Decentralized Transaction Mechanism based on Smart Contracts

RISHABH GARG

3rd International Conference on Blockchain and IoT | Sydney Aus.

3rd International Conference on Blockchain and Internet of Things | Sydney, Australia - 26-27 March 2022
Date of Submission: 30-07-2021 Date of Acceptance: 14-09-2021

DECENTRALIZED TRANSACTION MECHANISM BASED ON SMART CONTRACTS

Rishabh Garg

Department of Electrical & Electronics Engineering,
Birla Institute of Technology & Science, K.K. Birla Goa Campus, Sancoale, Goa - 403726
rishabhgargdps@gmail.com

ABSTRACT

Blockchain comes with a possibility to oust the outdated identity system and eliminate the intermediaries. The identity management, through blockchain, can allow individuals to have ownership of their identity by creating a global ID to serve multiple purposes. For user security and ledger consistency, asymmetric cryptography and distributed consensus algorithms can be employed. The blockchain technology, by virtue of its key features like decentralization, persistency, anonymity and auditability, would save the cost and increase the efficiency. Further, the digital identity platform would benefit citizens by allowing them to save time when accessing or providing their personal data and records. Instead of being required to show up to services in-person to produce a physical form of ID, users could be provided with a digital ID through a personal device, like smartphone, that can be shared with services conveniently and securely through a DLT.

KEYWORDS

Blockchain, Decentralized Apps, Data Portability, Decentralized Public Key Infrastructure (DPKI), DID, Ethereum, Hash, IAM framework, Identity Management System (IMS), IPFS, Private Key, Public Key, Revocation, SSI, Storage Variables, Validation, Zero Knowledge Proof.

1. INTRODUCTION

All over the World, residents have several forms of identity documents, for different purposes, such as Voter Card for election purpose, a driver's license on road, a passport for travelling abroad, or a social security number to record the covered wages or self-employment earnings. One country that has toiled hard to provide an official identity to all its citizens is India. The idea of a Universal Identity cropped-up in 2006, with a primary objective to provide a biometrics enabled unique number to every resident of India. The flagship project of UIDAI (Unique Identification Authority of India), prevalently known as Aadhaar, proves to be world's largest National Identity Project, which collects biometric and demographic data of residents and store them in a centralized electronic repository.

Till date, 1.29 billion users have been enrolled in the system, with a total expenditure of Rs. 12.96 crores, over the last 12 years [1], [2]. This system of identification, with a centralized biometric database, was expected to brace the identity and access management in India, but the ground reality is far from such claims. Such a silo-based approach has resulted in perpetration of fake identities that has further aggravated the magnitude of the problem.

2. PROBLEMS WITH EXISTING ID MANAGEMENT SYSTEM

The current Identity Management System is full of flaws. There are endless numbers of identities and to fetch those documents, one comes across long queues, lengthy procedures, bulk formalities, intervention of proxies and agents. Over and above, verification of these documents, at each level, is another dreary exercise. Even, during online process, every App generates or asks for a new ID and password [3]. There are a number of the challenges, like:

1.1 Lack of Compatibility

The Apps, on which a typical ID management systems works, do not get updated on regular basis. They do not comply with security measures.

1.2 Identity theft

According to the Breach Level Index, 4.8 million records are stolen every day. It happens because people often share their personal information to unknown sources, for availing online services. Such online information fall prey to hackers, as they are stored in a central server.

1.3 Weak Authentication Protocols

The existing authentication process involves three stakeholders: i) verifying /KYC companies; ii) users; and iii) the third-party that need to check the identity of the user.

Since KYC companies have to cater to the requirements of banks, healthcare providers, immigration officials, and so on, they require more resources to fasten up their tasks. Consequently, they extract a big amount from the individuals as hidden processing fee. Despite the fact that the process gets expedited, the third-party companies are kept waiting for a long time to onboard the customers.

1.4 Lack of Control

At present, the users do not have any control over the personally identifiable information (PII). Without being aware of the fact that how many times their data has been shared or where has it been stored, the users are making compromise with their own privacy.

Thus, it emerges as a fact that identities must be portable and verifiable anywhere, any time. At the same time, they need to be private and secure. So that, they would overcome the lapses of current identity management systems:

- There should be a proper interoperation network between the government and the complex bureaucratic setup to curtail processing time and cost.
- Education structure should be systematized and equipped with a robust authentication and verification process.
- The functionaries in health care zones - hospitals, clinics, doctors, pharmacies and insurance, must be intertwined properly, on operational front, to offer prompt and efficient healthcare facilities for patients.
- Banking must be made secure and more user friendly by avoiding the repeated ‘sign-in and sign-out’ exercise to make access to their bank accounts, for every transaction.

2. PROPOSED GATEWAY

In order to have safe, secure and private digital identity, one technology that has risen to the top of the list, is the blockchain. Distributed ledger technologies (DLT), blockchain being the most well-known example, ensure that information is never held at single repository; rather it’s securely managed in decentralized databases. It eliminates the intermediaries and lack of control. It will allow individuals to enjoy ownership of their identity by creating a global ID to serve multiple purposes.

