrypted and uploaded to the SAFE Network, a secure decentralized data management service. According to Noall, ExistenceID chose the SAFE (Secure Access For Everyone) Network for identity document storage because thats what ExistenceID view as the safest data storage in the world at the moment.

The SAFE Network uses advanced peer-to-peer technology that joins together the spare computing capacity of all SAFE users, creating a global network. It provides decentralized and encrypted data to ensure that only user can access the data. It is completely distributed. There is no central point of control.Before user uploads a file, it is encrypted using Bitcoin blockchain. After encryption, the file is defragmented and spread to the distributed network (multiple computers) where data is stored with redundancy in SAFE network. Files are autonomously moved by the network as connected computers are turned on and off. Only user can have the credentials to make it available again[79].

Advantages: Below are the advantages of the ExistenceID [77]

1. It is saving time to find identity documents - always know where your documents are and know they are safe.

2. It is used to keep important documents safe when moving jobs, home or country, whether by choice or necessity (war or natural disaster).

3. To prove that user is the real person, if someone else is trying to steals the identity. advantage of ExistenceID is to prevent the lost documents.

Use case: This amazingly secure storage can be applied to medical records, so that anyone can share them with medical team. Also, it is applicable to the secure land transactions. Future work: ExistenceID plans to begin work with corporate beta customers in October 2017. Beta identity capsule accounts will be made available to consumers in November[76].

2.1.13 Guardtimeâs BLT

Introduction: Guardtime is the first and only platform for ensuring the integrity of data and systems at industrial scale, announced BLT (named on the initials of last name of its founders; Ahto Buldas, Risto Laanoja and Ahto Truu) in 2014 for the authentication and signature protocol meant to replace RSA (An algorithm for public-key cryptography, it is named on its founders; Ron Rivest, Adi Shamir and Leonard Adleman) as the standard for digital signatures since 1971. BLT is a new cryptographic algorithm invented by Guardtime cryptographers. In contrast to RSAâs reliance on quantum-vulnerable asymmetric key cryptography, BLT is based on Guardtimeâs quantum-secure Keyless Signature Infrastructure (KSI) technology, which uses only hash function cryptography[80].

RSA has been the dominant digital signature scheme since the 1970s, but its outdated and cannot scale for the explosion of data or devices, it is not compatible with IoT (Internet of Things), mobile and machine-to-machine technologies.Most importantly, on the advent of quantum computers, RSA could be rendered completely useless. No practical and scalable alternative for the market exists, until now, said Mike Gault, CEO of Guardtime. âOur scientists invented BLT in recognition of the urgency to find a scalable alternative to RSA in a world of continuously connected machines[80].

KSI blockchain technology employs one-way hash functions to generate digital signatures that can prove the time, integrity and attribution of origin for electronic data. BLT extends this approach to provide human and machine identity management, with a level of non-repudiation consistent with existing digital signature schemes[80].

As the sophistication of nation-state cyber-attacks continues to increase on a daily basis, there was an urgent need to find alternatives to RSA to protect strategic national assets and critical infrastructure. BLT represents game-changing innovation for cyber-security and ensures that critical infrastructure can remain protected even in an age of quantum computers[80].

How it operates: BLT works on the following principles [80]

1. Baseline: The Platform records the state of all KSI-instrumented digital assets by registering them in a global KSI Blockchain, generating a mathematically verifiable baseline image of the network - a Clean State Proof. Once this state has been achieved, it becomes possible to continuously verify that the network remains in a clean state and act when a compromise is detected.

2. Verify: The Platform enables continuous verification of whether your network is still free of compromise and Clean State Proof still valid. This concept is called Active Integrity and it provides you with a real-time situational awareness of digital assets like firmware, operating systems, network routing tables, switch and router configuration parameters, event logs, data stores or computer memory.

3. Remedy: The changed integrity state provides a real-time alert, enabling you to make immediate decisions in the event that the network and/or asset is compromised and rapidly identify the cause and specific components responsible i.e. if an asset is affected by malware, the asset can be âsandboxedâ or fire-walled before further propagation. The infrastructure of KSI is given in Figure 13 below (Keyless Signature Infrastructure) KSI Service Infrastructure Core Cluster: It is a component responsible for managing the KSI blockchain.

Aggregation Network: a component providing scale, redundancy and global reach for the KSI service delivery network. **Gateway Server**: A hardware or software component at the customer premises providing access to the KSI service. Application Integration: Guardtime provides fully featured SDK-s for C, Java and .NET to facilitate KSI service integration to customer applications.

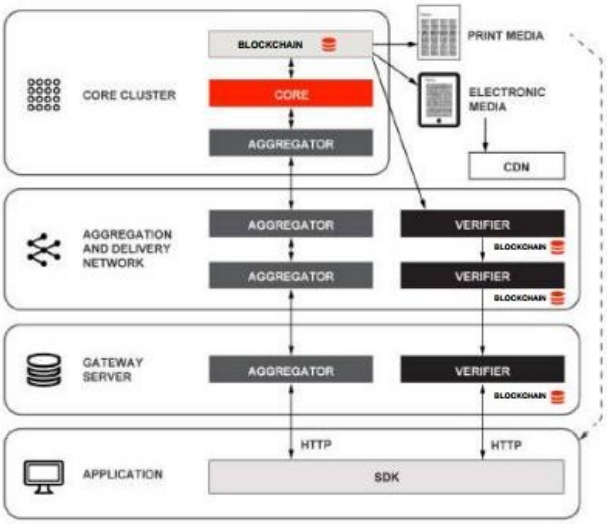

Figure 2.16: Architecture of KSI

Advantages: Here are the advantages of Guardtime BLT [80]

1. Simplified revocation management: In BLT, signing key status is checked at the signature issuance, and then the signature is sealed using KSI. Thereâs no need to find and check a Certificate Revocation List (CRL) when verifying the signature in the future.

2. Long-term validity: There is no need for periodic re-timestamping of signatures due to expiring keys - time and integrity of the signature can be proven mathematically without reliance on security of keys or trusted parties.

3. Cryptographic non-repudiation: It is mathematically impossible for the CA(Computer Associate) to generate the signatures on behalf of the user.

4. Limited liability: In BLT the signatures are created with server assistance â they require the CA to assist in the process of generating a signature (at the same time without being trusted). This is valuable as the CA can monitor or limit the number of signatures issued by a user.

5. Quantum immunity: BLT uses only industry standard cryptographic hash-functions for signature generation and verification. Unlike asymmetric cryptography used in today's PKI solutions (i.e. RSA, elliptic curves,) hash-functions cannot be efficiently broken using quantum algorithms.

6. Scale and efficiency: BLT easily scales for next-generation IoT applications assuming billions of online devices needing to be validated, and is more efficient to calculate and store than RSA. (guardtime)

7. BLT collapses security issues and removes traditional trust anchors with this new signature scheme. Itâs clean, efficient and beautifully simple, demonstrating the power of KSI to transform the worldâs security landscape

8. The KSI blockchain platform enables real-time cybersecurity and data-centric asset protection, directly supporting enhanced continuity of operations, data loss prevention, and is a new form of real-time Advanced Persistent Threat (APT) detection.

9. Guardtime's KSI blockchain enables organizations to ensure the integrity of their networks, prevent loss of critical digital assets and track data securely throughout its supply chain.

10. If an intruder were to get access to a data store and even so much as touch any file therein, an administrator is notified immediately. The automation of the BLT software immediately re-secures the store and traps the intruder so that no more files can be compromised[81]. endenumearte

Use case: Apart from robust security, e-commerce and/or device registration applications, BLT greatly improves the strength of any signing and authentication process, says Matt Johnson, CTO (Chief Technology Officer) of Guardtime[80].

Guardtime announces BLT after more than seven years in development, which is already being utilized in government, enterprise and private applications. The country of Estonia ensures the integrity of the worlds most advanced digital society with Guardtime. Ericsson, a world leader in communications technology and services, recently announced a data-centric security offering based on Guardtimeâs technology that will enhance trust, transparency and accountability for IoT and for machine-to-machine applications[80].

Guardtime BLT underpins an entire government and our customers including the largest global defense and telecom vendors.

BLTâs key insight is that the most valuable application of blockchain is for supply chains - software, physical and information supply chains that are within and across organizations. It works with clients to understand those supply chains and build solutions to harden them, eliminating inefficiencies and providing mathematical certainty for their integrity - track and trace at the digital and physical item level[80].

Design: The KSI blockchain technology stack consists of a specialized Black Lantern security appliance hardware with advanced anti-tamper functionality, software suite for real-time monitoring of the integrity state of your network and a service that provides KSI blockchain based signatures needed for network instrumentation[80].

Black Lantern software is digitally signed and encrypted at rest with KSI and NIST (National Institute of Standards and Technology) / ETSI (European Telecommunications Standard Institutes) approved encryption algorithms. The hardware is incapable of executing unsigned code - it will not boot if the software and hardware runtime environment is not authentic.

Black Lantern Security Appliance is self-protecting. Tamper events are immediately evident and the device engages protection mechanisms to wipe keys and software, rendering the system inoperable, or into various maintenance modes. It is not possible to use Black Lantern to stage an attack, either against the device itself, or against other assets in your network[80].

Black Lantern Appliance uses advanced ASICs (Application-Specific Integrated Circuits) with customized tamper protection features and escalation reaction monitors for added security given a variety of physical attack vectors so that it is capable of defending itself against remote attack and physical attacks. The Guardtime stack is the Unix philosophy applied to blockchain-abstraction and encapsulation into layers, each of which does one function well. This approach provides scalability, interoperability, reliability and works with legacy systems. Crypto-currency protocols are great for what they were designed for - not for large scale enterprise data supply chains[80].

Rather than relying on public and private keys (PKI) as RSA does, BLT is based on hash-function cryptography, which requires no keys and so requires no issuing, updating or revoking of keys. As a result, it can scale to cover exabytes (1018 bytes) with little overhead, says the company's CEO Mike Gault. And there are no cryptographic secrets to be compromised. [82] **Challenges**: The following challenges

are faced by KSI technology (Keyless Signature Infrastructure)

Scalability: One of the most significant challenges with traditional blockchain approaches is scalability, they scale at O(n) complexity i.e. they grow linearly with the number of transactions. In contrast the KSI blockchain scales at O(t) complexity it grows linearly with time and independently from the number of transactions. Settlement time: In contrast to the widely distributed crypto-currency approach, the number of participants in KSI blockchain distributed consensus protocol is limited. By limiting the number of participants it becomes possible to achieve consensus synchronously, eliminating the need for Proof of Work and ensuring settlement can occur within one second.

2.1.14 HYPR

Introduction: HYPR is biometric security suite provides enterprises a fully interoperable solution to secure users across mobile, desktop and IoT systems. It was founded by CEO George and CTO Bojan in 2014. HYPR enhances the user experience by allowing user to choose from voice, face, touch and eye recognition. This decentralized authentication platform allows enterprises to leverage biometrics without worrying about hackers attacking a biometric server or centralized password database[8].

We are living in an age of cyber-attacks. From government secrets and individual identities to credit cards and connected carsâhackers have proven that everyone and everything is vulnerable. The hackers are winning and no amount of complex passwords or firewalls can stop them. Now more than ever before-users expect the best usability, security, and privacy. HYPR is the first authentication solution to unite frictionless digital experiences with best-in-class security and privacy protection[83.. By leveraging billions of biometric sensors across our fully interoperable architecture, HYPR takes the password out of the equation and ensures your user data is kept private [83].

How it operates: HYPR biometric encryption ensures user credentials are decentralized and stored offline. A cryptographic digital key is generated from a biometric such as a fingerprint or voice and is used to sign transactions initiated by a relying party. Raw biometric data is never sent through the network or stored in a central database. The FIDO (Fast Identity Online) alliance has established, Fast Identity Online Authentication. This authentication standard procedure provides security standards and methods that go beyond passwords in creating secure identity management. The two major technical specifications under FIDO Authentication are U2F (Universal 2nd Factor) where a token is used alongside a password; and UAF (Universal Authentication Factor) where local biometric authentication creates a password-less experience. The steps of HYPR secure biometric FIDO authentication are shown in Figure 2.17. [83]

Moreover, the architecture of FIDO U2F is illustrated in Figure 2.18. [83]

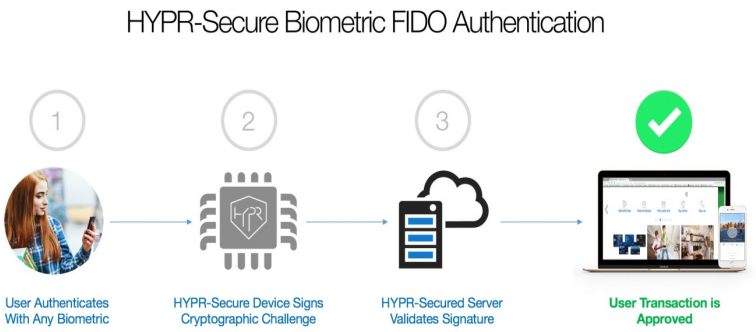

Figure 2.17: HYPR secure biometric FIDO authentication

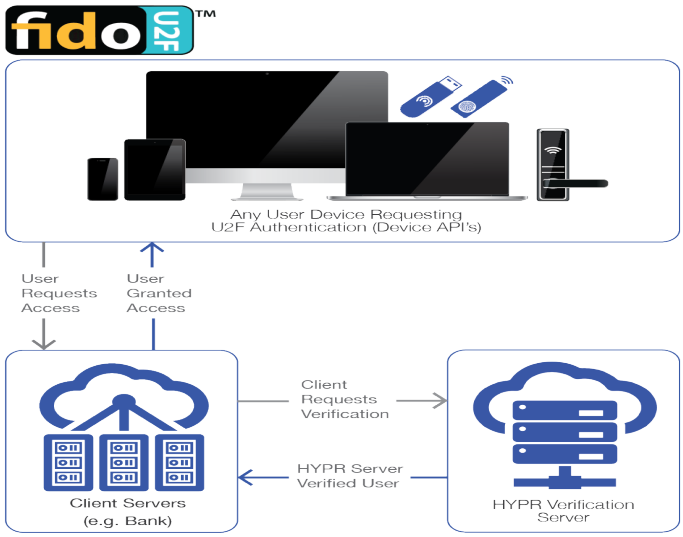

Figure 2.18: Architecture of FIDO

The HYPR-Secure biometric server ensures that biometric templates and credentials never leave users devices. Tokens and cryptographic signatures are validated on the server-side through FIDO authentication server. (HYPR)

HYPR offers following operation/ functionalities to its users [83];

Fingerprint Authentication: HYPR learned from the 2015 OPM breach, fingerprint sensors are not secure without a properly implemented public key infrastructure. HYPR biometric tokenization ensures usersâ fingerprints securely decentralized and safe from hackers

Voice authentication: HYPR provides best-in-class voice recognition as part of its end-to-end biometric security suite. Voice authentication matches a previously recorded voice model template to the vocal behavior and quality of the person seeking access. All voices are unique, and consumers are increasingly comfortable with the voice-first access offered by things like smartphones and home entertainment systems.

