Journal of Blockchain Research Volume 1 (2022) 51–63

Distributed ecosystem for identity management

Rishabh Garg

The blockchain identity ecosystem offers the possibility of rejecting the outdated identity system and eliminate the intermediaries. Identity management, through blockchain, can allow individuals to take ownership of their identity by creating a global identity (ID) to serve multiple purposes. For user security and ledger consistency, asymmetric cryptography and distributed consensus algorithms can be implemented. Blockchain technology would be able to save costs and increase efficiency due to its key features such as decentralization, persistence, anonymity and auditability. In addition, the digital identity platform would save citizens' time in accessing or exchanging their personal data and records. Instead of being required to appear physically before the service provider, the user may be provided with a digital ID through his/her personal device, such as a smartphone, through which he/she can share his identity details with the service provider, using distributed ledger technology (DLT).

Keywords and phrases: Blockchain, Decentralized apps (dApps), Data portability, Decentralized public key infrastructure (DPKI), Decentralized identifiers (DID), Ethereum, Hash, Identity management system (IMS), IPFS, Private key, Public key, Revocation, Self sovereign identity, Storage variables, Validation, Zero knowledge proof.

1. INTRODUCTION

Globally, 1.1 billion people, covering 21 million refugees, lack proof of their legal existence. This problem overly affects kids and women from rural areas in Asia and Africa. Without an official identity, it becomes difficult to access education and medical services, open a bank account, and get benefits of public distribution system (PDS). Recent advances in digital technology and biometrics (iris scan, face recognition and voice recognition) make it easier for governments to provide secure digital identities (ID). Further, digital records are less prone to tinkering or degradation.

During the last one decade, several countries - Estonia, India, Pakistan, Peru, Singapore and Thailand, have adopted digital ID systems, with Estonia being the first to hold a fully digital framework embracing the most advanced national ID system in the world. The system involves the use of an 11-digit national ID card with citizen information, duly encrypted by a pair of public and a private key. Estonians use this card to carry out a variety of functions in online as well as off-line mode. It includes travel within the EU, national health insurance, log into bank accounts, digital signatures, filing of tax-returns, and making access to government databases.

Another country is India that has registered around 1.27 billion residents out of its 1.4 billion population [1], [2]. Established in 2009, it has emerged as the world's largest biometric ID project. 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 is a long list of identity documents and to collect those documents, one has to face long queues, endless processes, bulk formalities, and intervention of agents and proxies. Over and above, the verification of these documents at each level, is another tedious task. Even so, during the online process, each app generates or asks for a new identity (ID) and password [3] which increases rather than reduces challenges, such as:

2.1 Lack of compatibility

Apps that operate a typical ID management system are neither updated regularly nor do they comply with security measures.

2.2 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.

2.3 Weak authentication protocols

The existing authentication process involves three stakeholders: i) companies undertaking Know Your Customer (KYC) verification; ii) User; and iii) that need to check the

identity of the user. Since KYC companies have to cater to the requirements of banks, healthcare providers, immigration officials etc., they need more resources to expedite their operations. As a result, they charge a huge amount from individuals in the form of hidden processing fees. Despite the fact that the process is speeded up, customers have to wait longer to connect with third party.

2.4 Lack of control

Currently, Users have no control over their Personally Identifiable Information (PII). Users are compromising their privacy without being aware of whom and how often their data is shared or where it is stored. Identity should therefore be secure and under user control, which can be verified whenever and wherever necessary. In order to overcome the shortcomings of existing identity management systems:

- There should be a proper interoperability network between the government and the complex bureaucratic system to reduce 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.

3. 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.

3.1 Blockchain

Blockchain is a type of DLT where transaction records are saved in the ledger as a series of blocks. All nodes maintain the ledger, so the overall computational power gets distributed among them, which gives better results. Blockchain provides:

- An enhanced security - each data is deeply encrypted (hashed) allowing a higher level of security. This makes hacking impossible;
- Faster disbursements - relatively faster than normal payment systems, although transaction rates can be slow in larger networks; and
- Consensus - that supports a wide range of consensus algorithms that help nodes make the right decisions.

Once a transaction is made, nodes on the network verify it. After verification, the transaction gets a unique hash ID along with the recent transaction hash ID, and gets stored in the ledger. Once it is added to the ledger, no one can change or delete the transaction.

3.2 Types of blockchain

Current blockchain systems are largely classified into three broad categories: public blockchain, private blockchain, and consortium blockchain [4].

In a public blockchain, all records are visible to the public and each node can participate in the consensus process. In contrast, private blockchain only allows nodes that come from a specific organization, to participate in the consensus process. Being wholly controlled by an organization, it is often thought of as a centralized network. In order to make the best use of both public and private blockchain solutions, a hybrid blockchain model can also be adopted.

The consortium blockchain enables a group of preselected nodes to participate in the consensus process. Since, only a small fraction of nodes are selected to determine consensus, the consortium blockchain built by multiple organizations is decentralized to some extent. The comparison between the three types of blockchain is given in Table 1.

3.3 Evolution of blockchain

Over the years, the scope of blockchain applications has expanded from virtual currencies to financial applications and education, health, science, transportation, and government. Blockchain is known as Blockchain 1.0, 2.0 and 3.0 depending on its applications.

3.3.1 Blockchain 1.0

Blockchain 1.0 was limited to virtual currencies, such as bitcoin, which was the first and most widely accepted digital currency [5]. Most Blockchain 1.0 applications were digital currencies, used in commercial transactions, relying on the cryptocurrency ecosystem, for small-value payments, foreign exchange, gambling and money laundering.