2.1 Identity Models

Since the advent of the Internet, the models for online identity have advanced through four broad stages:

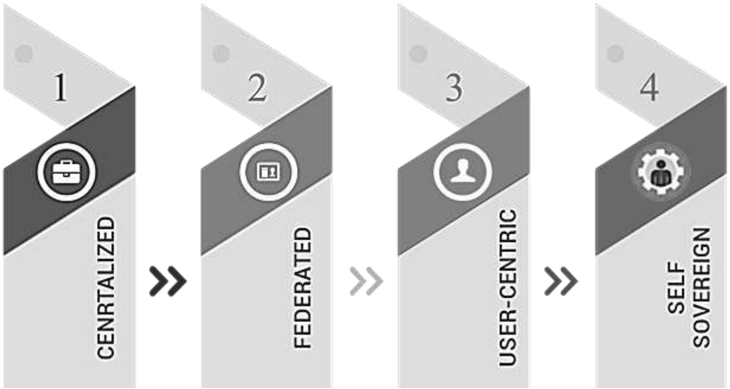


Fig - 1: Decentralized Models of Online Identity

2.1.1 - Centralized Identity

The first model of digital identity management is extensively being used worldwide. It is controlled by a single authority. Each organization issues a digital identity credential to a user to allow him to access its services. Each user needs a new digital identity credential for every new organization he engages with. UID (Aadhaar) is an eloquent testimony to this prototype.

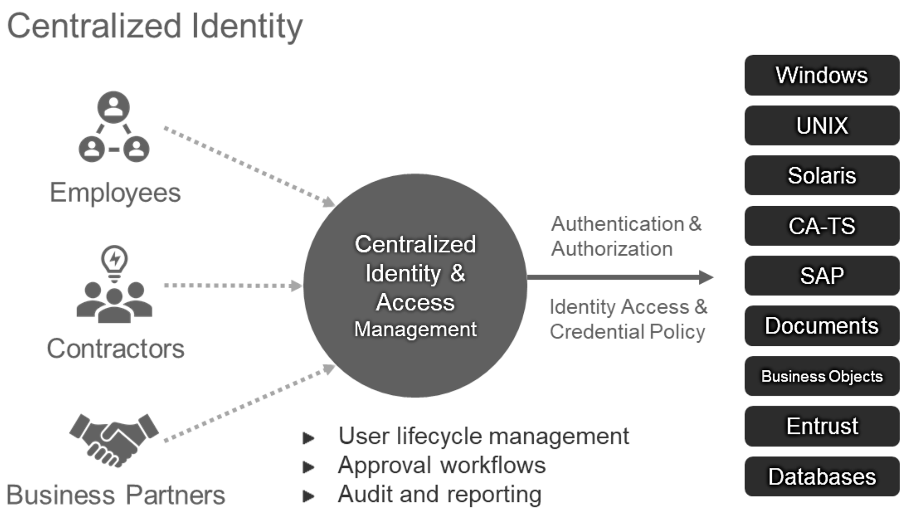


Fig - 2: Centralized Identity

2.1.2 - Federated Identity

Federated identity permits users to wander from site to site under the system. However, each individual site remains an authority. Microsoft's Passport (1999) was the first to imagine federated identity, which allowed users to utilize the same identity on multiple sites.

2.1.3 - User-centric Identity

It is controlled by an individual, across multiple authorities, without requiring a federation. This identity model is based on the assumption that every individual have the right to control his or her own online identity. A user can theoretically register his own Open ID, which he can use independently.

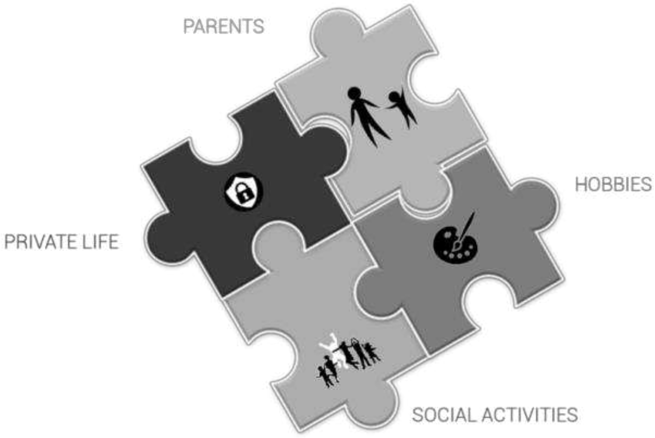


Fig - 3: User-centric Identity

2.1.4 - Self-Sovereign Identity

Self-Sovereign Identity confers full right and control of identity, to the users, across multiple authorities, and therefore, it suits best to the contemporary needs of identification and access management. This evades the honeypot problem too. Since the credentials are usually stored directly on the user's device or distributed data storage systems like Inter Planetary File System (IPFS), decentralized structures renders zero possibility of unauthorized data access.