Face Authentication: The âmapâ of a personâs face is used as the mode of identification. It can be done live or from a digital image. The map is stored as

a template for identification and authentication matching in the future. HYPR technology dramatically reduces the number of false positives that often happen with other solutions.

Selfie Authentication: When using selfie authentication, the person seeking authorization takes a selfie so that their identity can be authenticated through facial data points. These data points are matched against a reference selfie kept on file by the authorizer. HYPR's solution protects against spoofing by using a passive non-challenge response such as a blink from the user and a series of facial recognition biometrics that ensure liveness and true identity. HYPR is fully interoperable and empowers enterprises to leverage any front-facing camera with support for over 1 billion mobile and desktop devices. It also provides facility to integrate face authentication into any application today for a secure password-less authentication experience.

Eye Authentication: HYPR provides enterprises secure FIDO-Certified eye authentication solutions for employee and customer-facing applications. Each day millions of eye recognition templates are authenticated and secured with HYPRs end-to-end biometric tokenization.

Palm Authentication: Adoption of palm recognition has often been hindered by expensive and bulky hardware sensors. By leveraging device cameras, our biometrics platform empowers enterprise deployment of secure palm recognition across millions of compatible phones, tablets, and laptops. The HYPR suite is engineered to be fully interoperable with any front-facing camera â enabling users to authenticate anything with a palm scan â without having to purchase additional hardware.

At the time of registration, the validation server and a trusted deviceâs embedded biometric sensor jointly establish a secure communication channel to verify that they are corresponding only with one another and not to a remote malicious party. The authenticator, e.g. a fingerprint reader, then assures that a userâs initial registration request has arrived from FIDO (Fast ID Online) Certified validation server. The outcome of the registration process is the formation of a symmetric token seed. This seed token validates a specific accountâs authentication requests. At inception, following creation of a seed token, future validation requests will occur seamlessly without the need for user verification to happen as a consequence of a return-trip mechanism[83].

Platform/ Technology used: The details of platforms and technologies used by HYPR are given below [83]

1. FIDO certified implementation is fully interoperable across these operating systems

- OSX
- Windows 7,Windows 8 and 8,1, Windows 10,
- iOS
- Android

2. The HYPR biometric architecture is engineered from the ground up to be fully interoperable with OAUTH, SAML, Active Directory, Kerberos, and most major

IDP (Integrated Data Processing) solutions.

3. HYPR supports these cloud services: Amazon Web Services, Azure, Google Cloud.

Advantages: Advantages of HYPR are listed below [83]

(a) HYPR provides enterprises an end-to-end solution for deploying decentralized biometric authentication securely across millions of users. This software is integrated into employee and customer-facing applications to eliminate fraud, enhance user experience, and increase revenue.

(b) People are forgetting MFA (Multi Factor Authentication). Industry leaders trust HYPR decentralized authentication to secure Touch ID, Windows Hello, Android M, and all other biometric user experiences across all platforms.

(c) Enterprises leverage HYPR omni-channel authentication to deploy and manage millions of biometric identities. From mobile to web portals, call centers to help desks, branches and ATMs (Automated Teller Machines)âHYPR empowers a secure digital experience across all channels.

(d) From biometric banking to employee access, HYPR enables faster transaction speeds and frictionless experiences across mobile, web and IoT systems.

(e) HYPR generates millions in new streams of revenue by delivering best-in-class user experiences to your customers, employees, and partners.

(f) HYPR joins the hundreds of enterprises transitioning to password-less authentication and never worry about a data breach again.

(g) With HYPR's Biometrics as a Service, companies no longer have to install and run security applications on their own servers. This eliminates the expenses of hardware acquisition, software installation and maintenance, and support. The solutions are scalable and automatically updated based on the needs of the business.

(h) User's biometric data remains secure through HYPR decentralized biometric security. We also make sure that user can integrate HYPR suite of solutions with own software through APIs (Application Programming Interfaces).

(i) Step up authentication in HYPR is easily the killer application when it comes to multi-factor security. Two or more biometric factors can be combined to deploy the most appropriate level of security based on the user action and the desired level of access.

(j) HYPR enables secure biometric out-of-band authentication (OOBA) a process requiring approval from two different channels or networks. This ensures that a transaction cannot be completed without the user having access to both devices.

Design: It is designed in such a way that user can do following tasks [83]

- Select Any Biometrics: Instantly add voice, face, touch, eye, palm or any combination of authenticators for a secure digital experience.
- Secure Applications: Unlock the power of HYPR next generation biometric multi-factor authentication in any application, on any device.

- Deploy to Millions of Users: With the push of a button, deploy HYPRâs omnichannel authentication to all of your customers, employees, and partners.

FIDO is offering following functionalities [83];

FIDO Server Architecture: Easily deploy HYPR-Secure FIDO server and empower users with a fully biometric user experience. Also, the FIDO UAF Server provides the server side of Universal Authentication Framework protocols. HYPR made it easy to deploy on-premises or as a cloud solution.

FIDO U2F Authentication: The FIDO U2F server enables the use of any additional hardware token authenticator as a Universal Second Factor.

FIDO SDK: Whether you build or buy, the FIDO SDK brings decentralized authentication to any application.

FIDO for IoT: Authenticate online or offline with FIDO IoT solutions powered by the HYPR biometric security platform.

Biometric U2F: The HYPR-3 biometric token is the worldâs first fully biometric FIDO U2F token where maximum levels of assurance are required.

FIDO Biometrics: Deploy a future-proof password-less user experience by integrating biometric FIDO UAF built-in support for fingerprint, voice, face, eye, and palm recognition.

FIDO Cloud: The HYPR FIDO cloud offering is available on-premise or on Amazon Web Services, Azure, and Google Cloud.

HYPR Biometrics Platform: Manage and deploy next generation security at scale with the HYPR biometrics platform.

Use case: From connected cars to smart homes, IoT authentication is changing how HYPR interact with the connected world. HYPR extends biometric tokenization to the firmware level to transform connected things into secure things. Large number of HYPR use cases are available which are as follows [83];

(a) Payments: Eliminate fraud, speed up transactions and generate more revenue with secure biometric payments powered by HYPR.

(b) Banking: HYPR is powering next generation experiences across mobile, web, and ATM experiences.

(c) Insurance: Insurance companies are focused on risk. HYPR mitigates risk. Itâs biometric insurance solution is eliminating identity fraud and service costs for some of the largest players in this space.

(d) Retail: From selfie payments to voice-activated purchases, HYPR can elevate retail brand experience to the next level.

(e) Customer Approval: HYPR stops spending millions of dollars on help desk requests and call centers. Biometric customer authentication presents additional layers of security while reducing costs and enhancing the end-user experience.

(f) Employee Access: Enterprises leverage HYPR mobile authentication platform to easily deploy biometric security across the global workforce. Employee Login Remote Access Virtual Desktop Infrastructure (VDI)

(g) Cars: HYPR's secure biometric car on the road is new feature. From in-vehicle payments to biometric ride-sharing, HYPR solution is redefining the connected car experience.

(h) Locks: When it comes to physical access, biometric authentication eliminates the two weakest links a physical key and lock cylinder. HYPR-Secure biometric locks are revolutionizing the lock industry and redefining the meaning of a digital key.

(i) Homes: When it comes to connected homes, HYPR protect that which matters most. This biometric connected home technology is adaptive, allowing your security to adjust as the home systems become more predictive and interoperable.

(j) Biometric Login: The login screen is everyone's least favorite part of an application. Not anymore. Empower your users with a fast and frictionless experience by deploying HYPR-Secure biometric login.

(k) Password-less Authentication: Passwords are no longer viable for businesses or consumers but theyâre not going to just disappear overnight. HYPR password-less authentication addresses both the UX (User Experience) and security challenges allowing you the enterprise to focus on generating revenue.

(l) Door locks, cars, connected homes, medical devices and critical infrastructure, all part of a growing world of connected devices. HYPR is the only decentralized IoT authentication solution designed for the biometric internet of things.

(m) HYPR not only allows for quicker and more accurate customer identification, it also enables a more personalized and engaged customer experience across all business units. Deploy HYPR omni-channel authentication to all customers, partners, and employee channels with the push of a button.

2.1.15 Identifi

Introduction: Identifi is an address book application that stores its data in a distributed fashion on the BitTorrent-like IPFS (Inter Planetary File System) network. (IPFS is a protocol designed to create a permanent and decentralized method of storing and sharing files). The stored information is not owned or centrally administered by anyone. In addition to keeping your contact details such as phone number or bitcoin address up-to-date, you can give other users trust ratings and feedback. You can filter all shown information by your web of trust, for example by displaying only the information stored by your friends and the people they trust[84].

Rating can be of three types: Positive, Neutral and Negative as shown in Figure 2.19.

Moreover, Identifi can filter all information by its author's position in your web of trust. For example, it only shows the content created by your friends and the people they trust. Identifi is decentralized where data is stored and indexed on the devices of its users (On IPFS), compares to a phone's address book or a local DNS (Domain Name Servers) cache. Identifi provides API (Application Programming Interface) for integration with various trust or identity dependent applications[85].

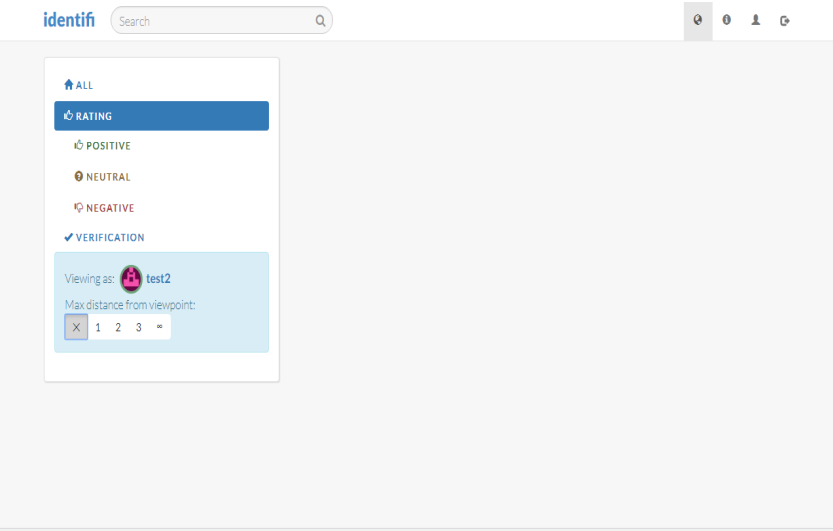

Figure 2.19: Ratings of Identifi

How it operates: The software (Identifi) itself is fork of bitcoin daemon, so it uses the same sort of networking mechanisms (the way you connect with other network peers or information is flooded to other peers), command line interface, JSON RPC API, public key cryptography. So, for the large part, it works same as the bitcoin network. It does not use mining, proof or work scheme, objective logic i.e. consensus. The major difference is, there is no blockchain technology. The following operations are present in the Identifi [85]

- Identifi messages [author identifiers, recipient identifiers, message, signatures] are Identified by content hash. These messages are signed by the entity which verified that the message originates from the named. author. Thus, all end users need not to have a crypto key of their own. Also, encoded and signed as JSON Web Tokens (JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties).
- Messages are stored and indexed locally in an SQL database where nodes maintain their own trust indexes which are updated as new messages arrive. Message storage priority is based on its author's and signer's position in the node's web of trust. Messages and indexes are also globally stored on IPFS. These can be used serverless mode and btree indexes (B-tree is a self-balancing tree data structure that keeps data sorted and allows searches, sequential access, insertions, and deletions in logarithmic time).
- It utilizes Crawl initial data (Crawling usually refers to dealing with large datasets where you develop your own crawlers (or bots) which crawl to the deepest of the web pages from existing social networks and review systems.

Advantages: Advantages of the Identifi are given below [85]

(a) Keep your contact details, payment addresses etc. up-to-date and verified by using Identifi.

(b) Identifi helps to trust people you have never met by utilizing your good reputation in various services and situations. Also, it reduces risk of trade or loan, thus reducing cost.

(c) Identifi prevent spam (by accepting messages only from trusted / socially connected senders).

(d) It prevents fake accounts used for commercial or propaganda purposes.

(e) Identify provide identity verifications to people who lack official ID.

(f) It also facilitates gift economy (It is a mode of exchange where valuables are not traded or sold, but rather given without an explicit agreement for immediate or future rewards) / time banking (With time banking, a person with one skill set can bank and trade hours of work for equal hours of work in another skill set instead of paying or being paid for services.).

(g) Distributed public messaging, with trust lists instead of centralized moderator power.

(h) It is censorship-resistance.

(i) It facilitates the no monopoly on credit ratings by giving insight to the open database, vs. proprietary information silos of reputation and online identity.

(j) It allows ubiquitous reputation as non-violent, cost-effective and decentralized justice so that everyone can choose whose judgment or review to trust. Another important thing to mention here is the focus on incentive against antisocial behavior. Incentive to restore trust by compensation and apology for misdeeds.

Use case: The use cases of the Identifi are as follows [85]

(a) Identifi can be applied to the facial recognition and identification with AR (Augmented Reality) glasses. For example, thumbs up to the friendly bus driver, policeman or the stranger who helped you.

(b) Mywot.com-style browser plug-in for website reviews.

(c) To generate trusted senders list from email history, Email plug-ins are developed. It requires new senders to be on identifi - send automatic response if not.

(d) It is used in decentralized marketplaces, P2P trade and finance. The reason to introduce Identifi is to check escrow or trader reputation in Airbnb, eBay, Uber, LocalBitcoins etc.

(e) Identifi is beneficial for uncensored and sockpuppet-resistant reviews and recommendations for products, restaurants etc.

(f) Another advantage is about public messaging which automatically show or hide authors.

(g) It gives a new direction to the users regarding social network based routing protocols.

Design: User can add entry from the main website . In order to create the entry, User needs to Login first. There are three kinds of Login options available as shown in the Figure 2.20.

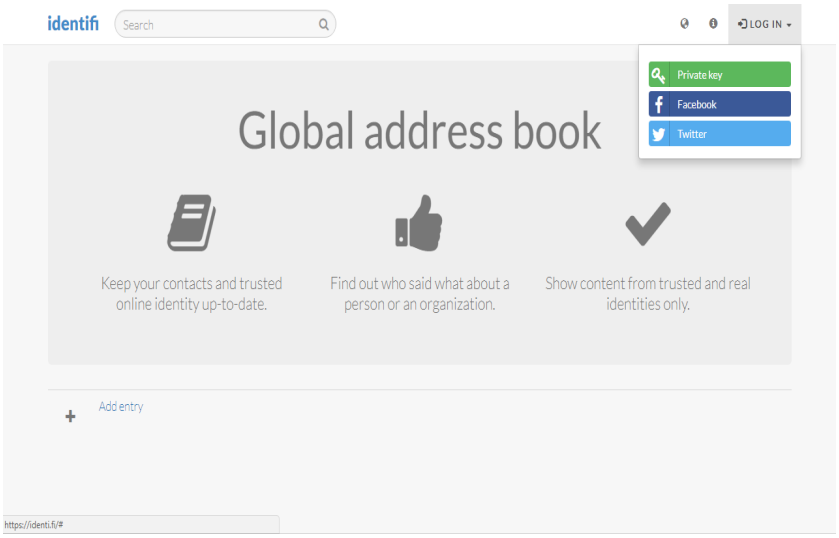

Figure 2.20: Login

(a) Private key: In order to login using private key, Firstly, user has to generate a new key using Generate new key button, as soon as key is generated user can Login as shown in the Figure 3. This private key obtained can also be downloaded by Download key.