3.3.2 Blockchain 2.0

Blockchain 2.0 mainly includes bitcoin 2.0, smart-contracts, decentralized applications (dApps), decentralized autonomous organizations (DAO), and decentralized autonomous corporations (DAC) [5]. However, it was used in particular areas of finance to disrupt traditional currency and payment systems, primarily banking, stock trading, credit systems, supply chain finance, payment clearing, anti-counter-fitting and mutual insurance. Some programmable contract languages, such as Ethereum, Codius, and Hyperledger, were used to implement smart contracts.

Table 1. Comparison among the three types of blockchain

Property	Public blockchain	Consortium blockchain	Private blockchain
Centralized	Decentralized	Partially centralized	Fully centralized
Consensus process	Permission less (anyone can join the consensus process)	Permissioned	Permissioned
Consensus determination	All miners (each node could take part in the consensus process)	Only a selected set of nodes are responsible for validating the block	Fully controlled by one organization that could determine the final consensus
Read permission	Public	Depends, could be public or restricted	Depends, could be public or restricted
Immutability	Nearly impossible to tamper since records are stored with large number of participants	Could be tampered easily as there is only limited number of participants	Could be tampered easily as there is only limited number of participants
Efficiency	Low (transaction throughput is limited and the latency is high because of the large number of nodes on the public blockchain network).	High (with fewer validators, the system is more efficient).	High (with fewer validators, the system is more efficient).
Examples	Bitcoin, Dash, Ethereum, IOTA, Litecoin, Monera, Steemit, Stellar, Zcash, etc.	Quorum, Hyperledger, and Corda	R3 (banks), EWF (Energy), B3i (Insurance Corda)
Miners	Don't know each other	May or may not know each other	Know each other

3.3.3 Blockchain 3.0

Blockchain 3.0 is considered the blue-print of the new economy. It can be employed in sectors such as education, health, science, transportation and logistics, apart from currency and finance. The scope of this type of blockchain and its potential applications suggests that blockchain technology is an ongoing goal [7]. This involves a more advanced form of smart contracts setting up a distributed organizational unit that creates its own laws and operates with a high degree of autonomy [8].

The merger of Blockchain with Token is an important addition to Blockchain 3.0. The token is a verification of digital rights, and therefore the block chain token is widely recognized with due credit to Ethereum and its ERC20 standard. Tokens can serve as verification of any number of rights, including personal identification, educational diplomas, currency, receipts, keys, discount points, vouchers, stocks and bonds. It can be said that tokens are its front-end economic face while blockchain is the new age back-end technology.

Thus, by using blockchain technology, a digital architecture can be introduced that can combine authentication capabilities and personal privacy protection to generate a frictionless experience of identity.

3.4 Identity models

Since the advent of the Internet, models of online identity, as shown in figure 1, have progressed through four broad stages:

3.4.1 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, as illustrated in figure 2, 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.

3.4.2 Federated identity

The second model of digital identity management, known as Federated Model, is controlled by multiple federated authorities. 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 envision federated identity, which allowed users to utilize the same identity on multiple sites.

The best examples are 'login with Facebook' and 'login with Google' functionalities, wherein Facebook and Google served as intermediaries. Companies outsourced their identity management to major corporations who have an economic interest in gathering personal databases of users. Eventually, this raised many privacy and security concerns.

3.4.3 User-centric identity

It is controlled by an individual, across multiple authorities, without requiring a federation, as depicted in figure 3. This identity model is based on the assumption that every

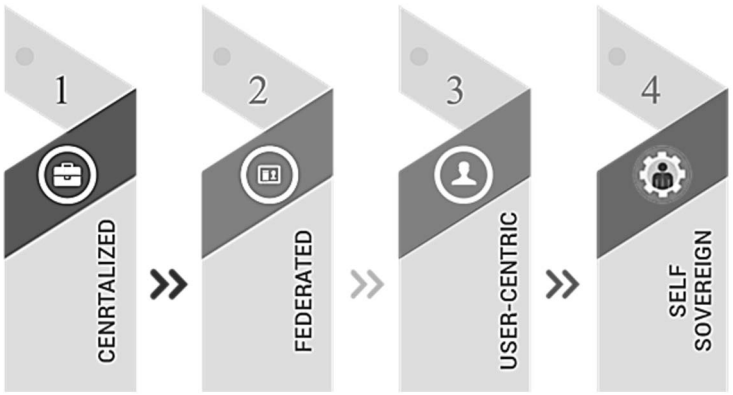

Figure 1. Decentralized Models of Online Identity.