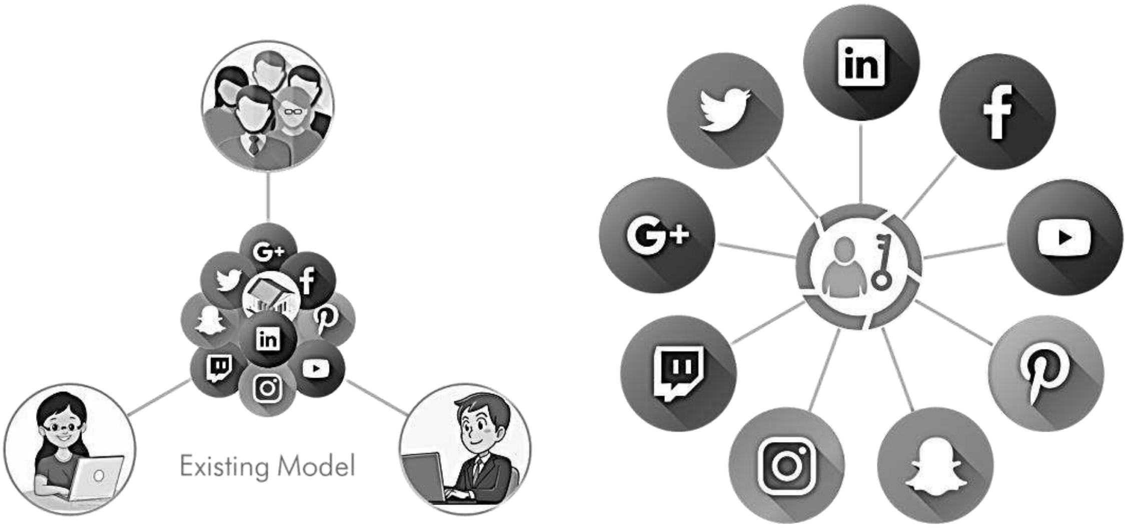


Fig - 4: Comparison between the Existing Model and the Proposed Model

2.2. Suggested Platform

Since Ethereum is too heavy to store big data objects like images, videos; hence, a cloud storage like IPFS can be used. IPFS (Inter Planetary File System) is a decentralized storage solution for blockchain-based content.

2.2.1 Inter Planetary File System (IPFS)

IPFS uses a P2P (Peer-to-Peer) network model for file sharing that is decentralized and distributed across many computers or nodes. Files are broken down into different parts and stored across a network of nodes that track the file by hashes. When the parts are assembled together, based on their hash value, it recreates the original file. The use of Distributed Hash Tables (DHT) for file system storage and retrieval is the core innovation for IPFS. It is similar to the BitTorrent protocol, but different in the way they point to the file for sharing. This stores files on a blockchain as key value pairs. The data is broken up into 256 KB chunks and spread across a network of nodes or computers. It is efficiently coordinated to enable efficient access and lookup between nodes. BitTorrent does not use a blockchain, but rely on torrents instead of pointing to files. You can have different torrents pointing to the same file, but in IPFS you only need one hash ID that points to a file.

Files are not posted to IPFS in the same way as posting a file to the cloud. IPFS uses secure hash of the file contents for the location identification and Distributed Hash Table (DHT) for location resolution. This is done as the resource or object is not available on a server but on a decentralized platform. When someone requests data, the data is represented directly by its hash ID and not the actual file itself. IPFS thus provides an abstraction to the actual location of the file, so the actual physical location does not matter to the application. This abstraction removes the complexity for application developers.

IPFS is different from location based storage system, viz. the conventional HTTP family of protocols or the centralized namespace. When a storage system is based on location, it tracks a host by a logical addressing scheme (e.g. IP address) mapped to a user friendly name. If the host changes its name or address, it must also be modified in the name service table.

Content-based addressing storage requires a content identifier that determines the physical location of a file. In this case, the data is accessed on the basis of its cryptographic hash rather than logical address, almost like a digital fingerprint of a file. The network always return the same content based on that hash regardless of who uploaded the file, where and when it was uploaded.

2.2.2 IPFS commands

```
cd go-ipfs
./install.sh
/ipfs init
ipfs cat <readme file>
cat <filename>
ipfs add <filename>
```

When it comes to speed and reliability, IPFS perform better than HTTP. Instead of depending on a server location to fetch a file, a content addressed storage system may provide the file from any server, whichever is the nearest to the user. It implies that a user can simply search for a file without a search engine to refer the location i.e. the server name or address. Rather, he may reference it by the file's hash, which will be available from the nearest available nodes (a peer or node) on the IPFS network.

IPFS

```
//using the infura.io node, otherwise ipfs requires you to run a daemon on your own computer/server. See IPFS.io docs
const IPFS = require('ipfs-api');
const ipfs = new IPFS({ host: 'ipfs.infura.io', port: 5001, protocol: 'https' });
//run with local daemon
// const ipfsApi = require('ipfs-api');
// const ipfs = new ipfsApi('localhost', '5001', {protocol: 'http'});
export default ipfs;
```

3. Anticipated Identity Management

In order to avail any facility or service, the identity of a person needs to undergo a two-step method: authentication and verification process. To prove that the identity belongs to the same person who has approached the authority, his name and identifying documents are checked by the authentication process. To know, whether the documents indicating name, address or passport number, submitted by the person are correct or not, there is a process of verification. That means that a verifying entity confirms that the data, which is claimed by the individual as his own is genuine or not. This is usually done through the verification of identifying documents.

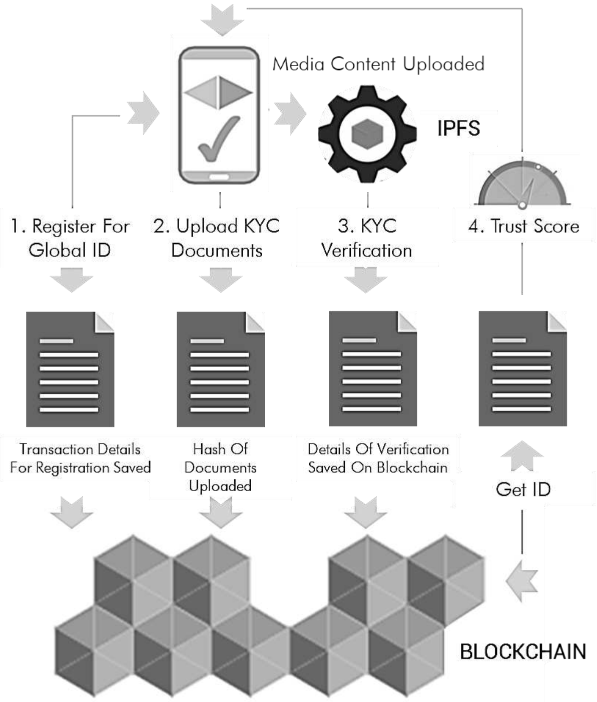

Media Content Uploaded
IPFS
1. Register For Global ID
2. Upload KYC Documents
3. KYC Verification
4. Trust Score
Transaction Details For Registration Saved
Hash Of Documents Uploaded
Details Of Verification Saved On Blockchain
Get ID
BLOCKCHAIN

Fig. 5: Identity and Access Management through Blockchain

In distributed ledgers, each entity of the block in the network, has same source of truth, about the validity of credentials, and the information about the attesting authority also, without the obligation of holding or revealing all his actual details.