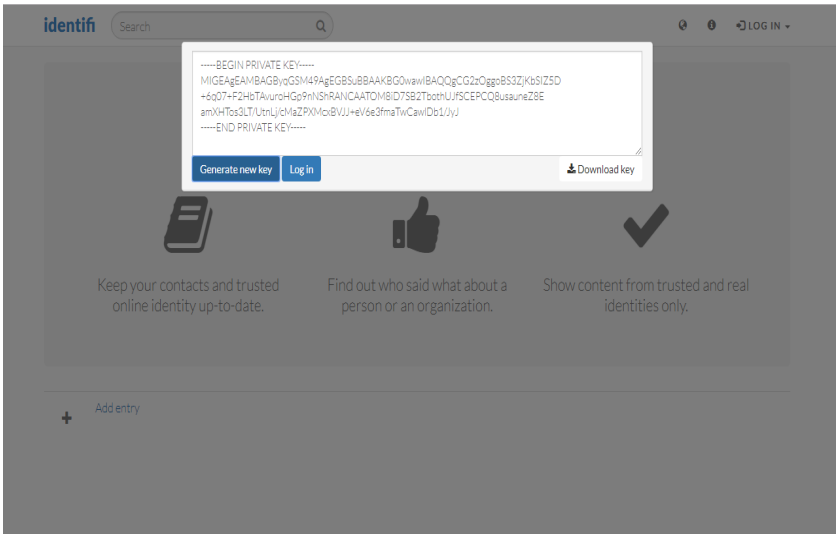

Figure 2.21: Login via private key

(b) Facebook

(c) Twitter

The desired information from Facebook or Twitter account is accessed and user can login. After Login, user can create a public entry by providing âName, email, phone number and URL (Uniform Resource Locator) of social media profile or any other profileâ illustrated in Figure 2.21. All stored information is made public and broadcast to the IPFS network. Identifi is released under the terms of the MIT (Massachusetts Institute of Technology) license.

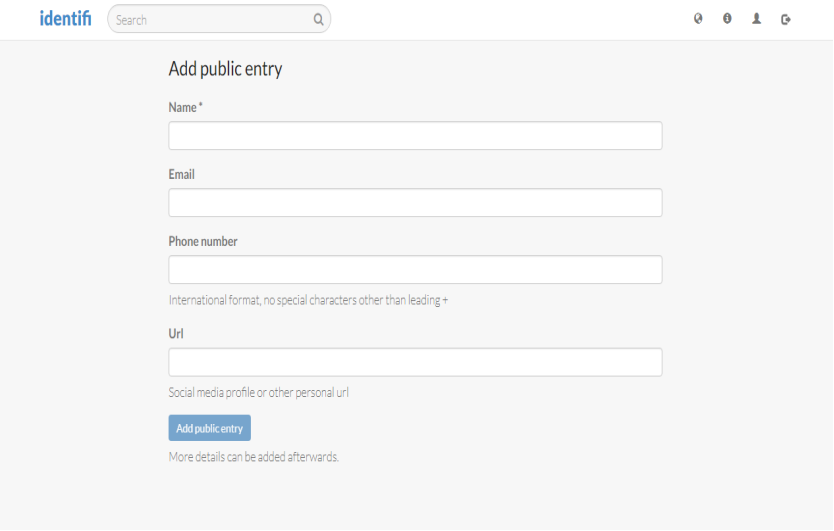

Figure 2.22: Public entry of Identifi

2.1.16 Open Identity Exchange

Introduction: Don is the Founder and Chairman of Open Identity Exchange (OIX). OIX is a non-profit, technology agnostic, collaborative cross-sector membership organization with the purpose of accelerating the adoption of digital identity services based on open standards[86]. Without clear agreements on the business, legal, and technical terms of a transaction, how can parties trust each other? OIX was formed to facilitate the development of the business and legal policies that match open identity technologies, thereby establishing trust among act actors trust that will enable deeper deployments of existing services and rapid deployments of new online products[86].

The Open Identity Exchange was publicly launched at RSA 2010. The open identity community, led by members of the OpenID Foundation and Information Card Foundation (ICF) and it addressed the building trust in online identity as outlined below:

- Relying parties must be able to trust that the Identity Provider is providing accurate data.
- Identity providers must be able to trust that the Relying Party is legitimate (i.e. not a hacker, phisher, etc.)
- Direct relying parties to identity provider trust agreements are a common solution, but are impossible to manage at Internet scale.

How it operates: OIX is developed by the Open Identity Trust Framework (OITF) model. This model breaks apart centralized control of certification into separate functions in order to create an open competitive market for each function.

Also, OIX members are collaborating to test identity verification and the elevation of authentication through the use of social media attributes in the Internet Life

Verification Alpha Project. Advantages: The top benefits exclusively available to OIX members are the ability to: [86]

(a) COLLABORATE with competitors, suppliers and partners to build pragmatic industry-wide solutions to common issues.

(b) REGISTER at OIXnet to discover, publish and validate your organizationsâ participation in global trust frameworks

(c) GAIN EARLY INSIGHT into dynamic market conditions to enhance existing services, explore adjacent markets and launch new products.

(d) DEVELOP BUSINESS AND BRAND by working with a worldwide network of market leaders, domain experts and innovative start-ups.

(e) SHARE COSTS in research and field tests of key business, legal, and technical issues in internet identity. All this is something one company can do, but when done on a collect basisâwith the most innovative names and brains in the industr. it is more cost effective, and hold and greater market impact.

(f) INFLUENCE the direction and requirements of public and private sector initiatives through an established, neutral, non-profit, global

(g) industry association.

Use case: The OIX Board represents leaders in online identity in the

(a) internet

(b) telecom

(c) data aggregation industries concerned with both market expansion and information security. (Open Identity Exchange).

If you are a provider of identity services, a site that wants to consume identity credentials from certified providers, or a professional IT industry assessor/auditor, OIX is the market in this case. OIX welcomes governments, professional associations, non-profit networks, and other communities who want to develop their own trust frameworks.Also, OIX members work together to jointly fund and participate in pilot projects (sometimes referred to as alpha projects). These pilots test business, legal, and/or technical concepts or theory and their interoperability in real world use cases[86].

Design: To effectively provide digital services, businesses and governments need to validate, verify, and authenticate identity in a cheap, reliable, repeatable manner. The rapid advancement of open identity technologies has created an interoperable technical platform to make this possible. While the technology exists for relying parties (such as an online retailer or government agency) to utilize third-party identity providers, the business and legal policies that set the rules for identity issues such digital transactions have lagged behind.

2.1.17 OIXNet

Introduction: Open Identity Exchange (OIX) Launches OIXnet: A Global Registry for Trust Frameworks. OIXnet is an official online and publicly-accessible

repository of documents and information relating to identity systems and identity system participants. Referred to as a registry, it functions as an official and centralized source of such documents and information, much like a government-operated recorder of deeds. That is, individuals and entities can register documents and information with the OIXnet Registry to provide notice of their contents to the public, and members of the public seeking access to such documents or information can go to that single authoritative location to find them [87]. There are several proposed or operational registries relating to identity systems other than OIXnet. Most such registries provide limited types of registration with respect to a particular identity system. OIXnet is, in essence, a registry of registries. It aims to provide, in one central location, an authoritative compilation of information regarding multiple registrations, so as to provide a one-stop shop. [87]

How it operates: At this time, there are currently (2) registration options available to TFPs (Trust Framework Providers)/ COIs (Communities of Interests):

Option 1: TFP/COI Only Registers Information at OIXnet[87]

In this case, the TFP/COI registers their trust framework requirements, scheme rules, conformance requirements, etc. at OIXnet. This is referred to as qualified material in the OIXnet Terms of Service. The TFP/COI does not require participants to register in this use case. These TFPs/COIs view registration as way of promoting their trusted identity system(s) while enabling interoperability. It is shown in Figure 2.23.

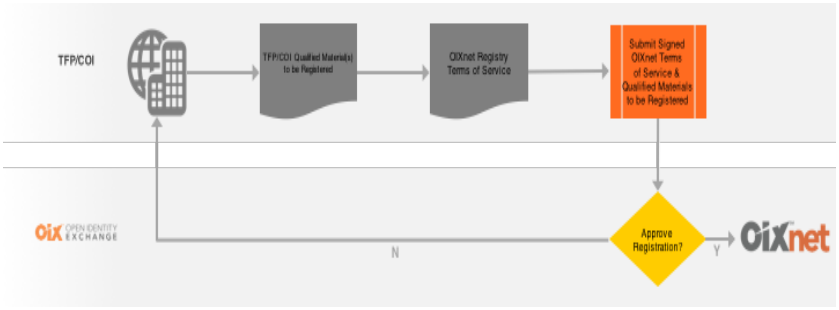

Figure 2.23: TFP/COI Only Registers Information at OIXnet

Option 2: TFP/COI Requires Participant Registration [87]

In this case, the TFP requires participating organizations to be certified and registered to participate in the trust framework. The TFP/COI registers these certifications at OIXnet on behalf of members/participants. This case is similar to the OpenID Connect self-certifications being registered at OIXnet.

Process of registration: It allows participants and users of identity systems to post relevant documents and information about the operation of their systems, their capabilities, and/or their performance, and provides other interested parties with centralized access to that information for purposes of using and relying on such systems and/or participants. Registration is the process by which a document or information is officially filed and recorded with a registry (such as the OIXnet Registry), and thereby made accessible by the operator of the registry for review by

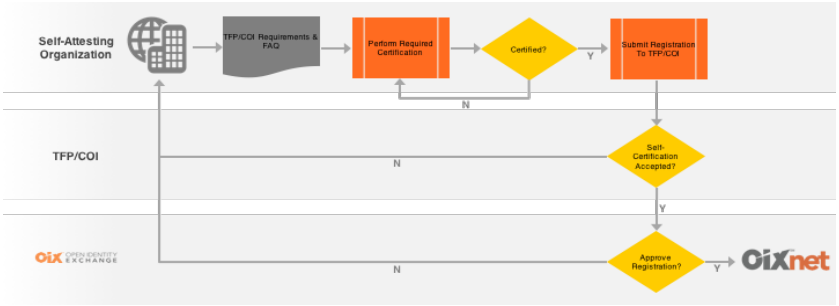

Figure 2.24: TFP/COI Requires Participant Registration

other interested stakeholders. It is anticipated that most registrations will not expire. In some cases where it makes business sense, some registrations may have registration-specific terms. All registrations will include the date of registration. [87]

In OIXnet Registry rollout, trust framework providers like the SAFE-BioPharma Association and SecureKey will register business legal and technical interoperability requirements at OIXnet. BioPharma will register its digital identity and signature standards for its trust framework participants at OIXnet. SAFE-BioPharma provides global high-assurance identity trust for cyber-transactions across the biopharmaceutical and healthcare industries. The global biopharmaceutical industry relies on the SAFE-BioPharma digital identity standard to assure trust in its cyber transactions. Participation in the OIX Net registry accelerates delivery of global interoperability and trust,â said Peter Alterman, COO, SAFE-BioPharma Association[87].

SecureKey: SecureKey will register its SecureKey Concierge trust framework in the OIX Registry. SecureKey Concierge is a service that Canadians use to access public sector services in Canada where high assurance is required. Canadian banks, which already have existing strong and trusted relationships with Canadians, are the trust anchors for the service; banks are ideally situated to establish trust for consumers online with government organizations. [87]

Advantages: The advantages linked with OIXnet are [87]

(a) It is the first registry developed by global leaders across industry sectors to enable online transactions at higher volumes, velocity and variety.

(b) The OIXnet registry provides the transparency into market leading OpenID Connect deployments and services. Also, OIXnet provides the visibility and understandability needed to enable trust among identity system participants.

(c) Registration helps enable the discovery of the legal assurance of technical conformance that ensures interoperability and accelerates adoption of this important global standard.

(d) OIXnet is a neutral, open online registry that enables a similar level of trust and discovery at Internet scale for a wide variety of trust frameworks.

(e) OIXnet provides a single authoritative source of trust-related information across multiple identity systems and multiple participants. It functions as a one-stop-shop that is increasingly being recognized as an authoritative source of cross-system trust information.

Design: OIXnet is designed to provide a neutral, public place trust framework provider (TFPs) and Communities of Interest (COIs) post their business, legal and technical policies and requirements relative to utilization of various means of asserting identity online. The initial example of OIXnet is the OpenID Foundation registering member and OpenID Connect certifications at OIXnet. Moreover, the IDESG (Identity Ecosystem Steering Group) self-attestation listing is just that: a listing of entities that assert that their policies and/or practices align with, or intend to align with, the goals of the organization.[87]

The OIXnet registry is multi-tenant, technology and policy agnostic, it offers no comment or judgment on TFPs/COIs requirements of registrants. In order to understand it, the IDESG registry will operate exclusively to register compliance with the Identity Ecosystem Steering Group Trust Frameworkâs requirements. The OIXnet registry is designed to provide a single comprehensive and authoritative location where information relating to identity systems can be safely stored for the purpose of putting others on notice of certain facts, and from which such documents and information can be accessed by interested stakeholders seeking such information. Identity systems registered at OIXnet include but are not limited to trust frameworks, trust schemes and certification programs. The OIXnet registry offers identity system participants in the private and public sectors an opportunity to share trust-related information about their respective systems and deployments to encourage global interoperability while enabling transparency and best practices [87].

Use case: The OpenID Foundation was the first to leverage OIXnet, registering OpenID certifications of deployment by members, including Google, Microsoft, ForgeRock, Ping Identity, PayPal, and Nomura Research Institute[87].

Any established trust framework provider (TFP) or Community of Interest (COI) that have established participation guidelines and requirements may register authorized documents or identity information on OIXnet, provided that it meets the applicable requirements set by OIXnet for the type of document or information it seeks to register[87].

The OIXnet Registry will continue to evolve and develop over time. At present, the following documents and items of information are authorized for registration on OIXnet[87]:

- Identity system trust frameworks (a.k.a. scheme rules or system rules)
- Self-certifications of compliance with an identity system standard, trust framework, or set of requirements
- Third-party certifications of compliance with an identity system standard, trust framework, or set of requirements

- Identity system white lists

Challenges: OIXnet registry will be human-readable-only. OIXnet is planning for a machine-readable service in the future. Also, the OIXnet registry will initially provide an index. As it evolves, it will incorporate additional functionality such as look-up and search. Of course, the contents of the OIXnet Registry is also searchable via search engines. [87]

2.1.18 KYC-Chain

Introduction: KYC (Know Your Customer)-Chain is based in Hong Kong and because users âownâ their identity, they get to choose which information is to be shared, and with whom. It is a novel platform built over the convenience and security of DLT (Distributed Ledger Technology), allowing users to manage their digital identity securely, while businesses and financial institutions are able to manage customer data in a reliable and easy manner[88].