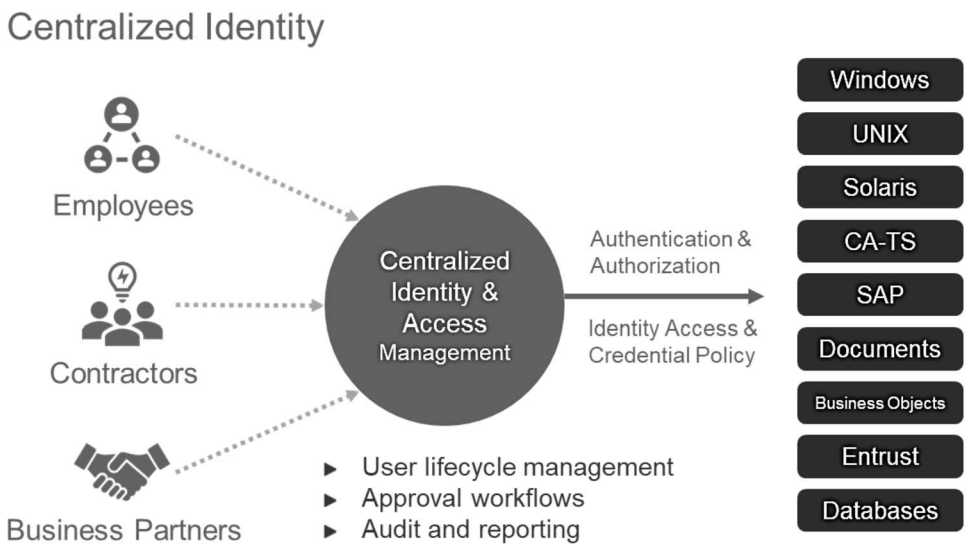

Figure 2. Centralized Identity.

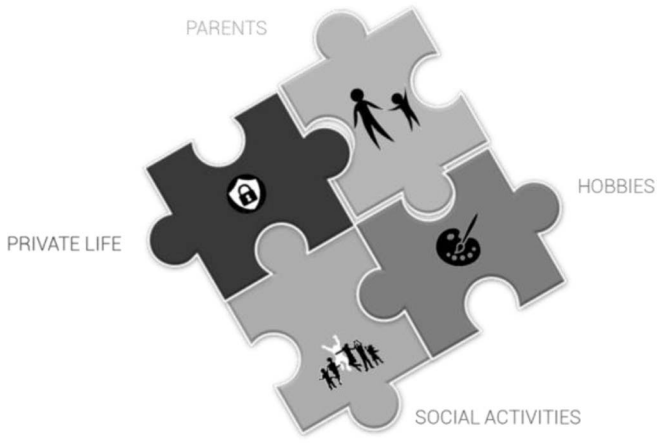

Figure 3. User-centric Identity.

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, and store all his personal data on his own devices, without relying on a central repository of identity data.

In a user-centric identity model, there exists a single identifier and credentials provider that is used by all service providers. The user-centric identity model can be implemented in many ways, such as - common user identifier model, meta-identifier model and single sign-on.

The Common User Identity solution allows a user to access all service providers using the same set of identifiers and credentials. This can, for example, be implemented by a PKI where a single certificate authority (CA), or its subordinate issue certificates to all users within the domain. Given that all criteria required for PKI to operate are satisfied, users only need a set of identifiers, say email addresses and credentials to be authenticated by all service providers.

Besides, the Meta User Identity Model can be implemented by mapping all service provider unique identifiers to a single meta-identifier, associating credentials with them. However, this would require policy agreement and strong trust between the parties involved.

A single-sign-on identity domain allows a user authenticated by one service provider to be considered authenticated by other service providers. This is commonly called a Single Sign-On (SSO) Model because the user needs to authenticate (sign on) only once to access all the services. Microsoft.NET Passport is an example of an SSO execution for e-commerce, where email addresses are espoused as user identifiers. NET passport model, issuance of credentials and authentication are centralized functions under the control of Microsoft.

3.4.4 Self sovereign identity

Self-Sovereign Identity (SSI) 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. Figure 4 clearly indicates how the proposed SSI model is better than the existing ones. 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.

3.5 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 (Interplanetary File System) is a decentralized storage solution for blockchain-based content.

3.5.1 Interplanetary file system (IPFS)

IPFS uses a peer-to-peer (P2P) network model for file sharing that is decentralized and distributed across multiple computers or nodes. Files are split into different parts and stored in a network of nodes that track the file by hash. 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 main innovation for IPFS. It is similar to the BitTorrent protocol, but differs in the way the file is indicated for sharing. It stores files on a blockchain as key value pairs. The data is split 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 relies on torrents instead of pointing to files. You can have different torrents pointing to the same file, but in IPFS you only need a hash ID that points to a single file.

Files are not posted to IPFS in the same way that a file is posted to the cloud. IPFS uses a secure hash of the file contents for location identification and DHT for location resolution. This is done because the resource or object is not available on the server but on a decentralized platform. When someone requests data, the data is directly represented by its hash ID, not by the actual file. 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 takes away the complexity for the application developers.

IPFS differs from location-based storage systems, i.e. the conventional Hypertext Transfer Protocol (HTTP) family of protocols or the centralized namespaces. When a storage system is location-based, it tracks the host by a logical addressing scheme (such as an 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 the file. In this case, the data is accessed based on its cryptographic hash

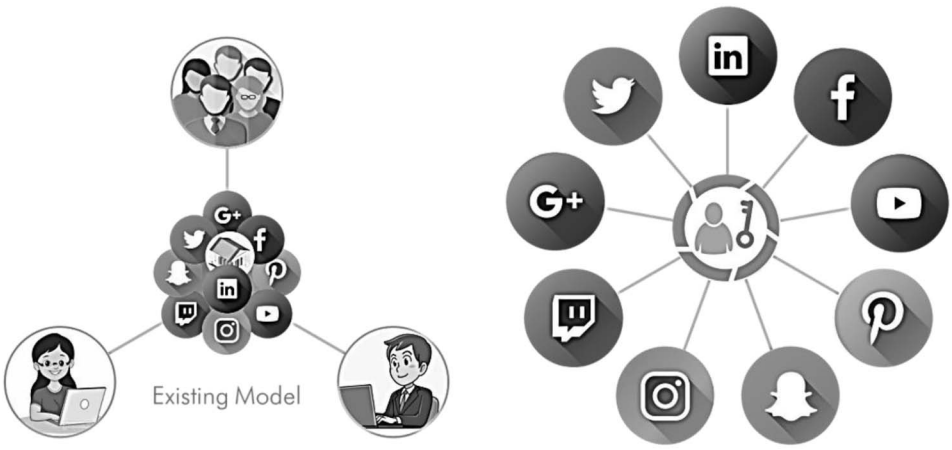

Figure 4. Comparison between the Existing Model and the Proposed Model.