Leveraging blockchain technology for Identity and Access Management, three different performers - identity owners, identity issuers and identity verifiers, play their characters. The identity issuer is a reliable authority such as a government body that has the right to issue personal credentials for an identity owner (the user). It acts as an attestation authority that stamps the validity of the personal data (e.g. last name and date of birth) by issuing a credential. The identity owner, as a rule, store these credentials in their PI wallet and utilize this to prove his identity to the third party on demand. The third party or the verifier determines the validity of proof through the legitimacy of attestation and the reliability of attesting party. It does not probe into the validity of the actual data provided in the proof.

3.1 Data Portability

Decentralized structure would slash down the need of re-verification of identity across various services and platforms. With DIDs and verifiable credentials, it is likely to transfer identities that were anchored on one target system to another with ease. Data portability reduces inordinate friction for the user, while making the sign-up process simple and user-friendly.

It would also empower user to re-verify himself to meet the regulatory KYC (Know Your Customer) requirements. This will skip the cumbersome identity verification process, where a series of documents are required and checked, and this would successively curtail customer's time onboard, avoid drop-out rates and reduce cost in the financial sector.

3.2 Right and Control

In centralized identity systems, the authority issuing the identity is usually responsible for data protection. However, in decentralized framework, security becomes the onus of the user, who may determine his or her own security measures or outsource the task to a service provider agency, a service app or a digital bank vault.

3.3 Revocation

Revocation means withdrawal, annulment or revision of a credential. The possibility for an issuer to revoke a credential is crucial to an identity infrastructure for the very reason that identities are dynamic. Whenever attributes change, a new credential needs to be issued and the old one needs to be declared void. The registry contains the status of each credential, whether it has been revoked (deleted or updated) or it is still valid.

3.4 Prevention of Identity theft

In Blockchain identity management, each user can store his identity credentials on a digital identity wallet on a device, like his smartphone. Digital Identity credentials are only valid if used from a device, which is authorized to do so. If the device is lost, the user can use another authorized device, may be his laptop, to write on the blockchain that his cell-phone's authorization is now revoked.

This would take instant effect and stop anyone from using the digital identity credentials on the cell-phone. The burglar would not be able to impersonate the user even though he has his passwords, biometrics or the device because the immutable and secure chain (blockchain) would now hold a revocation registry for the phone. Thus, the thief will not be able to create new relationships.

In the next step, the existing relationship keys (pairwise connections, where each of them has a unique key) are to be revoked. This prevents the thief to explore the existing relationships between the device and other people or organizations.

Conventional ID Management	**Comparative characters**	**Blockchain ID Management**
Honeypots - treasure of information is likely to be attacked by hackers	Network	Provides anonymity & privacy through permissioned blockchain network
Users use the same password for different sites. If one password is stolen, all apps will be compromised with.	Password Protection	Encrypted public key creates a secure digital reference about the identity of the user (a secured alternative to password)
The use of cloud computing for various purposes has led to the challenge of tracking usage of resources across environments.	Cloud Applications	May augment existing single sign on solutions or be designed to track activity across platforms.
Multifactor authentication acts as a challenge to manage due to the infrastructure requirements to support it.	Authentication Protocol	Blockchain technology can enable MFA without the need for additional infrastructure
Introduces a challenge of having a single source of truth, which makes audits difficult to conduct.	Source of Truth	Transactions are immutable by nature, they can be used to both store and retrieve data that needs to be regulated by various compliance standards.

Table - 1: Benefits of Blockchain Identity over Conventional ID System

Blockchain technology, through smart contracts, establishes trust between the parties and guarantees the authenticity of the data and attestations, without actually storing any personal data on the blockchain. Further, the transactions once packed into the blockchain, cannot be tampered. Therefore, it has transformative potential in various fields like financial services [4], online payments [5], public services [6], Internet of Things (IoT) [7], reputation systems [8] and security services [9].

4. IDENTITY BASED APPLICATIONS

4.1 Crowd Operations (Voting)

Decentralized Applications can implement Ethereum Smart Contracts to automate processes involving crowd operations. Application Programming Interface or APIs can be used to publish a set of methods and functions to access the data, programmatically invoke operations and store the data. In this case, APIs can help expose a set of services of the DApp.

Categories of APIs in blockchain

1. Management APIs - e.g. admin, miner, personal, txpool
2. Web3 APIs - e.g. web3, eth, net

   admin.addPeer(): Here admin is the API and addPeer() is the method/function of the API.
   debug.dumpBlock(): This can display the block header details of the block number 16.

These APIs can be used to encode the specific operations for common users using the DApp as buttons for intuitive interface and abstraction.

4.2 Prediction Markets

A Prediction Market implies betting on outcomes that can be accessed by the smart contracts. It comprises - Market creator, who posts a market event on the platform; Market reporters, who speculate on the outcome of the event; and Market participants, who can use their tokens/cryptocurrency for stake. If the predicted outcome is correct/wrong, participants win/lose rewards. The tokens used are called Reputation Tokens (REP tokens) and are used for staking purpose in case of dispute while the trading currency is Ether. The end-to-end marketplace of stocks, futures, products, ideas etc. is facilitated by Smart contracts.