How it operates: Built over distributed ledger technology, KYC-Chain provides consensus on identity of individuals and companies at the highest level of trust, bringing a new level of ease and simplicity to the process of onboarding new customers for businesses and financial institutions, while ensuring the compliance of regulatory standards[88].

Privacy self-sovereignty is handled when users own the ”keys” to their personal data and identity certificates. Therefore, identity owners are the only ones who get to choose which part of their information is to be shared, with whom and under what terms[88].

Strong cryptographic protocols are employed on the different layers of the platform in order to provide high-grade security, privacy and verifiable proofs of identity secured by the immutability of distributed ledgers[88].

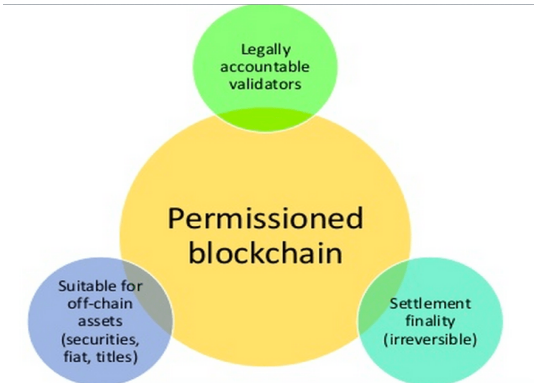

Figure 2.25: Framework of KYC (flagtheory)

As shown in Figure 2.25, permissioned blockchain is a ledger or distributed database to which certain actors have read and write access, and control of the network is limited to certain actors. It may or may not have an inherent currency; in fact, the system as detailed below is proposed without any mining. It deals only with

the underlying technology of blockchain consensus and distributed storage, and not censorship proofing or Byzantine fault tolerance[89].

Currently, KYC is kept in different silos each company maintains its own due diligence on customers. KYC, or Know Your Customer, has become a bane to regulated businesses in many industries, due to increased costs incurred from the collection and maintenance of customers due diligence materials. Essentially, these institutions must collect (and later, if audited, prove to regulators that they have sufficiently collected) documents that show that their customers satisfy the following three criteria: Proof of identity, proof of address, and proof of wealth. The exact standards for these documents are less important, and they vary slightly according to different jurisdictions. They are:

1. Proof of identity: Usually, a passport or government-issued ID, which should be certified or displayed in person. (First Flag of Flag Theory: Citizenship)

KYC suggest using video, as proof of identity is harder to fake when doing so than with a picture that is uploaded or scanned. It can also potentially use other systems if a higher level of authentication is needed. In the U.S., Europe and other regions that require this, knowledge-based authentication (KBA) can be utilized to provide an additional layer of verification. However, the quickest and easiest way to get authenticated is to use a public notary. [89]

2. Proof of residency: Usually, a utility bill or address that clearly lists the customer name and is current within 60 days (Second Flag of Flag Theory: Residency)

This criterion can be satisfied by the individual typing in the address, which is then cross-referenced with utility bill. KYC could then cross-refer users IP (Internet Protocol) address or browser heading with the stated address or utility bill. Eventually, KYC-Chain may be able to use a webhook or API (Application Programming Interface) provided by the utility company to gather the data directly. This would be particularly useful when it comes to utility bills that are issued in a foreign language; as such documents currently require a certified translation. Most importantly, KYC-Chain can be assured of not only the existence of these due diligence documents, but also their ongoing veracity. Currently, individuals or companies are required to submit these documents each time they open a new account, and banks and other financial institutions have no knowledge of account closures or adverse actions taken against the individual or company. However, with a blockchain, it can have a shared ledger to write and read, and financial institutions can then easily verify a client's bankability[89].

3. Proof of wealth: Letter of recommendation from a banker, accountant or lawyer who knows your financial affairs and can certify that your wealth was acquired by legitimate means. (Third Flag of Flag Theory: Banking)

KYC is storing IDâs on the blockchain but there are startups already working on this. The differentiating value here is that KYC is doing it: [89]

(a) Specifically for companies

(b) In accordance with existing KYC laws and regulations.

(c) In a way that enables debt and equity financing in capital markets at any point from incorporation to IPO (Initial Public Offering) with more confidence.

For a company, the following information is usually requested for KYC purposes shown in Figure 2.26:

Figure 2.26: Requirements of KYC [89]

Although these documents are more involved, KYC can perform the initial due diligence and then add the company to the blockchain in the same way. Basically, in KYC-Chain, one would need to provide this information to a trusted Oracle who permits access to the network. There are a number of reasons for this â the first and foremost being that KYC has a unified ledger to reach consensus, and the second being that individuals will no longer have to go through the entire KYC process from step one again. What KYC suggest is a permissioned blockchain for KYC individuals, with Oracles (or gatekeepers), who are trusted to control access to this chain. [89]

Ultimately, what a person need is a system that allows users to get KYC-verified just once, with their information being allowed to be used from incorporation all the way to IPO (Initial Public Offering). As there can be efficiencies in sharing the information and reducing the amount of independent KYC events, all parties save time. A key aspect of KYC-Chain is that users can easily prove they are who they say they are, but in a way that is private represented in Figure 2.27. [89]

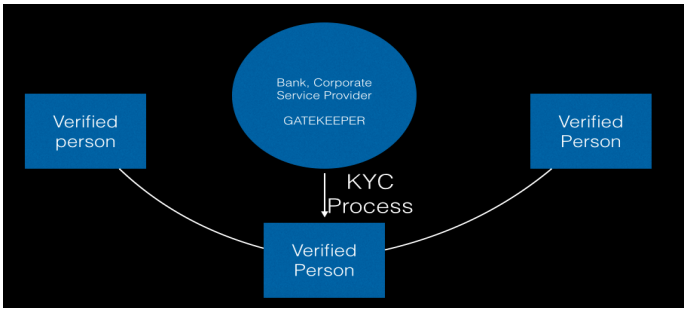

Figure 2.27: Verification with KYC (flagtheory)

Once a natural person or company has undergone a KYC check and his identity is verified and certain, user is then added to the network. This allows us to be certain

that everyone on the network has undergone the due diligence process represented in Figure 2.28.

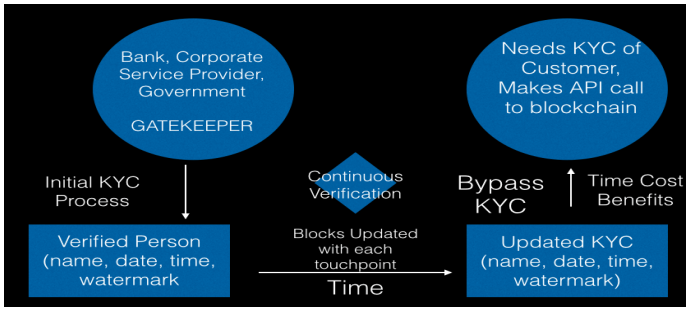

Figure 2.28: User added in KYC (flagtheory)

These improvements are made in existing systems; 1. The veracity of the identity improves over time (the opposite of current systems) 2. Both sides (the identifier and the identified) gain a time and cost advantage the more the system is used. [89]

Example: Exchange of KYC for Financing for Equity (flagtheory)NewCO Inc. wants to borrow in the form of sale of stock on the capital market. Citibank first needs the KYC information of the individual Tom Jones.

STEP 1: Personal KYC

Tom Jones goes through KYC with Citibank.

- Proof$_o f_C itizenship : U.S.Passport48989543 Proof_o f_R esidency : 123 FakeStreet$

- Proof$_W ealth : CustomeratCitibankNewYork forpastthreeyears$

STEP 2: Company KYC

Tom also controls the private keys to the shares in NewCo, with private key 5624bea9352 4050300a4bf83, so he authorizes Citibank to view the KYC. He shares the following information about NewCo:

- Jurisdiction: Delaware
- Company Name: NewCo Inc.
- Company Type: Delaware Corporation
- Company Registration Number: 901239123
- Registered Address: 123 Fake Street, Wilmington DE 09893

STEP 3: Document signed and financing approved

Using a smart contract editor, Tom, or his lawyer, is able to quickly append to the document the pertinent information for identifying the company and parties.

Tom performs a board resolution to quickly process the additional extra forms. The forms are signed by Tomâs private key, sent to Citibank, and a watermark is recorded to the blockchain.

Smart Contracts Corporate Governance: In the example above, we can see that a company, NewCo, has stored information about the founding of the company,

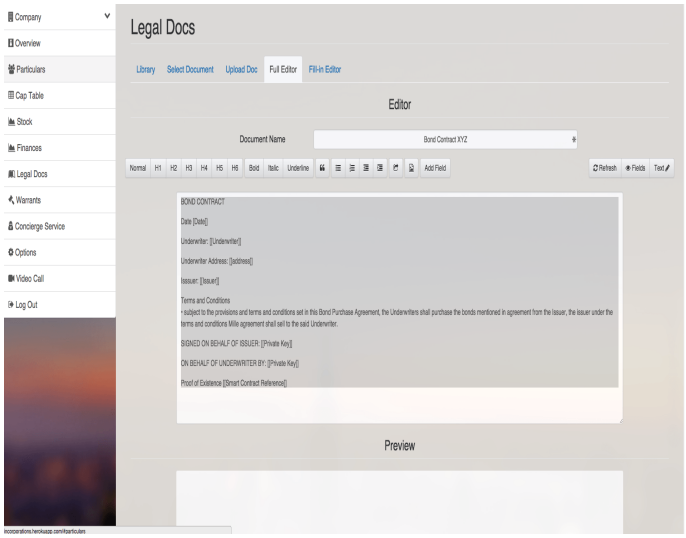

Figure 2.29: Working of KYC reference (flagtheory)

and the owner has the ability to upload his KYC documents. KYC-Chain can implement this system on top of legacy KYC systems, as long as an Oracle is keeping the file in a database off the chain.

Once a user has access to the KYC chain, he can associate his public key with ownership representation (in contracts) and actions (such as signing off a board meeting) with a private key. [89]

Advantages: The advantages of KYC-Chain of are as follows

(a) Distributed Ledger technology provides a reliable source of truth for identity and related events, also secured by a collection of cryptographic mechanisms to ensure that data can't be tampered with, thus serving as a solid provenance for audits and regulatory checks. [88]

(b) KYC-Chain is built taking into account the actual legal framework regarding identity and customer data at a global scale. Multiple mechanisms are provided to aid institutions to comply with regulatory norms, such as automatic smart checks on external data sources. [88]

(c) KYC-Chain provides a secure platform for sharing verifiable identity claims, data or documents suitable to satisfy compliance requirements for KYC onboarding or refresh without compromising the privacy of the owners while preserving the integrity of the data [88].

(d) Businesses and financial Institutions can onboard new customers with more efficiency and more trust in the data provided. KYC-Chain breaks admission barriers by providing secure mechanisms to verify digital identity[88].

(e) If KYC-Chain is going to entrust the banking system with our KYC information, it should transfer that information as securely and privately as possible. Arguably, blockchains can (but not without effort) have better security protocols than a traditional database[88]. (

(f) Due to blockchain technology, all records cannot be changed and a failure at one point does not mean a system-wide failure (decentralization). (flagtheory)

(g) It helps to reach consensus and avoid double identity or double spend: When dealing with identity, there can be only one instance. Sharing a distributed ledger helps prevent one legal entity or individual having multiple identities. [89]

(h) It allows for better integration across applications: Open-source blockchain solutions are a better platform to build on than a traditional SQL database controlled by a single company. [89]

(i) It is outside the complete control of any one entity: Distributed ledgers can be designed to stave off the hostile or negligent actions of a single dictator

(j) From incorporation all the way to IPO, permissioned blockchains and specifically the KYC-Chain implementation can help businesses increase efficiency and decrease costs [89].

Use case: Following are the use cases of the KYC (flagtheory) **Company incorporation**: Identity does not only apply to natural persons. Being able to prove the legitimacy of legal entities is also critical. KYC-Chain provides a convenient platform for incorporating companies, by allowing registered agents and owners to share the pertinent documents and get them digitally attested by notaries and institutions.KYC-Chain can help entrepreneurs, SME (Small and Medium sized Enterprise), larger institutions, investors, bondholders, stockholders and financial institutions while satisfying regulators with a private but transparent system to transact important private data with greater efficiency[88].

Capital markets: Currently, KYC checks must be performed on companies in a capital market, and whether a company will offer debt or equity is of little consequence. KYC will briefly discuss two very common options for financing within capital markets: Equity financing (through the sale of shares), and debt financing (through corporate bonds)[89].

Equity Financing: Equity financing in any jurisdiction requires that the offered conduct some due diligence and perform KYC checks on the individual or company buying shares. While there are several companies that work on clearing and settlement of bonds and equity, KYC-Chain would seek to integrate as the KYC provider, first by allowing participants to easily have their KYC added to a chain, and then by allowing that chain to be referenced in settlement. By utilizing smart contracts or even traditional legal documents, it can refer to the entity on the KYC-Chain network and have confidence that KYC checks have already been performed. KYC-Chain can also have further advantages and minority shareholder rights programmed into a specific company[89].

Debt Financing: Debt instruments are currently very difficult to transfer. Though KYC-Chain is not specifically a solution to work on settlement, it does facilitate identity and ownership of assets. It is a settlement system used by KYC-Chain to perform KYC checks. It can work with paper documents, as well as smart contracts

as these instruments move to being on a distributed ledger, and KYC-Chain can be 100 percent assured that the KYC process has been performed correctly. KYC-Chain can also do board meetings and other resolutions on the fly. KYC-Chain can reference a KYC watermark or transfer the files in an encrypted manner without the requesting entity or the granting entity needing any knowledge of encryption keys[89].

Design: KYC-Chain can be described as useful for record-keeping purposes, allowing for ownership of shares and identity, as there are two levels individual natural person KYC, and legal entity KYC. As proven in U.S. case law, companies are people, but they are also owned by natural persons, and as Ultimate Beneficial Ownership (UBO) information is critical to banking systems, this the primary objective of KYC-Chain: Verifying identity of people and companies, and ensuring proper KYC onboarding and maintenance.

2.1.19 Netki

Introduction: Netki Founders are Justin Newton, Dawn Newton [90]. Netkiâs designs enterprise-grade solutions promoting scalability, security and ease of use for Blockchain-based products. The Netki Wallet Name Service is an open standard that makes it easy to send digital currency between users or services, interconnecting the entire ecosystem. WNS is designed to allow service providers to easily register Wallet Names on their clientâs behalf, such as username.company.com, or for end users to register their own vanity names such as âpersonalname.meâ linking them directly to a wallet address[91].

One of the main issues that slowed the adoption of Bitcoin as a currency and payment system has been the complexity of Bitcoin addresses [92].

The blockchain lacks the human-friendly names normally found with websites and email addresses, which can make sending payments a rather cumbersome process. Netki wants to help people move away from confusing Bitcoin addresses, such as 15eA82FZLogpSb8nkQ5h5qaF3QNEwSeyCm, toward human-readable names such as kyletorpey.tip.me. Any bitcoin user would be able to send bitcoin to anyone else as easily as a Gmail user can send an email to someone using a web browser[92].