rather than a logical address, almost like a digital fingerprint of a file. Regardless of who uploaded the file, where and when, the network always returns the same content based on that hash.

3.5.2 IPFS commands

```
1. cd go-ipfs
2. ./install.sh
3. /ipfs init
4. ipfs cat <readme file>
5. cat <filename>
6. ipfs add <filename>
```

When it comes to speed and reliability, IPFS outperforms HTTP. Rather than relying on a server location to fetch a file, a content addressed storage system can serve a file from any server, whichever is closest to the user. This implies that the user can search for the file without any search engine having to refer to the location i.e. the server name or address. Instead, it can refer to it by the hash of the file, which will be available from the nearest available nodes (a peer or node) on the IPFS network.

IPFS

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

4. BLOCKCHAIN BASED IDENTITY SOLUTION

In order to avail any facility or service, the identity of a person has to go through two stages: authentication and verification process, as seen in figure 5. In order to prove that the identity belongs to the person who has approached the authority, his name and identity documents are verified by the authentication process. There is a process of verification to know whether the documents showing name, address or passport number submitted by the individual are correct or not. This means that a verifying entity verifies whether the data, claimed by the individual, is genuine or not. This is usually done through verification of the identity of the documents.

In distributed ledgers, each unit of a block in the network has a single source of truth about the validity of credentials, and also the information about the verification authority,

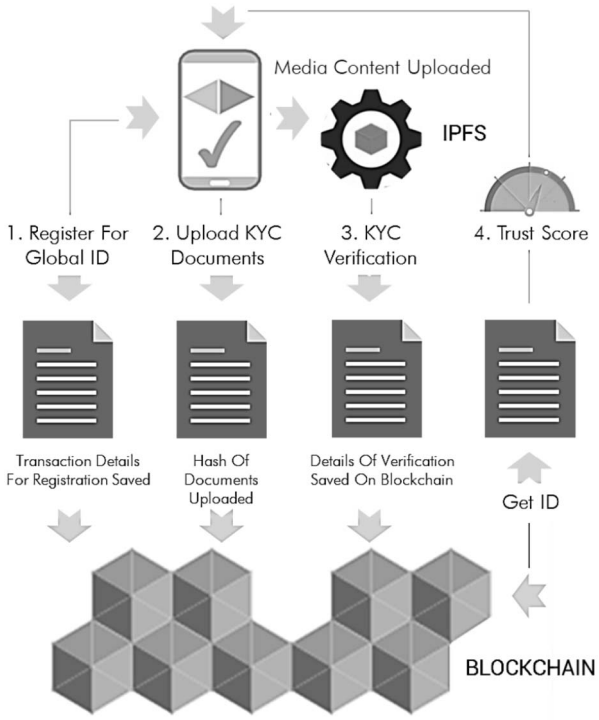

Figure 5. Identity and Access Management through Blockchain.

without the obligation to keep or reveal all of its actual details.

Leveraging blockchain technology for identity and access management, three distinct actors – identity owners, identity issuers and identity validators, play their roles. An identity issuer is a trusted authority such as a government body that has the authority to issue personal credentials to the identity owner (user). It acts as a verification authority that stamps the validity of personal data (such as last name and date of birth) by issuing a credential. The identity owner, as a rule, stores these credentials in their Pi Wallet and uses it to prove their identity to third parties on demand. The third party or verifier determines the validity of the proof through the validity of the verification and the credibility of the certifying party. It does not check the validity of the actual data given in the evidence.

4.1 Data portability

The decentralized structure reduces the need for re-verification of identities across different services and platforms. With decentralized identities (DIDs) and verifiable certificates, it is possible to transfer identities that are attached to one target system into another. Data portability reduces excessive friction for the user, making the sign-up process simple and user-friendly.

It will also empower the user to re-verify himself to meet regulatory KYC requirements. This will bypass the cumber-

Table 2. Benefits of Blockchain based ID management over conventional ID management

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 passcode)
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 infra-structure 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.

some identity verification process, where a series of documents are required and scrutinized, and it will progressively reduce customer time, avoid drop-out rates and reduce costs in the financial sector.

4.2 Right and control

In centralized identity systems, the identity issuing authority is usually responsible for data security. 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.

4.3 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. Each credential has a status in the registry, whether it has been revoked (deleted or updated) or is still valid.

4.4 Prevention of identity theft

In blockchain identity management, each user can store their identity credentials on a digital identity wallet on a device such as their smartphone. Digital identity authentication is only valid when used from a device that is authorized to do so. If the device is lost, the user can use any other authorized device, which could be his laptop - to write on the blockchain that the authorization of his cell-phone has now been revoked.