4.3 Distributed Resources and IoT

It operates on the idea of Distributed Energy Resources (DERs) and works on the Energy retail phase (out of Energy production, Transmission, Distribution, Retail) of the Electricity supply chain. It is a Permissioned Blockchain DApp implemented on the Ethereum smart contracts layer. It aims to move energy transfer and payment transactions through crypto tokens on the blockchain architecture. Market participants, other than electricity companies, own power plants and transmission lines. Companies sell electricity to these participants who in turn supply electricity to the end users.

Grid+ uses Smart Agent (a computing device) that hosts software for blockchain transaction, multisig crypto-wallet with PKI security. Intelligent electricity usage is done by coding efficient price options using smart contract. Integration with IoT devices further strengthen the process. ERC20 (fungible) tokens called BOLT are used for payment. For signing a transaction, two out of the MS1, MS2, MS3 signatures are required (MS2, MS3 are used for smart agent controlling). Smart agent escrow is used for holding the tokens with some security deposit (in case of extra electricity usage).

5. PROPOSED WORKING MECHANISM

Blockchain, by involving a few technical components, namely - native Android or iOS App for individuals & verification entities; IPFS to store user's PII; micro-services program using NodeJS; and public blockchain component, can allow people to create self-sovereign and encrypted digital identities, replacing the need for creating multiple usernames and passwords. In order to do so, an account address shall be generated using a unique private key. The private key can be an alpha-numeric password, appended to a random number employing mathematical algorithm. Biometrics cannot be used for generating private keys as the fingerprints and retinal blood vessels are subject to change with time.

5.1 Installation of Software

An individual will have to download the mobile app from play store or app store. After downloading the app in mobile phones, a user will create a profile on the app. Once the profile is created, the user will get the unique ID number from UDI authority which will help organizations to send or to get the access to user's identification documents.

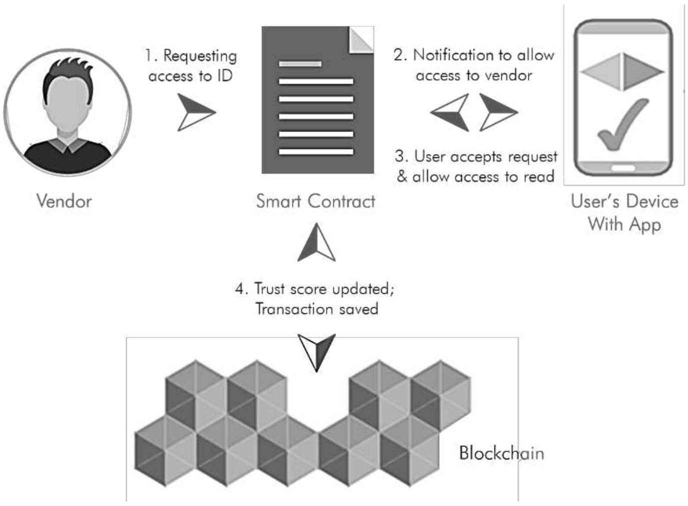
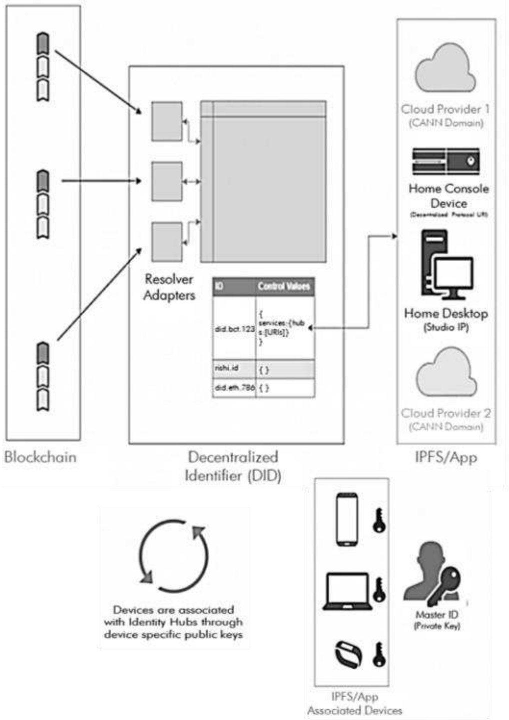

1. Requesting access to ID
2. Notification to allow access to vendor
3. User accepts request & allow access to read
Vendor
Smart Contract
User's Device With App
4. Trust score updated; Transaction saved
Blockchain

Fig. 6: Identity Access through Blockchain

5.2 Procurement of Documents

On having the unique ID number, the user needs to fetch the government issued IDs through the app which will be saved in the IPFS having hashed addresses stored in the blockchain. The app will extract the personal information from these ID's; so that user can do self-certification of his details.


Resolver Adapters
Cloud Provider 1 (CANN Domain)
Home Console Device (Decentralized Protocol URI)
Home Desktop (Studio IP)
Cloud Provider 2 (CANN Domain)
Blockchain
Decentralized Identifier (DID)
IPFS/App
Devices are associated with Identity Hubs through device specific public keys
Master ID (Private Key)
IPFS/App Associated Devices

ID	Control Values
did.bct.123	{ services:{hubs:[URIs]} }
rishi.id	{ }
did.eth.786	{ }

Fig. 7: Schematic diagram of Distributed Ledger Technology to record citizen data.