How it operates: Netki uses a combination of the Namecoin blockchain and Secure DNS (DNSSEC) to take care of name storage and mapping between a name and an address. Namecoin is an experimental open-source technology which improves decentralization, security, censorship resistance, privacy, and speed of certain components of the Internet infrastructure such as DNS and identities. âYour base records reside in the Namecoin blockchain proving ownership, and allowing for full, censor-proof control, Netki CEO Justin Newton explained via email. The actual wallet name toaddress lookups occur on standard DNS (Domain Name Service) records secured and authenticated using DNSSEC (Domain Name System Security Extension)[92].

This combination of decentralized and distributed solutions provides the control and ownership of the blockchain along with the privacy of keeping your name to address mapping off of a public ledger, Newton said[92].

The Netki CEO also explained that wallet providers will be able to hand out names in a manner similar to how email addresses are handed out to Gmail, Outlook, Yahoo and other online mail providers. He specifically mentioned ChangeTip use of the tip.me domain as an example of this feature[92].

Newton was also able to share his thoughts on the differences between Netki and another Bitcoin name system, OneName: We believe that a lot of what OneName is doing is really fantastic. There is a need for a decentralized way to validate your social identity, and their roadmap feature of using signatures instead of passwords for logins is excellent and long overdue. Netki do believe, however, that tying your identity to your wallet address on a public ledger negates the possibility of privacy on the blockchain. For Netki, making it easy to share your address with anyone without having to publish it to everyone is one of the keys to our service[92].

Netki also supports Payment Requests, which are sometimes referred to as the SSL (Secure Socket Layers) for wallet addresses. Newton explained that the integration of Payment Requests will allow users to see a green lock next to an address in the To field of a Bitcoin wallet. That lock helps users confirm that they are sending bitcoin to the correct individual, organization, or company. This process is similar to the green lock found next to website URLs (Uniform Resource Locator) that have been secured via SSL and an HTTP(Hyper Text Transfer Protocols) connection.The combination of HD Wallets and Payment Requests with Wallet Names increases the privacy and security of sending bitcoin, while at the same time making it more user friendly and reassuring to end users, Newton said[92].

The application uses the Hyperledger blockchain to provide a decentralized, open-source app, approved by governments, and fully Anti-Money Laundering (AML) and Know Your Customer (KYC) inclusive. Once a Digital ID is created and validated, it can be easily shared via digital identity certificates that are legally valid in the U.S. and other jurisdictions, said Netki CEO, Justin Newton. Netki Digital ID addresses various regulatory requirements, including the U.S. Department of Treasury's Travel Rule, which states that all four participants in a transaction (sender, receiver and each of their financial partners) must disclose validated identities before exchanging amount [93].

Advantages:

(a) Digital identity is a fundamental requirement for compliant blockchains. Netki is excited to do its part by delivering a production-ready service that makes blockchain safe for mainstream adoption and makes identity as easy to manage as PayPal.Said Newton (Parker, Netki launches Digital ID solution, which Bitt is using with Central Banks in the Caribbean, 2017)

(b) Netki co-authored a new peer to peer payment protocol (BIP75) that allow sender, receiver and their financial partners to exchange all four identities via a private encrypted channel. BIP75 provides a critical foundation for compliant blockchain transaction and is publicly available as an open source protocol[94].

(c) Netki delivers software and services that enable financial technology and service companies to meet regulatory and legal compliance requirements on both public and private blockchains. Netki digital ID and Wallet names makes blockchain safe for a broad range of business and personal use cases, while meeting national and international legal standards[94].

(d) The service provides automated onboarding and validation of new customers, and easy sharing of digital identities, thus closing a critical compliance gap that limits blockchain innovation and adoption[94].

(e) Netki protocol will allow its user base to easily verify, and exchange digital identity by enabling its immutable blockchain-based platform to strengthen these use cases. The company's wallet service is also made to be more simple with users generating a name associated with their wallet rather than a 16 digit Bitcoin address[95].

Use Case: California blockchain startup Netki announced the launch of their highly-anticipated Digital ID smartphone application at Consensus 2017. The ID platform was designed to help people control their identities better, while at the same time giving anyone who needs a government-approved identification a feature-rich, blockchain-based, free solution that can be used anywhere[93].

The software suite can be embedded into variety of finance, health care and business applications[94].

Financial services complying with regulatory standards can implement Netki services utilizing the ability to track and verify digital identity, the company says. This includes KYC (You are your Customer)/ AML(Anti Money Laundering) requirements, traditional banking verification, and overall security of digital identity free from vulnerability. During the announcement CEO and co-founder Justin Newton told Bitcoin.com: Netki is proud to have OATV (Oreilly AlphaTech Ventures) leading our round. This funding will allow us to invest in our open source tools and support our growing global customer base.OATV and its affiliate O Reilly Media have deeply respected roots in the open source developer community, adds Newton. They understand the value of creating standards early on that can be built upon to enable widespread, rapid growth of a nascent technology. We are thrilled that Netki is OATV's first investment in the blockchain space[95].

Design: To use Netki platform, anyone can simply download the free application, use it to take a selfie, and then attach a scan of both the front and back of their state-issued identification card, which is then run through an authorization check. The whole process of making a legal, digital ID takes âonly a couple of minutes,â according to the company[93].

Besides the easy onboarding of new customers, the application also provides validation and sharing of the digital identities with other users. Webmasters and other developers are currently able to use their open source API (Application Programming Interface) to validate IDs using the system, making the ID useful in a wide range of use cases. Pricing, Netki says, is charged to businesses and institutions based on the number of certificates and complexity of validation[93].

2.1.20 ShoCard

Introduction: ShoCard is a digital identity and authentication platform built on a public blockchain data layer, using public/private key encryption and data hashing to safely store and exchange identity data, which includes biometrics such as fingerprint, facial, iris and voice. ShoCard's approach to identity is different than existing solutions in that the user owns and carries her own data within her mobile app and is the sole person who decides with whom to share it with and which pieces of identification to share. The blockchain in then used to validate that information and confirm other third parties who have definitively certified the identity of the user. There is no privately held central location that holds userâs private information and pieces of a userâs identification does not need to be spread in other services in order to authenticate or prove ownership of an account. The mobile app is as easy and intuitive to use as a drivers license, but secure enough for a bank. It was founded in 2015[96].

A lot of companies are looking at the blockchain for things other than bitcoin. ShoCard created a digital identity card that is as easy to use as a drivers license but it is so secure that a bank can rely on it, ShoCard co-founder Jeff Weitzman told[97].

How it operates: ShoCard allows users and enterprises to establish their identities with one another in a secure, verified way so that any transactionâwhether its to login, share personal information, or complete a financial transaction can be accomplished quickly, seamlessly and with peace of mind. Creating a ShoCard ID can be done either through application, or a company or entity can build in our technology into their existing Apps via our SDK (Software Development Kit).

Figure 2.30 represents the workflow of ShoCard

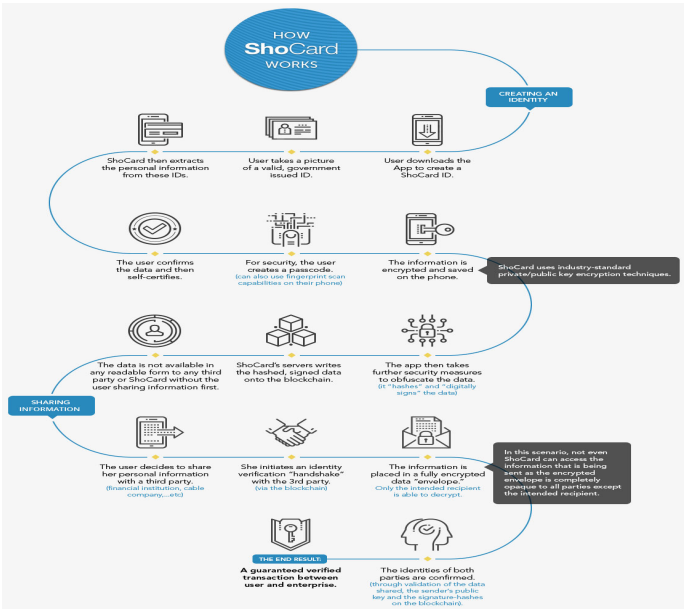

Figure 2.30: How ShoCard Works

Figure 2.31: User credential

Figure 2.32: Verification

Certifying a Userâs Credentials: The Certification process can be done as part of a third partyâs âKnow Your Customerâ process.

With permission the users ID credentials are verified for authenticity.

The user may be asked further questions to verify they are, in fact, who they say they are.

As a final security step the third party may review the information in the App.

Once an authoritative 3rd party (such as a financial institution, government or other trusted entity) Certifies the users ID, all other future parties can reference this certification and be assured that the information provided by user through the application is, in fact, accurate and belongs to them.

Example: Its perhaps best explained by a car crash. As veteran entrepreneur Armin Ebrahimi tells it in interview, his car was hit by a truck two nights ago. The driver had no insurance, and he had little reason to trust him because of the poor quality of his government-issued driver's license. "The picture did not really match him. It was difficult to know its him, the picture was a little more clean cut. Its got a PO box address on it, so I took the information I could,Ebrahimi explained[98].

In interview, Ebrahimi provided a deeper dive into the underlying technology of the product he hopes will transform identity on the web, mobile and real world. Ebrahimi told CoinDeskShoCard create a private and public key pair that allows

Figure 2.33: further verification

you to access the blockchain and create separate key pairs for each of the fields that you are going to be storing [on your ShoCard]. So user has a master private key and private keys for individual data fields[98].

While top of mind given his recent experience, Ebrahimi sees ShoCard as effective beyond insurance incidents, impacting how people verify themselves to e-commerce providers, banks or any third party to whom they must prove their identity to ShoCard in practice [98].

Figure 2.34: Identity authentication

Though still in the prelaunch phase, ShoCards digital ID provides details such as the full name, address, signature, date of birth and physical details of each user. While it looks like a mobile drivers license and contains the same information, the difference, according to Ebrahimi, is each field on the ShoCard is protected with cryptography[98].

ShoCard create signatures for each field and hash that encrypts the data thats on there, then it creates a digital signature of it, then put it on the blockchain, he explains. ShoCard doesn't put the user's data on the blockchain, rather just its own cryptographic proof that the data is correct[98].

All you can do is validate that later," he added. "I would give you my public key and name and say here's my entry on the blockchain with a signature. You can use that data to go in and validate it, but I have to provide you my name to validate it[98].

If both parties in the car crash were using the ShoCard system, Ebrahimi said, the application could be made to produce a QR code that when scanned could allow the users to pass the blockchain record of their identities to each other securely[98].

"My ShoCard would go in, pull the data out of it to verify that it is on the blockchain. Let's say [the truck driver] was certified by the DMV(Department of Motor Vehicles) and his bank. I could look at those [certifications] and say that these are ones that I can trust." [98]

Additionally, users could have control over what they share. In the instance of a car crash, a user might need to take another party's name and address before submitting it to a third party like an insurance provider[98].

"I don't have to see everything else," he continued. "I don't need to ask for his weight and eye color." A similar exchange, he said, could also take place without QR codes

using a Wi-Fi transfer protocol such as Apple's AirDrop. Either way, digital data is validated securely using bitcoin's secure digital ledger[98].

Advantages:

(a) If someone is using your credit card to purchase something online, you will get a notification and you can block the purchase right away[97].

(b) ShoCard is tackling use cases in mind and is already in talks with companies that deal with identity management â credit card networks, banks, anti-phishing companies and others[97].

(c) "Until the blockchain there was no way to build the best infrastructure, keep it as secure as you can and make sure no one can compromise what's inside. There are so many public cases where credit card data is breached, we see that happen publicly over and over" [98].

(d) Blockchain provides compelling benefits even when compared to two-factor authentication, which has recently proven susceptible to hacking and interference. "Two factor is a great step forward in terms of providing security, but we're looking at two years from now, how does that landscape change and how do we do we focus on identity" [98].

(e) One of the things ShoCard has done is hidden away a lot of that complexity from the users. You understand looking at your ID, because it's pushed out by a trusted enterprise.

Use Case: There are some systems out there now that banks are using. it can be a window that appears from your bank and says you have to log in here and use this PIN code that we gave you three years ago, Weitzman said. ShoCard wants to partner with banks to replace these weird redirections when you do an online purchase. It is a win-win situation: ShoCard gives you peace of mind because you have to approve purchases with your phone, and the credit card company gets a definitive identity check.

Working with banks is a smart first step for the startup. Banks have been subjected to know your customer laws and already need to thoroughly check your identity when you open an account. They can verify your identity before it is sealed using ShoCard, making this process much simpler for the startup[97].

Ebrahimi suggested ShoCard is already talking to banks interested in the technology, but declined to name potential partners. Presentations for the company suggest ShoCard believes its solution could be a compelling alternative to services like Verified by Visa, which while allowing major financial institutions to leverage access to user data, require them to store it in centralized databases. More immediately, Ebrahimi sees the service as potentially appealing to bitcoin companies that currently rely on two-factor authentication services or other tools. [98]

Still, Ebrahimi believes ShoCard will perhaps be most immediately useful online, where online authentication is increasingly handled by Internet giants such as Google and Facebook. Part of the current problem, Ebrahimi argues, is that these companies earn revenue from reselling data, and further, they have the ability to update

their policies often, and in ways that might not always be friendly to users. ShoCard, Ebrahimi believes, could compete against these systems if it could achieve a similar scale because the blockchain would help return control to users [98].

"The people we have to convince, most of them are interested in blockchain," he said. "A bank would have a hard time trusting another database, but you don't need to trust us in storing or maintaining the integrity of the data, making sure it doesn't get hacked into. I can independently validate the data and insist on its accuracy with an open database"[98].

ShoCard SSO: ShoBadge is the enterprise-level Identity Provider (IdP) using ShoCardâs Identity Management System (IMS). ShoBadge provides enterprises with the most secure form of ID management, eliminating the need for large databases of usernames and passwords vulnerable to hacker breaches. Employee ID information is stored encrypted on the employeesâ mobile devices, then verified through the blockchain, creating user-centric identity storage, paving the way toward Bring Your Own Identity (BYOID). ShoBadge seamlessly integrates into existing solutions, like Okta and Azure Active Directory for easy deployment[99].

- Company Admin sends out an invite to an employee.
- Employee accepts the invitation and registers ID information on their device.
- To login, a unique SessionID is created in a secure QR Code, employee signs by clicking or scanning the QR code on their login screen (no usernames or passwords).
- Employee verifies login.
- Secure authentication is completed.
- All applications used by the employee (email, Salesforce, Amazon Web Services, etc.) can be accessed post verification.

Password Login: ShoCard Password-less Login provides the ability for a user to log into a website (that's enabled with the ShoCard platform), without the need to remember passwords. The first time the user visits a site, they would need to link their ShoCard ID with the website and register. Once the registration is completed, they would be able to interact as normal with the website. Any subsequent visit to the website can be completed by scanning the QR code for login, or by entering their username without a password and attempting a login. This would allow them to authorize the login via their ShoCard App. [99]

- User enters their username or scans a QR code.
- The user then receives a notice to authenticate using Touch ID.
- The user verifies login.
- Secure authentication is completed.