This will come into force with immediate effect and prevent anyone from using digital identity certificates on cellphones. Regardless of whether it has a password, biometrics or device, the burglar will not be able to impersonate the user because the immutable and secure chain (blockchain) will now maintain a revocation registry for the phone. Thus, the thief will not be able to build new relationships.

In the next step, the existing relation keys (pairwise connections, where each of them has a unique key) will be revoked. This prevents the thief from finding out the existing relationship between the device and other people or organizations. A brief comparison between traditional ID management and blockchain ID management is presented in Table 2.

5. IDENTITY BASED APPLICATIONS

With the increasing sophistication of smartphones, advances in cryptography, and the advent of blockchain technology, a new identity management system can be built on the concept of decentralized identifiers (DIDs), which is hereafter referred to as a new subset of decentralized identities - Self Sovereign Identities (SSI) [9].

For the security of user data and the stability of the ledger, asymmetric cryptography and distributed consensus algorithms can be implemented. Blockchain technology, through smart contracts, establishes trust between parties and assures authenticity of data and verification. Blockchain technology will save costs and increase efficiency due to key features such as decentralization, persistence, anonymity and auditability. Most importantly, transactions once packaged in the blockchain cannot be tampered with. Therefore, it has transformative potential in various sectors such as education and employment verification [10], crowd funding,

banking and investment, trade [11], online payments [12], e-commerce, predictive markets, distributed resources, public services [13], Internet of Things (IoT) [14], reputation systems [15], security services [16], healthcare, content creation and research.

5.1 Crowd operations (voting)

Decentralized Applications can implement Ethereum Smart Contracts to automate processes involving crowd operations. Application Programming Interface (API) 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 dApps.

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.

5.2 Prediction markets

A prediction market refers to betting on outcomes that can be accessed by smart contracts. This includes - market creator, who posts market events on the platform; market journalists, who speculate on the outcome of the event; and market participants, who can use their token/cryptocurrency for stake. If the predicted result is true/false, the participants win/lose the prize. The tokens used are called Reputation Tokens (REP Tokens) and are used for the intended purpose in case of a dispute, while the trading currency is Ether. An end-to-end marketplace of stocks, futures, products, ideas, etc. is facilitated by smart contracts.

5.3 Distributed resources and IoT

It works on the concept of Distributed Energy Resources (DER) and works on the energy retail stage (energy generation, transmission, distribution, out of retail) of the power supply chain. It is a permissioned blockchain dApp implemented at the Ethereum smart contract layer. It aims to make energy transfer and payment transactions through crypto tokens on the blockchain architecture. Market participants, in addition to power 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 transactions, Multisig (MS) cryptowallet with PKI security. Intelligent electricity usage is done by coding efficient price options using smart contract. The integration with IoT devices further strengthens the process. An ERC20 (fungible) token called BOLT is used for payment. To sign a transaction, two of the MS1, MS2, MS3 signatures are required (MS2, MS3 are used for smart agent control). Smart Agent Escrow is used to hold tokens along with some security deposit (in case of excess electricity usage).

Thus blockchain has immense potential for real world applications. Whilst millions of transactions are recorded across hundreds of nodes scattered over thousands of financial institutions, notwithstanding any geographical or political boundaries; likewise, all identity documents, from different administrative organizations, can be recorded using a private key [17]. Consequently, all the identity details of the citizen would be available on a secure personal ledger. The private key can be an alpha-numeric password, fingerprints and/or a retina scan of a citizen.

6. PROPOSED WORKING MECHANISM

Blockchain, by incorporating certain technical components, namely – native Android or iOS apps for individuals and verification entities; IPFS to store the user's PII; micro service program using Node JS; and public blockchain components could allow people to create self-sovereign and encrypted digital identities, replacing the need to create multiple usernames and passwords. To do this, an account address will be generated using a unique private key. The private key can be an alpha-numeric password, associated to a random number employing a mathematical algorithm. Biometrics cannot be used to generate private keys because fingerprints and the blood vessels of the retina are subject to change with time.

6.1 Installation of software

One has to download the mobile app from Play Store or App Store. After downloading the app in the mobile phone, a profile will be created on the user app. Once the profile is created, the user will receive a unique ID number from the UDI authority which will help organizations to send or gain access to the identity documents of the user.

6.2 Procurement of documents

The user will have to input the government-issued ID, through the app, into the IPFS containing the hashed address stored in the blockchain. The proposed identity management scheme has been illustrated in figure 6.

The app will extract personal information from these IDs, so that the user can self-certify his details. Users will now have ownership of their own data. This will help the users to decide what information is to be shared with which organization. To share specific details or required information, it will encrypt the information (in this case the hash of the credentials) and share the relevant public key to whom it may ever concern (government organization/service

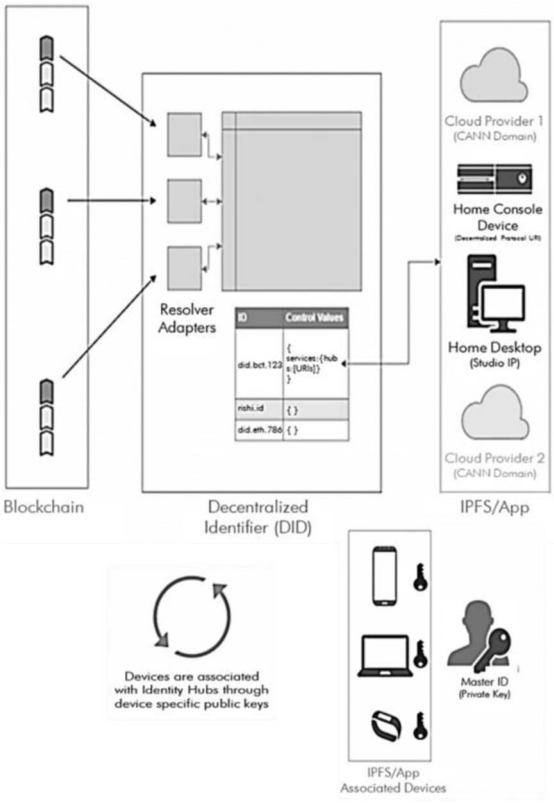

Figure 6. Schematic diagram of Distributed Ledger Technology to record citizen data.