The users will now have the ownership of their own data. It would help users to decide what information is to be shared with organizations. In order to share the specific details or required information, he will encrypt the information (hash of the credentials, in this case) and share the relevant public key to whom so ever it may concern (the government organization / service provider or verifier) for decryption. Without the user's consents, no information can be shared with any identity seekers.

In case of a new born baby, the Registrar, Births & Deaths would record the birth details and provide a 16-digit unique digital identification number (UDI). The Family details viz. name of the child, date of birth, place, parents' name, address, caste, and so on; together with Biometric Information (DNA Map, Finger Impressions, Retinal image, Blood Group etc. as per feasibility) of the child shall be uploaded through authorized service providing agency (in case of new born babies) or may be fetched from UDI database (in case of existing citizens) and saved on IPFS. The biometric details would be updated after every five years till the child attains 15.

Now, wherever the user moves, may it be to school, medical centre, job or market, this 16-digit ID number would serve as his roll number, enrolment number, registration number, bank account number, driving license number, vehicle registration number, mobile number, LPG gas number ……….. No additional number would be required for any purpose [10]. Even if the 16-digit ID becomes public, it cannot fetch the documents / information from the App unless gets access to the password. Further, the hacker cannot generate the private key from the passcode as the former contains a random number auto-generated by the system

To share specific credentials, two approaches can be adopted: i) One can send the respective hashes of all the credentials to the receiver or ii) He can compile the credentials into an object on the IPFS and send the root hash of the object. The root hash is generated by hashing the object entities by Merkle tree hash method.

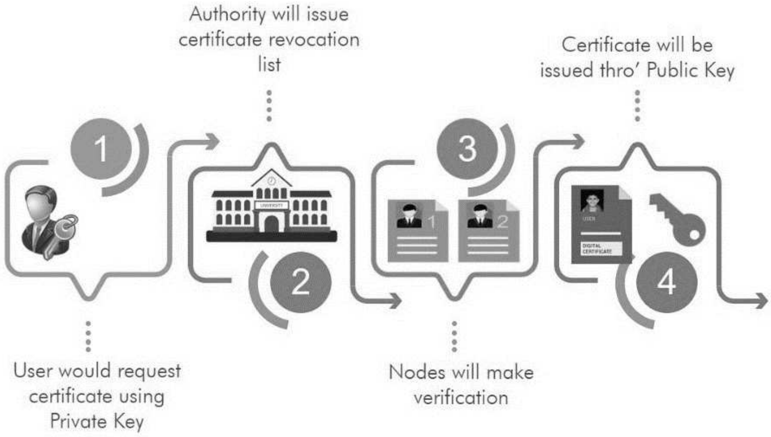

Authority will issue certificate revocation list
Certificate will be issued thro' Public Key
1
3
2
4
User would request certificate using Private Key
Nodes will make verification

Fig. 8: Endorsement of Documents on User's Profile

For example, if a child takes admission into a school, the parents (on behalf of the child) would share child's public key along with the hashes of the respective credentials, with the school administration to allow access to the relevant details (name, father's name, mother's name, date of birth, nationality …. duly encrypted). The school will write all accomplishments, viz. participations, scholastic grades, add-ons, extra-curricular attainments, sports, etc. of the candidate on the same IPFS [11].

On seeking transfer from one institution to another, the previous school would generate a transfer certificate, through its authority key. An authority key is a private key, specific to an official holding a position as authority which would be different from his individual private key. As soon as the child takes admission into the successive institution, his parents would share his public key, with all pertinent details, and the new school administration will start writing on his

IPFS. The school will write a revocation registry which will prevent the student from taking admission in two institutions at a time.

During periodical Census, the government can issue a notification to all citizens of the country to share their hashed data (encrypted with their private key), comprising most pertinent information such as name, parent's name, address, date of birth, educational qualifications with a public key to decrypt the same. The government should avoid gathering redundant information which may serve as honey-pot for hackers.

On attaining maturity, as per census records, the individual would automatically get the right to vote. Evidently, he would not require any separate EPIC [12]. Since the blockchain would verify the electoral rights of those who have attained 18 on day-to-day basis, no extra procedure would be required. On the day of polling, any citizen, who has attained 18, can make log-in through his password on DApp, anywhere in the world. Once he casts his vote, the account address would be disabled.

For barely a few services like passport, where document may be essential in paper form for visa or immigration procedures, there seems to be no valid argument for having a hard copy. For other services, this will simplify the procurement procedures too. As soon as the document is digitally issued by the authority, it will appear on the IPFS. Since most of the services would be available online; clerks or proxies will get seldom opportunity to make delays or expect bribes.

If one visits a hospital, either as an outdoor patient or gets hospitalized, all chronic and major ailments shall be entered into IPFS so that doctors would be able to study the entire medical history of the patient, if required. This will help the patients to get better treatment [13].

For all financial transactions, your UDI will be linked to only one object. Hence, it would be a matter of seconds to get the details of all deposits and borrowings using the tree root hash. Wherever you go, be it a restaurant, club, shopping mall or fly abroad, UDI linked IPFS object would carry statement of every penny you earn or spend. This would enable honest tax payer to display all his assets & liabilities before the IT authority. Even the IT authorities would have no reason to doubt his integrity. However, dishonest tax payers would have bad days.

In a similar way, documents pertaining to the Property, Occupation, Financial history, Medical records, Health Insurance … can be maintained by creating a Distributed Hash Table on a UDI linked IPFS [14]… and the hashes of same can be encrypted using public key of the user. These encrypted hashes will be operated, accessed or retrieved through a Multipurpose Digital ID card.