Financial Services Credentialing: In addition to know your customer (KYC) checks, financial services spend a lot of time and money on qualifying individuals

for the variety of financial instruments that are available. Most instruments require qualification including credit cards, auto loans, HELOC (Home Equity Line of Credit), and every time that the individual is qualified, it requires a separate payment for the credit check [99].

- With the use of the ShoCard credential framework, an institution could qualify an individual for a particular qualification (e.g., credit score > 700).
- The user is given the credit score and it's saved locally on their phone and that individual's certification is hashed and then digitally signed by the banks private key and placed onto the blockchain.
- Any other associated institution could then be passed that certification by the customer
- Because the certification was done by a trusted certifier, a re-check of the qualification would be unnecessary, saving the financial institution time and money, and the transaction can be done real-time and meet the customerâs expectations.

Improving customerâs travelling experience at airports hotels: The travel experience has been fully implemented as a proof of concept (POC) with SITA, the world leader in information technology for the aeronautic industry. Hereâs how it works: [99]

- A traveler that is embarking on a journey can obtain a single travel token for the entire duration of their trip.
- The initial check occurs at the ticket counter, where the individual would be positively identified and issued the travel token. A photo/selfie is also taken for verification purposes.
- The personally identifiable information, the travel token, and the photo are all stored secure on the individualâs mobile device.
- When the traveler approaches any gate or checkpoint, they can present the travel token via a QR code on the SITA Traveler App.
- The Agent or a kiosk would scan the code, validate the travel token and check that the individual matches the selfie. If the checks pass, the traveler is permitted through the checkpoint.
- A travel token would be persistent for the entire duration of the journey. The traveler can use the same token through the airport to their destination, during their trip, and as well on their journey back to their point of departure.

Call Center Authentication: Call centers require KYC (know your customer) checks prior to being able to assist a customer with any issues that they may be experiencing. These checks can take a long time to perform, and often may be frustrating since they may have outdated/incorrect information. The ShoCard Call Center Login solution is simple and more robust in terms of validation than the current processes (ShoCard) After a user has been verified as an individual, when a

user goes to a website or calls a call center, rather than answering a string of questions, they are simply prompted by their mobile device to approve the interaction [99]

- The call center representative initiates the authentication by entering the customer's account number, email, or some form of User ID.
- The customer then receives a notice to authenticate using Touch ID.
- The customer verifies login.
- Secure authentication is completed, and the agent is able to look at the customers' data and address the customers' need.

Identity Verification: Identity verification can be an initial step in a know your customer (KYC) process for Financial Institutions, Airlines, or Health Providers. These checks are safer and more robust than the standard offline methods, since physical documents may be forged or have become outdated but have not been physically rescinded. With ShoCard, the true state of the data can be verified and even compared with the biometrics of the individual to ensure the person presenting the data is the real-individual who owns the data [99].

- With ShoCard, identity verification is a simple and straightforward process. Depending on what pieces of information needs to be checked, the individual selects the appropriate fields in the ShoCard App (an image, name, address, age, or any other combination of personally identifiable information.
- Other cards may be added to the ShoCard App, such as Social Security Cards, Health Cards, Green Cards, Employment IDs, etc.
- The actual card images, as well as select information on each card, can be shared to the Agent that is performing the check.
- For each field or card being verified, each piece of data is hashed and compared to the signed hash of the same information that is on the Blockchain, as well as any related certifications shared that authenticate the data.
- All the pieces of information that pass the certification process will be displayed as being certified, and all the non-certified pieces of information will be highlighted as uncertified on the Agentâs device.

  Automated Registration: Online registration is often studied due to the high level of drop off that occurs in a sign-up process. Website registration can be assisted greatly using the ShoCard system, with the automated pre-fill and user-controlled passing of information directly to the website being registered. One-click registration could possibly be one of the most effective ways of improving the user experience and allowing users to immediately participate as a registered member to these websites[99].

- The process for registration would start at the login screen for the website. The individual would scan a QR code that appears on that screen, or click on a Register now button. The following setup screen would have another QR code, which could be scanned.

- The user would receive a prompt on their mobile device to confirm that a specific set of information is being requested to complete the login request.
- If the individual confirms, then the form is automatically filled out, and the user only needs to hit Submit to become a registered user.

This process also works for waivers and sign-ups at places like a sports club or a climbing gym. A QR code on the device being used to collect waivers is scanned, the mobile device is prompted to provide a signature and other pertinent information, and if the user accepts, the process is complete.

Proof of Age: When individuals need to prove that they are of age in the current paradigm, they typically must provide a physical driver's license to the agent that is checking that information. There are some issues that people do not typically consider with this namely the driver license contains a lot of information that you may not necessarily want to share with the agent. For example, a single lady at a bar may not want to share her name or her current address to a shady bartender. The ShoCard platform allows users to only share the pertinent information, and keep all other personally identifiable information (PII) hidden and safe with the individual [99].

There are many use cases for proof of age buying alcohol, going out to a club, entering an R-rated movie, buying cigarettes, etc. For each instance, the ShoCard implementation is relatively simple[99].

- On the ShoCard App, the individual selects that they want to share the fact that they are over 18, 21, or 55 (for senior citizens), and selects âShareâ.
- A QR code is generated on the individualâs phone, which is then scanned by the Agentâs device.
- The Agent then gets a verification (green check) or a denial of verification (red X) that the individual being checked is over the appropriate age.

Road Stop: Mobile driverâs licenses (mDL) and digital identity (dID) has been receiving a lot of attention from the standards organizations ANSI and ISO as well as the American Association of Motor Vehicle Administrators (AAMVA). ShoCard is actively participating with these organizations. There are many uses of a typical driverâs license outside of the original purpose of conveying the rights and privileges of driving. These include [99].

- Proof of address
- Proof of age
- Visual identity checking.

These same attributes are true for mDL and dID, and there are many benefits of having these forms of identification on a mobile device. Information on a mobile device is more secure than a physical ID if you show your driverâs license, you may be passing information that you donât want to be shared. With a mDL, only the information that is pertinent would be shared, depending on the situation. Verification is more robust with a mDL â the trust system that exists with the certification

network, and the nature of the blockchain allow for a robust environment for identity management. Also with a mDL, certifications and privileges are immediately changeable and revocable.

- The driver initiates an information sharing session and selects the information to be shared with the Peace Officer. This would typically include the photo of the driverâs license, all fields in the license, as well as a higher resolution photo of the individual.
- The officer would scan the QR code that the App generates with his Agent App, and the information would be verified against the blockchain as being certified data points, and visually inspect the photo as an additional verification step.
- The officer would then continue with the interaction knowing that the individual has been certified as the individual that they are claiming to be.
- Road stops and public safety enforcement would take place similar to the Age Verification or Identity Verification examples above. Some differences might be what additional fields would be passed â the privilege of driving a motorcycle, a commercial vehicle, etc.

Design: ShoCard is basically a tiny file that only you can manipulate. When you create your ShoCard, you first scan your identity document and sign it. Then, the mobile app will generate a private and public key to seal that record. It is encrypted, hashed and sent to the network of communicating nodes running bitcoin software for later use[97].

After this initial creation process, you will use the companyâs app to retrieve your information. But the best part of this technological feat is that ShoCard hides all this complexity for the consumer. There are multiple use cases for something like ShoCard, starting with online purchases[97].

Challenge: Question of scale is a challenge of ShoCard which means the most pressing challenge for ShoCard isn't technology, Ebrahimi acknowledges, it's a question of scale. As the car crash analogy illustrates, ShoCard can only be as useful as the number of people and third-party institutions using it. Identifying this "chicken-and-egg problem", Ebrahimi said, was a key factor in ShoCard choosing to adopt a business-to-business (B2B) marketing strategy [98].

2.1.21 UniquID

Introduction: Stefano Pepe is the CEO of Unique ID. UniquID Wallet provides secure identity management, integrated with fingerprint and other biometry on personal devices. Ready to be deployed on custom hardware, servers, personal computers or smart phones and tablets, UniquID Wallet runs also on battery and low-powered devices, providing integrity and interoperability at the edge of your infrastructure [100].

How it operates: UniquID Appliance provides lightweight trusted node service, built to run on virtual machines and workstations inside your infrastructure. Easily

customizable to userâs requirements of security, costs and scalability, this component hosts the blokchain infrastructure, keeping the smart contracts decentralized, confidential and redundant among your entire facility[100].

Advantages: [100]

(a) Identity before security: Devices are saved inside your private blockchain, a digital vault built to protect your digitally connected assets through secure authentications.

(b) Devices are independent: Authentications are device to device, without any intermediaries, ready for the increasing challenges of cyber security and Internet of Things.

(c) No more passwords: Device-centric solution recognizes users through personal connected objects, removing the inherited risk of user generated passwords.

Design: UniquID is solving the increasing challenges of the Internet of Things. Applying principles and strengths from the most successful decentralized applications, it provide a secure, productive and interoperable infrastructure where smart devices communicate and cooperate without boundaries, keeping their identity and valuable data away from remote and potentially vulnerable concentration points. Young talents and experienced enterprise IT professionals created from scratch a trustless, decentralized, Bitcoin-inspired access management solution for a brilliant and secure Internet of Things future[100].

UniquID Supervisor APIs are designed to create, inspect or revoke relations between devices, providing the tools necessary to manage access rights to your digital assets. Integrated with your existing resource management platforms is capable to seamlessly issue-update-sign-revoke relations on the blockchain, preserving your IT investments and best practices[100].

2.1.22 Uport

Introduction: It is developed by ConsenSys. uPort is building a secure, easy-to-use system for self-sovereign identity (Uport) Self-sovereign identity is the ability to own and control your identity. Many websites also choose not to hold personal data but use Facebook or Twitter as identity providers. Either way, once you provide your date of birth, it is in the service providerâs hands. What uPort and other self-sovereign identity systems do is utilize blockchain technology and therefore cryptography to wrestle ownership and control back to you[101].

It is built on Ethereum (Decentralized platform for smart contracts). Ethereum smart contracts provide us with the first general purpose solution to the problem of cryptographic key management, and set the groundwork for persistent identities. An Ethereum identity can be represented by the address of a smart contract or a traditional public key[102].

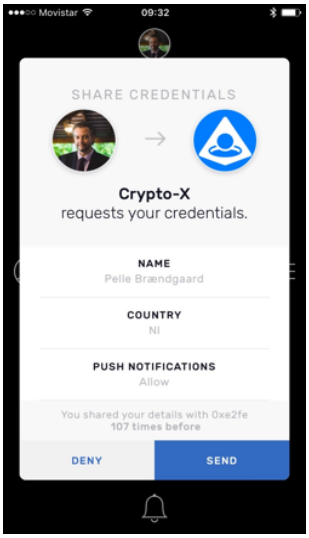

Figure 2.35: Working of uPort

Since smart contracts can be controlled by other smart contracts, they can be programmed to support various methods of key recovery logic. This flexibility of control logic enabled by Ethereum allows cryptographic identities to become both user friendly and meaningful. uPort identity is a very simple smart contract that is controlled by a replaceable controller contract, which contains key recovery and access control logic. The controller contract is in turn controlled by keys stored securely on your smartphone[102].

The uPort technology consists of three main components: [103]

1. Mobile application: The mobile application holds the users keys.

2. Smart contracts: Ethereum smart contracts form the core of the identity and contain logic that lets the user recover their identity if their mobile device is lost.

3. Developer libraries: Finally, the developer libraries are how third-party application developers would integrate support for uPort into their apps. How it operates: At the most basic level, uPort identity is an Ethereum address. So if all you need when interacting with an end user is their Ethereum address, this is provided by uPort. However, uPort also allows applications and their users to exchange information privately, while still backed by the security of the Ethereum blockchain as shown in the Figure 2.35.

In more detail, uPort identity is a complete digital representation of a person (or app, organization, device, or bot) that is able to make statements about who they are when interacting with smart contracts and other uPort identities. This ability to make statements about themselves, without relying on centralized identity providers, is what makes uPort a platform for self-sovereign identity.

The real power of uPort is that it makes Ethereum application more approachable to end users. Some of the interactions enabled by uPort are simple blockchain transactions like buying shares on the Gnosis prediction market, while others include off-chain interactions like making private statements to other uPort users or applications. All of this is possible without your end users having to endure complex key

management.

Each identity is capable of storing the hash of an attributed data blob, whether on IPFS (Inter Planetary File System), Azure, Dropbox, etc., which is where all data associated with that identity is securely stored. Identities are capable of updating this file themselves, such as adding a profile photo or a friend, or they can also grant others temporary permission to read or write specific files. Since they can interact with blockchains, uPort identities can also control digital bearer assets such as crypto currencies or other tokenized assets[104].

Example: Take this scenario. On Facebook users need to be aged 13 and over and require a D.O.B. (Date of Birth) instead of giving that data away, I can provide an attestation of my age via the blockchain. In other words, I claim that my birthday is Jan 1st, 1982 then I can have someone from an institution like a bank digitally sign that assertion and say we have checked this persons passport and we can attest to the fact that her birthday is Jan 1st, 1982. [101]. In the example above, at no point do I provide the actual date of my birthday and that is very neat but consider this. Without attestation from a 3rd party such as a bank, notary or a government system like RealMe in New Zealand to attest (verify) my actual birth date, I could claim my D.O.B to make me any age I want. 65 to get the pension and 12 to get kids price on movie tickets. Therefore, I do need to trust some reliable 3rd party to attest or back up my claim. And that is the crux of the matter. uPort does not claim to remove the need for trusting a 3rd party. uPort you have full flexibility to choose who you trust, and you can trust different identities or authorities for different things. Who verifies personal data? Therefore, it seems we still have to trust some 3rd party but there is more flexibility which is great. [101]

Advantages:

(a) Self-sovereign ID in uPort enables you to collect verifications, log-in without passwords, digitally sign transactions, and interact with Ethereum applications.

(b) uPort doesnât remove the need for trust in 3rd parties but instead users choose the 3rd parties they want to trust. [101]

(c) Uport facilitates for a persistent identity across projects with means of identity recovery if, say, the phone is lost.

(d) Official institutions, such as, say, the Passport Office, and others, can vouch for the correctness of an identity, making possible the signing of contracts through an Ethereum public key. [105]

Design: If user creates uPort identity within the uPort mobile application, user can set personal information about to a public profile. By default your name, image, banner image, and description are set to public. The way the uPort App works with the uPort Registry is really simple: [102]

- It creates a JSON (JavaScript Object Notation) profile object.

- The profile JSON is uploaded to IPFS.
- Finally it creates a set attributes transaction on the uPort Registry, which sets the resulting IPFS hash as a public statement.