provider or validator) for decryption. Without the consent of the user, no information may be shared with any identity seekers.

In case of a new born, 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 retrieved 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 [18]. Even if the 16-digit ID becomes public, it cannot retrieve the documents / information from the app unless it has 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.

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, addons, extra-curricular attainments, sports, etc. of the candidate on the same IPFS [19].

On seeking transfer from one institution to another, the previous school will generate a transfer certificate through its authorization key. An authorization key is a private key, unique to an officer who holds a position as authority that would be distinct from his/her personal private key. As the child takes admission into the successive institution, his/her parent will share his/her public key with all relevant details, and the new school administration will start writing to his/her IPFS. The school will write a revocation registry (figure 7), which will prevent the student from taking admission in two institutions at a time.

Often the postal department finds it difficult to provide quality service on time due to incomplete or incorrect address on the post or parcel received. If every citizen has a unique identification number, which can be entered on the portal of the Department of Posts, then the department will also not require the name and address of the consignee or recipient. He can decode the address on the basis of that identification number and provide services at the registered address. Such services are already being used, in a limited territorial range, by the aviation department, supply chain management etc.

During periodical census, the government may 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 [20]. 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.

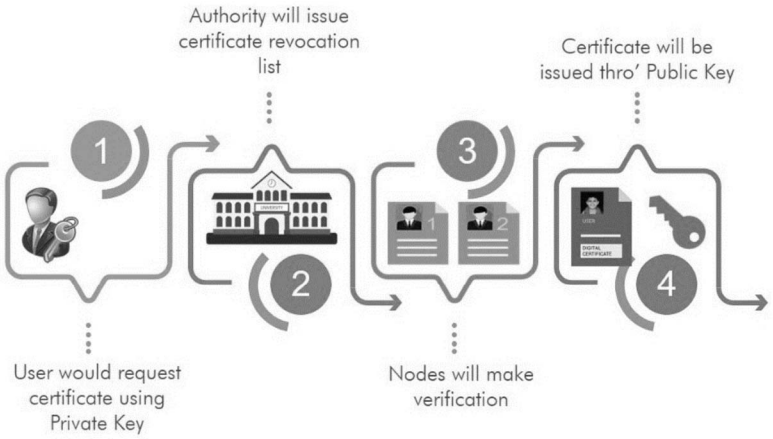

Figure 7. Endorsement of Documents on User's Profile.

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 rarely have the opportunity to make delays or ask for 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, at one go. This will help the patients to get better treatment [21].

For all financial transactions, the UDI will be linked to only one person. Therefore, getting all the deposit and lending details using the tree root hash will happen in a matter of seconds. Wherever he/she goes, be it a restaurant, club, shopping mall or traveling abroad, the IPFS object linked to the UDI will take account of every penny he earns or spends. This will enable the honest taxpayer to disclose all his assets and liabilities before the IT authority. Even IT executives will have no reason to doubt their integrity. However, unscrupulous taxpayers will have bad days.

Similarly, documents relating to assets, business, financial history, medical records, health insurance ... can be maintained by creating a distributed hash table on IPFS [22] linked to UDI ... and the hash of the same can be encrypted using public key of the user. These encrypted hashes may be operated, accessed or retrieved, using a multipurpose digital ID card.

One world - one identity

The Multipurpose ID (One Card - Multiple Use) will contain the name of the user, a Quick Response (QR) code, his/her photograph as shown in figure 8. This will be useful for all services. The card, when inserted into a card reader or a customized machine, will display the DHT containing all encrypted, hashed information for the items and its sub-items. The user can access the documents online using his private key.

Figure 8. Digital ID (One Card - Multiple Uses).

In case one loses his/her multipurpose ID, he/she can request the appropriate authority to issue the clone. This clone will be a vegetative copy of the original ID (since no mutation is possible in the blockchain). If a criminal tries to steal someone's identity, or takes advantage of it, he or she will not be able to do so because 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.

6.3 Third-party access

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

Blockchain does not store user data or information. The information is stored in the user's IPFS, and transactions that are carried out between the identity holder and third parties will only be recorded on the blockchain.

For example, if the passport authority verifies the person's identity through a public key or an app, that transaction will be added on the blockchain and visible to all connected nodes. Suppose there is a person named Rishi, who needs to authenticate himself in order to apply for a visa. Rishi will provide a hash of the object that contains all the necessary credentials (duly encrypted by Rishi's private key and the authority's public key), to help them access 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, as depicted in figure 9, and the transaction will be recorded on the blockchain. This is how the authorities would be able to validate his identity instantly [23].