One World - One Identity

The Multi-purpose ID would carry user's name, a QR Code, his photograph as depicted in Figure-10.6. The card on insertion into a card reader or a customized machine, shall display the DHT comprising all the encrypted, hashed information of the objects and its sub-objects. The user can make access to the online documents using his private key.

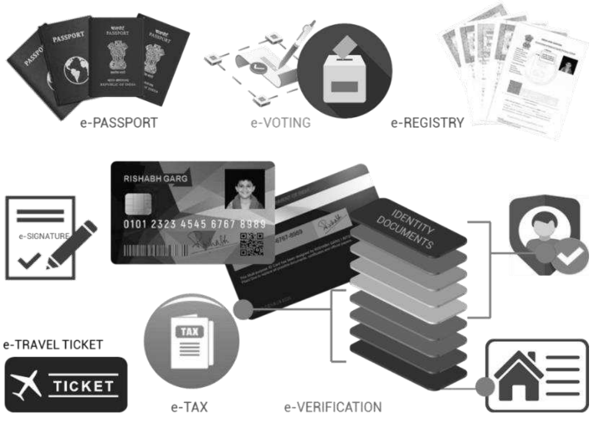


Fig. 9: Digital ID (One Card - Multiple Uses)

If somebody loses his Multi-purpose ID, he can request the appropriate authority to issue a clone. This clone will be a vegetative copy (because no mutation is possible in blockchain) of the original ID. If an offender tries to steal someone's identity, or reap the benefits thereof, he will not be able to do so as the entire information is encrypted through a private key.

On death, the Registrar of Birth & Death shall be informed. He would de-activate the UDI for further use. In such case, only the legal heir shall be entitled to draw claims through nomination or power of attorney.

5.3 Government or Third-party Access

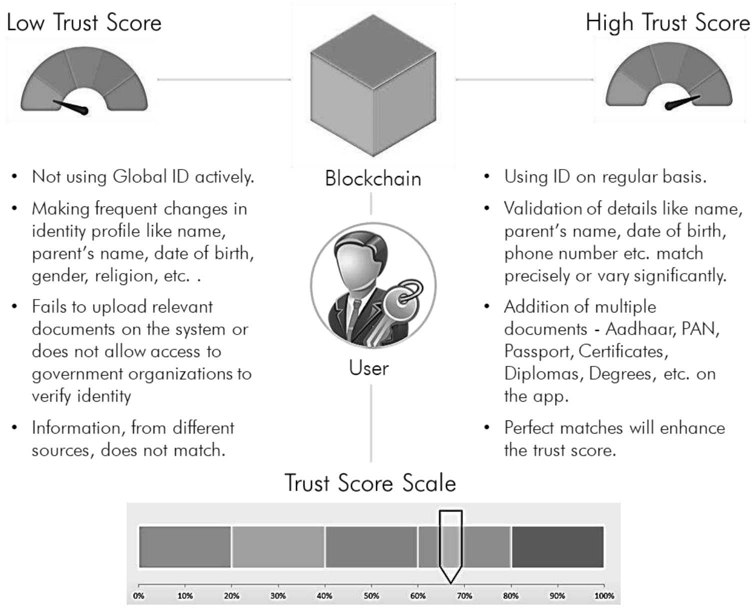
Any time, a government organization or any third party needs to make an access to some specific details of a person for authentication purposes, a notification will be sent to the individuals owning the identity. Once the user allows the third party to access his specific details, the said authority or entity can use the identifiable information only for authentication and the individual will be able to trace the purpose for which his PII has been used.

Blockchain does not store the user's data or information. The information is stored in user's IPFS, and it's the transactions that is made between identity holder and third-party, will only be recorded on the blockchain.

For instance, if a passport authority verifies the person's identity via public key or an app, then that transaction will be added on the blockchain and visible to all the connected nodes. Suppose there is a person named Rishi, who needs to authenticate himself to apply for a visa. Rishi will provide the hash of the object that contains all the required credentials (duly encrypted by Rishi's private key and the authority's public key) to the authorities, enabling them to make access to the information. The authority will decrypt the hash of the object using his authority key and Rishi's public key. Now the verifying authority can check his documents, and the transaction will be recorded on the blockchain. This is how the authorities would be able to validate his identity instantly [15].

5.4: Maintenance of Trust Score

Smart contracts containing the business logic can generate a trust score for a user from the information provided by him for creating a self-sovereign identity. Higher will be the trust score, higher will be the trustworthiness of an individual. This can help organizations validate user's identity on real-time basis.



- Not using Global ID actively.
- Making frequent changes in identity profile like name, parent's name, date of birth, gender, religion, etc. .
- Fails to upload relevant documents on the system or does not allow access to government organizations to verify identity
- Information, from different sources, does not match.

- Using ID on regular basis.
- Validation of details like name, parent's name, date of birth, phone number etc. match precisely or vary significantly.
- Addition of multiple documents - Aadhaar, PAN, Passport, Certificates, Diplomas, Degrees, etc. on the app.
- Perfect matches will enhance the trust score.

Based on a user's trust score, user's integrity can be determined.

Fig. 10: Rise & fall of Trust Score

An initial user may be kept under observation for the first six months; giving him the time to create the trust score. During the period, he may furnish the required information and upload the credentials to establish his identity. A user can achieve a higher trust score by uploading multiple documents on the app/IPFS. The system will verify if the details like name, parent's name, date of birth, etc. match precisely or vary significantly. Perfect matches will enhance the trust score.