Use Case: uPort allows end-users to: own and control their personal identity, reputation, data, and digital assets; securely and selectively disclose their data to counterparties; access digital services without using passwords; digitally sign claims, transactions, and documents; control and send value on a blockchain; interact with decentralized applications and smart contracts; and encrypt messages and data.

uPort allows enterprises to: establish a corporate identity; easily onboard new customers and employees; establish an improved and transitive Know-Your-Customer process; build secure access-controlled environments with less friction for employees; reduce liability by not holding sensitive customer information; increase compliance; maintain a network of vendors; establish role-specific, actor-agnostic identities (i.e. CTO) with specific permissions[105].

Challenges: In future versions of the application, user will be able to control what information is in your public profile, but for now you can think of it as the Ethereum equivalent of your public Facebook profile[102].

Chapter 3

Best Solution

3.1 Introduction

Cyberspace and real life are merging. With the Internet of Things (IoT), individuals and devices are increasingly connected to the Internet and physical objects are seamlessly integrated into information networks. Machines and robots are able to sense and analyze data, enabling control of the physical world from a distance. The IoT will change the way we live, work and communicate. No business will be unaffected in the long term. But these big changes imply new challenges, particularly with respect to security[106].

Security is essential for IoT, especially with respect to identity. If weâre going to connect our houses, cars and factories to the Internet, they must be secured. Individuals, machines and devices must be securely identified so that only authorized access is permitted. Private user data and corporate secrets must be protected from theft and fraud.. Therefore, security should be designed into IoT systems from the beginning, not tacked on later[106].

With the rise of IoT, device security and especially identity is more important than ever. IoT devices control critical systems such as cars, factory systems, door locks, and security cameras. Yet they are exposed to a variety of network-based threats. To block unauthorized parties and provide security, IoT devices must be able to conduct mutual authentication with users, other devices, and the cloud. Fortunately, device identity technologies are well established and widely available[106].

Cryptographic authentication is the best approach to IoT device identity. IoT devices are fully capable of establishing, maintaining, and employing long cryptographic keys. There is no reason to employ passwords for device identity. With security hardware, these cryptographic keys can be protected against disclosure. (Hanna, 2015) Some security chips such as the open standard Trusted Platform Module (TPM) â go further than establishing device identity by also performing encryption and detecting device compromise. Monitoring system integrity is especially important for IoT because a rogue device with proper credentials can cause real physical damage [106].

The contribution of this research is to extend the Blockstack application which is using following concepts

- Blockchain
- Decentralization
- Device identity

Blockstack: A decentralized internet is introduced by Blockstack. A decentralized internet is one where user doesnât need to trusts any intermediatory or third party. On this basis, blockstack was developed. With blockstack, user can control their data and application runs on their devices without any middleware, password, massive data breaches and service tracking around the world[107].

Preliminaries/Background Study:

Internet of Things: The term Internet of Things (IoT) was first used in 1999 by British technology pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors. Ashton coined the term to illustrate the power of connecting Radio-Frequency Identification (RFID) tags used in corporate supply chains to the Internet in order to count and track goods without the need for human intervention[108].

Today, the Internet of Things has become a popular term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items. While the term Internet of Things is relatively new, the concept of combining computers and networks to monitor and control devices has been around for decades. By the late 1970s, for example, systems for remotely monitoring meters on the electrical grid via telephone lines were already in commercial use. In the 1990s, advances in wireless technology allowed machineâtoâmachine (M2M) enterprise and industrial solutions for equipment monitoring and operation to become widespread. Many of these early M2M solutions, however, were based on closed purposeâbuilt networks and proprietary or industryâspecific standards, rather than on Internet Protocol (IP)âbased networks and Internet standards. Using IP to connect devices other than computers to the Internet is not a new idea. The first Internet âdeviceâââan IPâenabled toaster that could be turned on and off over the Internet was featured at an Internet conference in 1990[108].

IOT can be defined as follow *The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention.*

Identity Management: In the IoT world, identity management must be able to identify devices, sensors, monitors, and manage their access to sensitive and non-sensitive data.

Blockchain: By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Blockchain's network lacks centralized points of vulnerability that computer hackers can exploit. Todayâs internet has security problems that are familiar to everyone. People rely

on the username or password system to protect our identity and assets online. Blockchain security methods use encryption technology[109].

The basis for blockchain are the so-called public and private keys. A public key (a long, randomly-generated string of numbers) is a usersâ address on the blockchain. For example, Bitcoins sent across the network gets recorded as belonging to that address. The private key is like a password that gives its owner access to their Bitcoin or other digital assets. Store your data on the blockchain and it is incorruptible[109].

A blockchain is another type of database for recording transactions-one that is copied to all the computers in a participating network. A blockcahin is thus sometimes referred to as distributed ledger. Data in distributed ledger is stored in the form of structures called blocks. The important parts of blocks are (What is blockchain?) Header: it includes metadata, such as unique block reference number, the time the block was created and a link back to previous block. Content: It is validated list of digital assets and instruction statements, such as transactions made, their amounts and addresses of the parties to their transactions. Given the latest block, it is possible to access all previous blocks linked together in a chain, so a blockchain database retains the complete history of all assets and instructions executed since the very first one- making its data verifiable and independently auditable. As the number of participants grows, it becomes harder for malicious actors to overcome the verification activities of the majority. Therefore, the network becomes increasingly robust and secure[110].

3.2 Problem Statement

Security and Identity management where mainly neglected in the very beginning. When the Internet became available to the public in the early 90s, people were all free to impersonate whoever a user wanted Between 2002 and 2005, blogging became a widespread instrument, and with it a new mindset appeared: people wanted to stand behind their words Finally, social networks appeared, where it is more and more difficult to hide your own identity. Identity in this case is guaranteed by the people you know, who recognize and certify who you are[111].

There is a lot of research available in literature integrating human identity and blockchain (Mesropyan, 21 Companies Leveraging Blockchain for Identity Management and Authentication, 2017) but there is a lack of solutions offering device identity and blockchain coining IoT, identity management and blockhain together.

3.3 Best Solution

A device with an identity can develop a reputation or history that is tracked by a blockchain. This begins when a certification agency for devices audits the device and registers its identity on the blockchain from birth. As a blockchain is write forward and immutable, blockchain-born devices thus will have irreversible reputations and

identities. Needless to say device reputation could also have interesting applications in machine-to-machine commerce and interaction. Overall, it is strongly believed that device identity represents the foundation that will enable true device security and interoperability[112].

Blockstack: A decentralized internet is one where user donât need to trust any intermediator or third party. On this basis, blockstack was developed. With blockstack, user can control their data and application runs on their devices without any middleware, password, massive data breaches and service tracking around the world.

The main contributions of the blockstack are as follows; The applications on blockstack are server-less and decentralized. Developers start by building a single-page application in Javascript, then, instead of plugging the frontend into a centralized API, they plug into an API run by the user. Developers install a library called 'blockstack.js' and don't have to worry about running servers, maintaining databases, or building out user management systems. (Community, 2016). Blockstack offers decentralized identity, decentralized storage and decentralized payment system to make the blockstack truly decentralized system

1. Decentralized identity: With blockstack, user can own its identity. Digital keys are seamlessly generated and kept on your device. Identity is user-controlled and utilizes the blockchain for secure management of keys, devices and usernames. When user login with apps, they are anonymous by default and use an app-specific key, but their full identity can be revealed and proven at any time. Keys are for signing and encryption and can be changed as devices need to be added or removed[107].

2. Decentralized storage: Data storage is simple and reliable and uses existing cloud infrastructure. Users connect with their Dropbox, Google Drive, etc and data is synced from their local device up to the cloud[107].

3. Decentralized payment: Blockstack uses crypto currencies for simple peer to peer payments. These payments can be charged for buying DNS, for downloading applications and for subscription.

How it operates: Blockstack provides two different options on the screen to install Blockstack. These two options are for 1) user 2) developers. For user, Blockstack allows user to join waitlist. There is a need of email address to join waitlist. For developer, separate facility is provided. Developers are required to install the browser kit before installing the Blockstack. In order to develop application on Blockstack, java scripts code can be written by programmers which executes at client side without involving the servers. This decentralized internet or blockstack is a new internet, second internet or a parallel internet. It offers many facilitates to developers such as developing a new browser or creating decentralized DNS. Furthermore, Blockstack is innovative, having the inclusion capabilities, independent and encounter information security [113].

BLOCKSTACK LAYERS:

Layer 1(Blockchain): The blockchain occupies the lowest tier, and serves two purposes: it stores the sequence of Blockstack operations and it provides consensus in which the operations were written. Blockstack operations are encoded in transactions on the underlying blockchain. In this layer, blockstack IDs are created.

Blockstack ID is the name identity registered in the .id namespace on Blockstack. Your personal data and storage are built around this ID. Apps that want to access your data will be built around this as well.

Layer 2 (Virtual Chain): Blockstack is designed around a "virtual chain" concept, where nodes only need to reach consensus on the shared "virtual chain" they're interested in. Virtual chains do not interact with one another, and a single blockchain can host many virtual chains. These virtual chains can live in any blockchain for which there exists a driver, and virtual chain clients only need to execute their virtual chain transactions (i.e. Blockstack only processes Blockstack virtual chain transactions).

Above the blockchain is a virtualchain, which defines new operations without requiring changes to the underlying blockchain. Blockstack operations are defined in the virtualchain layer and are encoded in valid blockchain transactions as additional metadata. Blockchain nodes do see the raw transactions, but the logic to process Blockstack operations only exists at the virtualchain level (Ali, Blockstack: A Global Naming and Storage System, 2016).

Layer 3 (Routing): Blockstack separates the task of routing requests (i.e., how to discover data) from the actual storage of data. This avoids the need for the system to adopt any particular storage service from the onset, and instead allows multiple storage providers to coexist, including both commercial cloud storage and peer-to-peer systems [114].

Layer 4 (Storage): The top-most layer is the storage layer, which hosts the actual data values of name-value pairs. All stored data values are signed by the key of the respective owner of a name. By storing data values outside of the blockchain, Blockstack allows values of arbitrary size and allows for a variety of storage backends. Users do not need to trust the storage layer because they can verify the integrity of the data values in the control plane [114].

Operations or functionalities of the Blockstack are; digital keys are assigned to the users that are known to be their identity. By using these digital keys, user can sign in to decentralized application without the need of servers. Blockstack provides the storage systems to the user to control their data. This data is secured by encryption. Bitcoin and other digital currencies are used for payment.

Advantages: Advantages of blockstack are listed down

(a) It is open source application ready to adopt good services or changes.

(b) By using blockstack, developer can build applications to manage everything on the device by owning the device, keys, identity, storage and above all internet.

(c) User can truly own its data by keeping it in the device in encrypted form.

(d) Applications can be downloaded through secure decentralized DNS making it independent from third parties.

(e) The digital keys are generated and saved on the device. This let the users to keep their own identities.

(f) Internet services become more transparent without relying on third parties.

(g) Blockstack is used to empower the user as it is user controlled service.

(h) Blockstack records are extremely hard to tamper with.

This is because the bindings for name ownership (names on Blockstack are owned by public keys) are announced in a proof-of-work blockchain and to change these binding an attacker will need to come up with a blockchain with more proof-of-work than the current Bitcoin blockchain but with a different history.

Use cases: Blockstack can be used by developers in order to develop following applications

- **Community run-voting**: voting system as a public internet by the community can be built instead of single corporation i.e. election commission.
- **Verified document publishing**: Document is uploaded and message is sent to the appropriate parties to sign the document. This document is published once it has been signed.
- **Group funds:** Multiple party accounts are created on blockchain. A document is uploaded in terms of funds. A message is sent to the appropriate parties to deposit the funds and sign the agreement. Any party can submit the proposal in order to withdraw the funds.
- **Decentralized social networks or platform:** User can create channels and specify a list of pointers to storage mirrors. Users can post in channels and can have their content hosted in the mirror of the channel.

Design: The blockstack has three components

- **Virtual Chain:** A blockchain, implemented using virtualchains, is used to bind digital property, like domain names, to public keys. Blockstack's blockchain solves the problem of bootstrapping trust in a decentralized way i.e., a new node on the network can independently verify all data bindings. (Ali, Blockstack: A New Decentralized Internet, 2017)
- **Network design:** Blockstack does not use the typical Distributed Hash Table (DHT) in the DNS. Blockstack use atlas network. (Ali, Blockstack: A New Decentralized Internet, 2017)
- **Storage design:** It is the decentralized storage called Gaia storage used in blockstack which acts like a cloud storage. (Ali, Blockstack: A New Decentralized Internet, 2017) It gives a global index for discovery information The two important features of Gaia storage are
  (a) Cloud based
  (b) decentralized
- textbf Payment design: For creating DNS name on blockstack, user need to buy the bitcoin and these bitcoins are destroyed by sending them to NULL address (e.g. 000000). In return, one name registration is assigned to the user.

11. **Domain name service design**: Blockstack domains are not registered on the traditional DNS run by an organization called ICANN. Instead they're registered on a blockchain in a fully decentralized way. This means that Blockstack domains

are truly owned by their owners and cannot be taken away. All Blockstack domains have public keys by default (public keys are required to own the domains), unlike the traditional DNS where a small fraction of domains get the (optional) public key certificates.

Limits: The scalability issues of blockchain and peer to peer network are described in this section.

1. Blockchain based scalability issues There are three blockchain based scalability issues

i. Blockchain is not a general purpose database meaning some pointers and ownership data needs to be moved out from blockchain.

ii. Blockchain is not a general purpose computer meaning the complexity and logics need to be placed outside the blockchain.

iii. System design is also revolving around the limited scalability of blockchain as laws of physics and distributed systems should be taken into account (Ali, Blockstack: A Global Naming and Storage System, 2016).

2. Peer to peer scalability issues Two important peer to peer scalability issues are

i. Comparable performance of cloud storage is needed.

ii. Data discovery is the key problem to solve (Ali,

Blockstack: A Global Naming and Storage System, 2016).

Technology used:

Languages: Blocstack uses two languages python2 and Node.js for back end servers and JavaScript is used for front end server.

Servers: Two servers are maintained in blockstack. One server is for single page application available on dashboard. It manages the identity and storage. Another server manages the DNS which offers the DNS services such as creating/ using DNS and it allows you to have your DNS resolver on your local system using blockchain [113].

Chapter 4

Evaluation

In Table 1, the comparison of above twenty three companies is provided. The following parameters are taken into consideration. **Companies**: The names of the companies used for comparison are placed under this column.**Technology/language used**: The technology or languages used by the company are highlighted. **Blockchain**: This indicates the use of blockchain technology in a company. The yes indicates the presence of blockchain and no means the absence of the blockchain technology. **License:** It is used to indicate the name of the license; a company is associated with. **Payment**: It represents the payment system used by the company. **Identity**: This depicts the use of identity management and authentication of the user by the company.