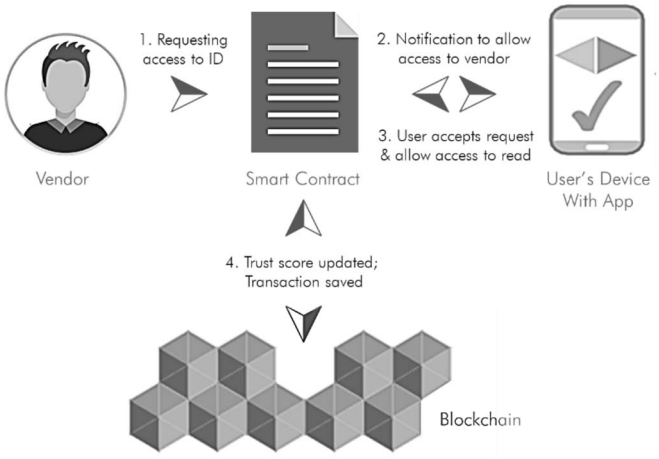

Figure 9. Identity Access through Blockchain.

6.4 Maintenance of trust score

Smart contracts containing business logic can generate a trust score for a user from the information provided by him to create a self-sovereign identity. The higher the trust score, the higher the credibility of the individual. It can help organizations to validate user identity on a real time basis.

An initial user may be kept under observation for the first six months to establish a trust score. During the period, he can submit the necessary information and upload the credentials to establish his identity. A user can achieve a high trust score by uploading multiple documents to the app/IPFS. The system will verify whether the details like name, parent's name, date of birth etc. match exactly or differ significantly. Perfect matches will increase trust score.

Conversely, if a user fails to upload the relevant documents on the system; does not allow access to government organizations to verify identity; or makes frequent changes to his identity profile, particularly with respect to his name, parent's name, date of birth, gender, religion, etc., his trust score will be reduced [24]. Based on the user's trust score, as depicted in fig 10, it can be determined whether it is a legitimate account or a suspicious one.

For example, if a bank needs to check the authenticity of a person to grant him a loan, they can check the trust score of the user. This can save time, money and provide an insight about user reliability [25]. Since the object, containing all information or transactions, will be protected by the user's public key, it is only the user who will be able to access 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.

7. BREAK-THROUGH EFFICIENCY

The recommended technology has a number of user optimized features:

A blockchain identity management system does not store any user data, rather it uses smart contracts to share personal information, and therefore data manipulation is not possible on the blockchain. Any transaction of user information may not take place without the explicit consent of the user which adds security to identity management.

No personal identity document of users is stored in a centralized database. All documents identifying users are stored on their devices backed by IPFS, making them safe from hackers [26]. Decentralization enables the distribution of information on each node in the network, reducing the possibility of a single point of failure (SPOF).

Users can get their identity verified worldwide, regardless of geographic boundaries. It is both cost and time effective.

Blockchain allows every person on its network to trace transactions. Every transaction recorded on the blockchain has a verifiable authenticity. However, the identity of the person involved in the transaction remains obscured [27].

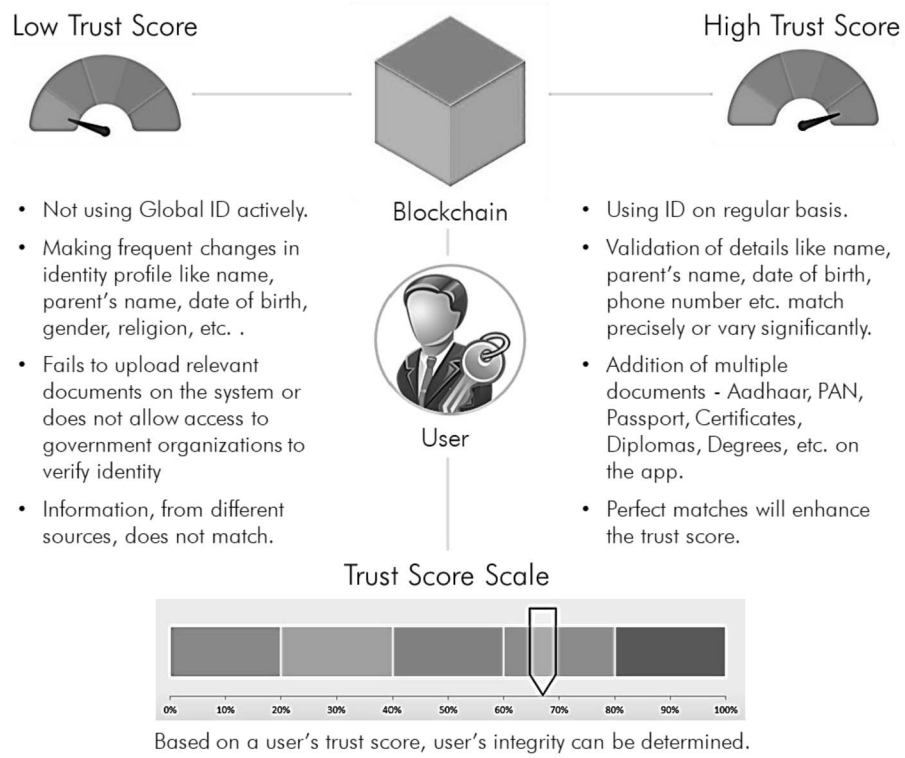

Figure 10. Rise & fall of Trust Score.

8. CONCLUSIONS

Blockchain enables safe storage of digital identities by providing a unified, interoperable and tamper-proof infrastructure with key benefits to governments, enterprises, users and IoT management systems. It performs middle and back office functions in a way that Internet and Web do to front office functions - that is, automated tasks that bring 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.