On the contrary, if a user fails to upload relevant documents on the system; does not allow access to government organizations to verify identity; or makes frequent changes in his identity profile, particularly with regard to his name, parent's name, date of birth, gender, religion, etc. will drop down his trust score [16]. Based on a user's trust score, it can be determined whether it's a valid account or a suspicious one.

For example, if a Bank needs to check the authenticity of the person for granting him a loan, they can check the user's trust score. It can save time, money and provide an insight to user's credibility [17]. Since the object containing all information or transactions, would be protected by the user's public key, it's only the user, who would be able to make access to the entire information.

In the wake of suspicion or illegitimate activities or suppression of information, a competent authority, duly appointed as per provisions of law, shall ask the user to share the requisite hashed information, duly encrypted, along with the public key of the authority and the private key of the user. If the user fails to share the pertinent information in a specified time period (say 15 days), the system will start dipping the user's trust score @ 20% for every 10 days. As the trust score drops down, the users will find it difficult to make transactions. He'll have no alternative except to share the key. No sooner does he share his public key, the trust score would automatically restore.

6. USER OPTIMIZED FEATURES

The recommended technology has a number of user optimized features:

- A blockchain identity management system does not store any user's data rather it uses Smart contracts to share the personal information, and hence data manipulation is not possible on the blockchain. No transaction of user's information can occur without the explicit consent of the user that adds security to identity management.
- No personal identity document of the users is stored in centralized database. All the documents that identify users are stored on their device backed by IPFS, making them safe from hackers [18]. Decentralization enables the distribution of information on every node in the network, reducing the chances of a single point of failure (SPOF).
- Irrespective of geographical boundaries, the users can get their identity verified across the globe. It is both cost and time effective.
- Blockchain allows every individual on its network to trace the transactions. Every transaction, recorded on the blockchain, has a verifiable authenticity. However, the identity of the person, involved in transaction, remain obscured [19].

7. CONCLUSIONS

Blockchain enables more secure management and storage of digital identities by providing unified, interoperable, and tamper-proof infrastructure with key benefits to government, enterprises, users, and IoT management systems. It performs the middle and back office functions in a way what the Internet and the Web do to the front office functions - that is, automate functions thus bringing efficiency and new business opportunities.

Automated IAM system would empower government offices to operate more efficiently by decreasing the effort, time and money that is usually required to manage access to their networks manually. Besides, it will help to preserve the details of issuing and verifying authority, secure the documents from tampering, make all the relevant information available to authorities through public key, easy access to personal information or original documents, anytime and anywhere, through users' private key, restrain malpractices, evasion of taxes and increase the economy of the nation [Garg, 2020].

The blockchain identity management doesn't set to any geographical boundaries. So, a user can use the platform across the borders to verify his identity. Since the system is decentralized, there will be no single point of failure (SPOF). Thus, blockchain would allow people to enjoy self-sovereign and encrypted digital identities, replacing the need for creating multiple usernames and passwords.

REFERENCES

[1] R. Garg, "Global Identity through Blockchain". International Webinar on Blockchain. Scholars Park, IN 2021, pp. 1-60.

[2] UIDAI. Official Website, 2021.

[3] R. Garg, "Digital ID with Electronic Surveillance System" Patent NIF/S&D/000-108-828, 2018.

[4] G.W. Peters, E. Panayi and A. Chapelle, "Trends in Cryptocurrencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective" 2015.

[5] G. Foroglou and A.L. Tsilidou, "Further Applications of the Blockchain," 2015.

[6] B.W. Akins, J.L. Chapman and J.M. Gordon, "A Whole New World: Income Tax Considerations of the Bitcoin Economy" Pittsburgh Tax Review, vol. 12, no.1, pp. 24-56, 2015.

[7] Y. Zhang and J. Wen, "An IOT Electric Business Model based on the Protocol of Bitcoin," Proc 18-ICIN, Paris, 2015, PP. 184-191.

[8] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward" in Proc EC-TEL2015, Lyon, France, 2015, pp. 490-496.

[9] C. Noyes, "Bitav: Fast Anti-Malware by Distributed Blockchain Consensus and Feed Forward Scanning" 2016.

[10] R. Garg, "Generic Information Tracker". India International Science Festival, New Delhi, 2016.

[11] R. Garg, "Multipurpose ID: One Nation - One Identity". Annual Convention - Indian Society for Technical Education (ISTE), India, 2019, pp. 39.

[12] R. Garg (2019). Multipurpose ID: A Digital Identity to 1.34 Billion Indians. Ideate for India - Creative Solutions using Technology. National e-Governance Division, Ministry of Electronics & Information Technology, Government of India.

[13] R. Garg, "Hi-Tech ID with Digital Tracking System". National Conference on Application of ICT for Built Environment, 2017.

[14] R. Garg, "Self Sovereign Identities". Lambert Heinrich-Böcking-Str. 6-8 | 66121 Saarbrücken, Germany, 2021, p. 1-96.

[15] R. Garg, "Blockchain based Decentralized Applications for Multiple Administrative Domain Networking". BITS - Pilani, KK Birla Goa Campus, India, 2021, pp. 01-69.

[16] R. Garg, "Blockchain Ecosystem for Education & Employment Verification". 13th International Conference on Network & Communication Security. Toronto, Canada, 2021.

[17] R. Garg, "Decentralized Transaction Mechanism based on Smart Contracts". 3rd International Conference on Blockchain & Internet of Things. Sydney Australia, 2021.

[18] R. Garg, "Distributed Framework for Real World Applications," Barnes & Noble USA, 2021, pp. 01-98.

[19] R. Garg, "Digital Identity Leveraging Blockchain", Barnes & Noble USA, 2021, pp. 1-124.