Table 1 gives the comparison of all the above companies

Sr. #	Companies	Technology/ Languages	Blockchain	Identity	Payment	License	Smart Contracts
1	2WAY.IO	Identifi	No	Yes	N/A	Open	N/A
2	Atencoin	X11 algorithm	Yes	Yes	Bitcoin	NCA	N/A
3	BlockAuth	OpenID connect	No	Yes	Bitcoin	Open	N/A
4	BlockStack	JavaScript, Phython 2, Nodejs	Yes	Yes	Bitcoin	Open	N/A
5	Bitnation	JavaScript, Go	Yes	Yes	Bitnation Bitcoin Debit card	Open source	N/A
6	Block Verify	QR code	Yes	No	N/A	N/A	N/A
7	Cambridge Blockchain LLC	PDS	Yes	Yes	N/A	N/A	N/A
8	Civic	Chain auth	Yes	Yes	N/A	N/A	Yes
9	Credits	Cryptography and Distributed messaging protocol	Yes	No	N/A	N/A	Yes
10	CredyCo	Trustatom	No	No	N/A	N/A	No
11	Cryptid	Factom	Yes	Yes	N/A	Open source	N/A
12	Evernym	JavaScript, Python, Rust, C++, Java	Yes	Yes	N/A	Open source	N/A
13	ExistanceID	SAFE	Yes	Yes	N/A	N/A	N/A
14	Guardtime's BLT	KSI	Yes	Yes	N/A	N/A	N/A
15	HYPR	FIDO	No	Yes	N/A	N/A	N/A
16	Identifi	JavaScript, CoffeeScript	No	Yes	N/A	Open	N/A
17	OIX	OITF	No	Yes	N/A	Open	N/A
18	OIXnet	OpenID	No	Yes	N/A	Open	N/A
19	KYC-Chain	Oracle	Yes	Yes	N/A	Open	N/A
20	Netki	Python, JavaScript, Java, Shell and C.	Yes	Yes	Bitcoin	Open source	N/A
21	ShoCard	QR code	Yes	Yes	N/A	N/A	N/A
22	UniqueID	IoT, Biometry	Yes	Yes	Bitcoin	Open source	Yes
23	uPort	Ethereum, JSON, IPFS	Yes	Yes	N/A	N/A	Yes

Chapter 5

Summary and Conclusions

The use of a Blockchain to secure the IoT would mean that all devices and users of those devices would use public key cryptography that would substitue default login credentials. Instead, each user would have his own private key that would be essential for communicating with any device and the private key would be known only to the user, and hence not be easily hackable. Also, only the manufacturer will be able to install firmware on a device by signing the digital content using his private key. The device will not run code coming from an unknown source. The identity/public key pairs will be stored on the Blockchain to enable a device to lookup when any login request/ digital content is triggered (as part of a decentralized PKI system based on Blockchain)[114].

Bibliography

[1] A Step-by- Step Guide For Beginners, https://blockgeeks.com/guides/what-is-blockchain-technology/

[2] Know More About Blockchain: Overview, Technology, Application Areas and Usecases,https://letstalkpayments.com/an-overview-of-blockchain-technology/

[3] Deloitte,https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html

[4] Solidity,https://solidity.readthedocs.io/en/develop/

[5] Ethereum, https://www.ethereum.org/

[6] wikipedia,https://en.wikipedia.org/wiki/Ethereum

[7] Datafloq,https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/

[8] Mesropyan, E: LTPs: https://letstalkpayments.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication/

[9] Kokoris-Kogias.: Managing Identities Using Blockchains and CoSi.Germany: HotPETs 2016, july 22.

[10] Samaniego, M.: Blockchain as a Service for IoT.IEEE International Conference on Internet of Things(iThings) and IEEE Green Computing and Communications(GreenCom) and IEEE Cyber, Physical and Social Computing(CPSCom) and IEEE Smart Data(SmartData). IEEE, 2016.

[11] Dorri, A.: IEEE PERCOM, 2017.

[12] Svetinovic, D.,Blockchain Engineering for the Internet of Things.IoTPTSâ17. Abu Dhabi.2017

[13] Krishnan, M.A.:(2017). Peer to Peer File Sharing by Blockchain Using IOT.Volume 3, Issue 2

[14] Christidis, K.,Blockchains And Smart Contracts For The Internet Of Things.

[15] Samaniego, M.: Hosting Virtual IoT Resources on Edge-Hosts with Blockchain.,2016.

[16] Yu Zhang, J.W:,An IoT Electric Business Model Based on the Protocol of Bitcoin. 18th International Conference on Intelligence in Next Generation Networks,2015 and Storage System.USENIX ATC-16,2016.

[17] Nguyen, Q.K: BlockchainâA Financial Technology For Future Sustainable Development. 3rd International Conference on Green Technology and Sustainable Development,2016.

[18] Lindman, J.:. Opportunities and risks of Blockchain Technologies in paymentsâ a research agenda.Proceedings of the 50th Hawaii International Conference on System Sciences.,2016.

[19] white paper, https://docs.google.com/document/d/16HDB9AABa5rTOVFJj_8VLdOxgMguovLLAMviaTkZ1q4/edit., 2014

[20] Mettler, M.:Blockchain Technology in Healthcare The Revolution Starts Here. 18thInternational Conference on e-Health Networking, Applications and Services(Healthcom) ,2016.

[21] Leiding, B.:,Self-Managed And Blockchain-Based Vehicular Ad-Hoc Networks.Ubicomp/Iswc 16 , (pp. 137-140). Germany

[22] Pastoor, T. http://2way.io/introducing-2way-io/

[23] Brave New Coin, https://bravenewcoin.com/news/hackcoin-a-digital-currency-and-blockchai-hackathon.

[24] Pastoor, T interviewed by M.Roy,2015, December 14.

[25] Youtube,https://www.youtube.com/watch?v=5lE0hMRi2LU

[26] Atencoin, http://atencoin.com/

[27] Brown, A ,Whitepaper, https://github.com/TechEndeavors/BlockAuth.com/blob/mater/Whitepaper.md

[28] Brown, A,deftnerd, https://deftnerd.com/

[29] OpenID., http://openid.net/connect/faq/

[30] LinkedIn:, https://www.linkedin.com/company-beta/3779680/,2014

[31] Johnston, D.A.: https://medium.com/@DJohnstonEC/informational-report-on-block-auth-f6496a51b97d

[32] Github, https://github.com/TechEndeavors/BlockAuth.com/blob/master/Technology%20Platform.md

[33] Tempelhof, S.T, White paper. 2016

[34] wikipedia, https://en.wikipedia.org/wiki/Bitnation., 2017.

[35] Github, https://github.com/Bit-Nation/BITNATION-Constitution.

[36] Tempelhof, S.T: Pangea Jurisdiction. 2017.

[37] blockverify, https://gust.com/companies/blockverify.

[38] Hulseapple, C.: https://cointelegraph.com/news/block-verify-uses-blockchains-to-end-counterfeiting-and-make-world-more-honest

[39] BLOCKVERIFY, http://www.blockverify.io/.

[40] Thomson, A.Using The Blockchain To Fight Crime And Save Lives, https://techcrunch.com/2015/09/27/using-the-blockchain-to-the-fight-crime-and-save-lives

[41] BUNTINX, J.,http://bitcoinist.com/block-verif-turns-bitcoin-life-saving-technology/

[42] Allison, I,blockverify, http://www.ibtimes.co.uk/bitnation-slock-it-blockverify-taking-part-lightning-blockchainpitchoff-1551262

[43] Traderman.: Titel,White paper https://themerkle.com/block-verify-a-blockchain-based-counterfeit-solution/

[44] Crunchbase, https://www.crunchbase.com/organization/netki-inc#/entity

[45] Cambridge Blockchain, http://cambridge-blockchain.com/,2015

[46] Oberhauser, A.: https://www.f6s.com/cambridgeblockchain, 2017.

[47] HAWKINS, F.: https://www.eema.org/luxtrust-cambridge-blockchain-announce-privacy-protecting-identity-platform/

[48] Alpha,blockchain, http://cambridge-blockchain.com/alpha_genesis_block.html, 2015, Sepetember 10.

[49] Higgins, S.:Coindesk, https://www.coindesk.com/identity-startup-cambridge-blockchain-finishes-2-million-fundraise

[50] Commons, M.,Startup Pitch: Solving Identity Verification with Blockchain..

[51] Handova, D.: B2B Solution of the Week: How blockchain technologies will affect B2B industries.Retrieved, https://www.b2bnn.com/2016/01/b2b-solution-of-the-week-how-blockchain-technologies-will-affect-b2b-industries/

[52] DinarVets: coorslite, http://dinarvets.com/forums/index.php?/topic/239875-civic/

[53] Rizzo, P.:Coindesk, https://www.coindesk.com/shocards-quest-secure-identity-blockchain/

[54] Rizzo, P: Coindesk, https://www.coindesk.com/anonymous-login-civic-goes-live-with-blockchain-authentication-service

[55] Leung, M.:Blockchain Smart Contracts Startup Trustatom Raises Seed From Cartmell, Lingham: http://allcoinsnews.com/2015/01/21/blockchain-smart-contracts-startup-trustatom-raises-seed-from-cartmell-lingham

[56] Perez, S.:techcrunch, https://techcrunch.com/2016/07/19/civic-launches-a-free-service-that-aims-to-stop-identity-theft-before-it-happens

[57] Credits., fromhttp://credits.readthedocs.io/en/latest/blockchain_details.html.

[58] Leung, M.:Blockchain Smart Contracts Startup Trustatom Raises Seed From Cartmell, Lingham, http://allcoinsnews.com/2015/01/21/blockchain-smart-contracts-startup-trustatom-raises-seed-from-cartmell-lingham

[59] Parker, L.: https://bravenewcoin.com/news/cryptid-open-source-identification-system-uses-the-blockchain-to-revolutionize-id

[60] Cryptid, http://www.cryptid.xyz

[61] Ambrosi, C: One world identity. Retrieved from Blockchain Identity Startup ExistenceID Announces Launch, https://oneworldidentity.com/2017/02/07/existenceid-launch/,2017, February 07.

[62] LinkedIn, https://www.linkedin.com/company/existence-id

[63] The Paypers, https://www.thepaypers.com/cryptocurrencies-bitcoin-virtual-currencies/existenceid-rolls-out-digital-identity-projects-using-blockchain/767859-39

[64] Greene, T.:New protocol from Guardtime hopes to unseat RSA for authentication,digital signatures.Retrieved from Network World, https://www.networkworld.com/article/2925215/security0/new-protocol-from-guardtime-hopes-to-unseat-rsa-for-authentication-digital-signatures.html

[65] Preimesberger, C.: http://www.eweek.com/security/why-guardtime-believes-it-will-replace-rsa-security-standard May 26.

[66] HYPR, https://www.hypr.com/

[67] GitHub., https://github.com/identifi/identifi

[68] Open Identity Exchange., http://www.openidentityexchange.org/about/

[69] KYC CHAIN, https://kyc-chain.com/ January 21.

[70] flagtheory, https://flagtheory.com/kyc-chain/

[71] Crunchbase, https://www.crunchbase.com/organization/cambridge-blockchain#/entity

[72] Azaria A, https://azure.microsoft.com/en-us/blog/azure-blockchain-as-a-service-update-4/, 2016.

[73] Torpey, K.:Bitcoin, Verlag, https://bitcoinmagazine.com/articles/netki-wants-replace-bitcoin-addresses-wallet-names-1429736009/,2015, April 22.

[74] Parker, L. :Netki launches Digital ID solution, which Bitt is using with Central Banks in the Caribbean.Retrieved, https://bravenewcoin.com/news/netki-launches-digital-id-solution-which-bitt-is-using-with-central-banks-in-the-caribbean

[75] Netki, https://netki.com/

[76] Dillet, R.: ShoCard Is A Digital Identity Card On The Blockchain.Retrieved, https://techcrunch.com/2015/05/05/shocard-is-a-digital-identity-card-on-the-blockchain/,2015, May 5.

[77] :ShoCard., https://shocard.com/

[78] UniqueID, http://uniquid.com/

[79] Sean.: https://decentralize.today/dont-forget-what-self-sovereign-identity-system-uport-doesn-t-claim-to-do-1f43ca228575

[80] Quentson, A.: Uport, An Ethereum Based Identity Project Wins the Blockchain Competition, https://www.cryptocoinsnews.com/ethereum-based

[81] Community, B.: https://blockstack.org/faq., 2016.

[82] Bitnation, http://bitnation.com/.

[83] white paper, https://www.cognizant.com/whitepapers/how-blockchain-can-help-retailers-fight-fraud-boost-marginsand-build-brands-codex2361.pdf

[84] Angle.co,Titel, https://angel.co/block-verify.,

[85] Bloomberg, https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=371771173.

[86] Bobthetoad, https://en.wikipedia.org/wiki/Blockstack., 2017.

[87] Brown, A, Titel, Verlag, http://..., Datum.

[88] Autoren: deftnerd, https://btcjam.com/listings/12504, 2014.

[89] Civic, https://www.civic.com/how-it-works

[90] CIVIC, https://www.civic.com/, 2017.

[91] Cryptid, http://cryptid.xyz/

[92] DeftNerd:Industry Opportunities.https://github.com/TechEndeavors/BlockAuth.com/blob/master/Industry%20Opportunities.md

[93] evernym, https://www.evernym.com,

[94] ExistenceID, http://www.existenceid.com/

[95] guardtime, https://guardtime.com/technology/blt-technology

[96] guardtime, https://guardtime.com

[97] https://en.wikipedia.org/wiki/Blockstack.

[98] Identifi, https://identi.fi/,

[99] Keyless Signature Infrastructure., https://guardtime.com/library

[100] Know more about blockchain: Overview, Technology, Application Areas and use cases, https://letstalkpayments.com/an-overview-of-blockchain-technology

[101] Lingham, V.: Civic: Enabling the future of privacy digital security with ChainAuth., Verlag, https://vinnylingham.com/civic-enablin-the-future-of-privacy-digital-security-with-chainauth-b79d61904d4c

[102] Lujan, S.: Linghamâs Civic to Protect ID Information by Leveraging Bitcoinâs Blockchain:, https://news.bitcoin.com/civic-prtects-id-information-by-leveraging-bitcoins-blockchain/, 2017, April 17.

[103] Masley, S.: https://devpost.com/software/cryptid

[104] Nelson, M.A.: Blockstack: A Global Naming

[105] OIX, http://www.openidentityexchange.org/blog/2015/04/22/oixnet/

[106] OIXnet., http://www.openidentityexchange.org/oixnet-registry/

[107] Uport, http://www.uport.me

[108] ,Weinswig D: Blockchain in Logistics and identity-project- uport-wins- the-blockchain- competition/, 2016. Publishing:,2017

[109] Ali,M blackstack,2017. https://blockstack.org/faq.,

[110] Amit, https://letstalkpayments.com/12-companies-leveraging-blockchain-for-identification-and-authentication

[111] blockstack, https://blockstack.org.

[112] Shae, R.:Innovation amp;amp; Inclusion w/Decentralized Apps., 2016.

[113] Shae, R.: The Decentralized Internet with Blockstack., 2017.

[114] Monitor Deloitte, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/TMT-Cyber-Security-Blockchain-March-2017-en-final.pdf

Abbreviations

DNS	Domain Name Service
AML	Anti Money Laundering
KYC	Know Your Customer
IoT	Internet og Things
WCN	World Crypto News
NAP	Non Aggression Principle
FDA	Food and Drug Administration
CEO	Chief Executive Officer

List of Figures