The ultimate challenge for any user-centric ID system is to influence the national government, since most of the services, citizens rely on, are provided by governments. Without government approval and participation, ID systems cannot hold their promises. The same tenet applies to international organizations too.

Received 27 February 2022

REFERENCES

[1] R. Garg, "Global Identity through Blockchain." International Webinar on Blockchain. Scholars Park, IN 2021, pp. 1–60.
[2] UIDAI. Official Website, February 2022.
[3] R. Garg, "Digital ID with Electronic Surveillance System," Patent NIF/S&D/000-108-828, 2018.
[4] V. Buterin, A Next-Generation Smart Contract and Decentralized Application Platform. White paper, 2014.
[5] M. Mainelli and M. Smith, Sharing Ledgers for Sharing Economies: An Exploration of Mutual Distributed Ledgers (Aka Blockchain Technology). Journal of Financial Perspect, 2015: 3(3) 38.
[6] M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015: 152.
[7] M. Crosby, P. Pattanayak and S. Verma, Blockchain Technology: Beyond Bitcoin. Applied Innovations, 2016: (2) 6–19.
[8] A. Pieroni A., N. Scarpato, L. Di Nunzio, F. Fallucchi and M. Raso, Smarter City: Smart Energy Grid based on Blockchain Technology. International Journal for Advances in Science, Engineering & Information Technology, 2018: 8(1) 298–306.
[9] R. Garg, "A Technological Approach to Address Deficiencies in UID (Aadhaar)." 3rd International Conference on Big Data, Blockchain and Security, Copenhagen, Denmark, 2022.
[10] R. Garg, "Blockchain Ecosystem for Education & Employment Verification." 13th International Conference on Network & Communication Security. Toronto, Canada, 2021.
[11] G.W. Peters, E. Panayi and A. Chapelle, "Trends in Cryptocurrencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective," 2015.
[12] G. Foroglou and A.L. Tsilidou, "Further Applications of the Blockchain," 2015.
[13] 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.

[14] Y. Zhang and J. Wen, "An IOT Electric Business Model based on the Protocol of Bitcoin," Proc 18-ICIN, Paris, 2015, pp. 184–191.
[15] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward," Proc EC-TEL2015, Lyon, France, 2015, pp. 490–496.
[16] C. Noyes, "Bitav: Fast Anti-Malware by Distributed Blockchain Consensus and Feed Forward Scanning," 2016.
[17] R. Garg, "Ethereum based Smart Contracts for Trade and Finance." International Conference on Blockchain and Smart Contracts, Bangkok, Thailand, 2022.
[18] R. Garg, "Generic Information Tracker." India International Science Festival, New Delhi, 2016.
[19] R. Garg, "Multipurpose ID: One Nation - One Identity." Annual Convention - Indian Society for Technical Education (ISTE), India, 2019, pp. 39.
[20] R. Garg, 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, 2019.
[21] R. Garg, "Hi-Tech ID with Digital Tracking System." National Conference on Application of ICT for Built Environment, 2017.
[22] R. Garg, "Self Sovereign Identities." Lambert Heinrich-Böcking-Str. 6-8 | 66121 Saarbrücken, Germany, 2021, pp. 1–96.
[23] R. Garg, "Blockchain based Decentralized Applications for Multiple Administrative Domain Networking." BITS - Pilani, KK Birla Goa Campus, India, 2021, pp. 01–69.
[24] R. Garg, "Interplanetary File System for Document Storage and e-Verification." 2nd International Conference on Software Engineering, Security and Blockchain, Sydney, Australia, 2021.
[25] R. Garg, "Decentralized Transaction Mechanism based on Smart Contracts." 3rd International Conference on Blockchain & Internet of Things. Sydney Australia, 2021.
[26] R. Garg, "Distributed Framework for Real World Applications," Barnes & Noble USA, 2021, pp. 01–98.
[27] R. Garg, "Digital Identity Leveraging Blockchain," Barnes & Noble USA, 2021, pp. 1–124.

BIONOTES

Rishabh Garg is a sophomore at BITS - Pilani, Goa; an upcoming Software Development Engineer with ServiceNow, Hyderabad and an SDE Intern with Ethan AI, Singapore. He has worked in Data Science for Indian Institute of Technology, New Delhi, and an SDE with Swiggy, Bangalore, India.

He has authored two books in six international languages in the US,! Germany, France, Italy, Moldova, Spain, and Portugal. He is a Journal Referee with IEEE Internet of Things, an Author with John Wiley & Sons, US; and a Program Committee Member for 3rd International Conference on Artificial Intelligence & Machine Learning to be held in Toronto, Canada. He is an active contributor to the open source software community and has accomplished 5 Major Projects in Web D; 4 in Machine Learning; 3 on Blockchain and 2 in Financial Management.

Rishabh is a recipient of the National Award for Exceptional Achievements in Innovation from the President of India and National CSIR Innovation Award from the Prime Minister of India. He has also received an International Bronze Award from the Royal Commonwealth Society, London and Young Scientist Award from Ministry of Science & Technology, and Earth Sciences, Government of India for creative technological solutions.

Rishabh Garg
Department of Electrical & Electronics Engineering
Birla Institute of Technology & Science
K.K. Birla Campus, Goa - 403726 India
E-mail address: rishabhgargdps@gmail.com