INTERNATIONAL

WEBINAR

GLOBAL IDENTITY

THROUGH BLOCKCHAIN

RISHABH GARG

BITS - Pilani | Goa | India

SCHOLARS PARK

36 | VRINDAVAN NAGAR | BHOPAL

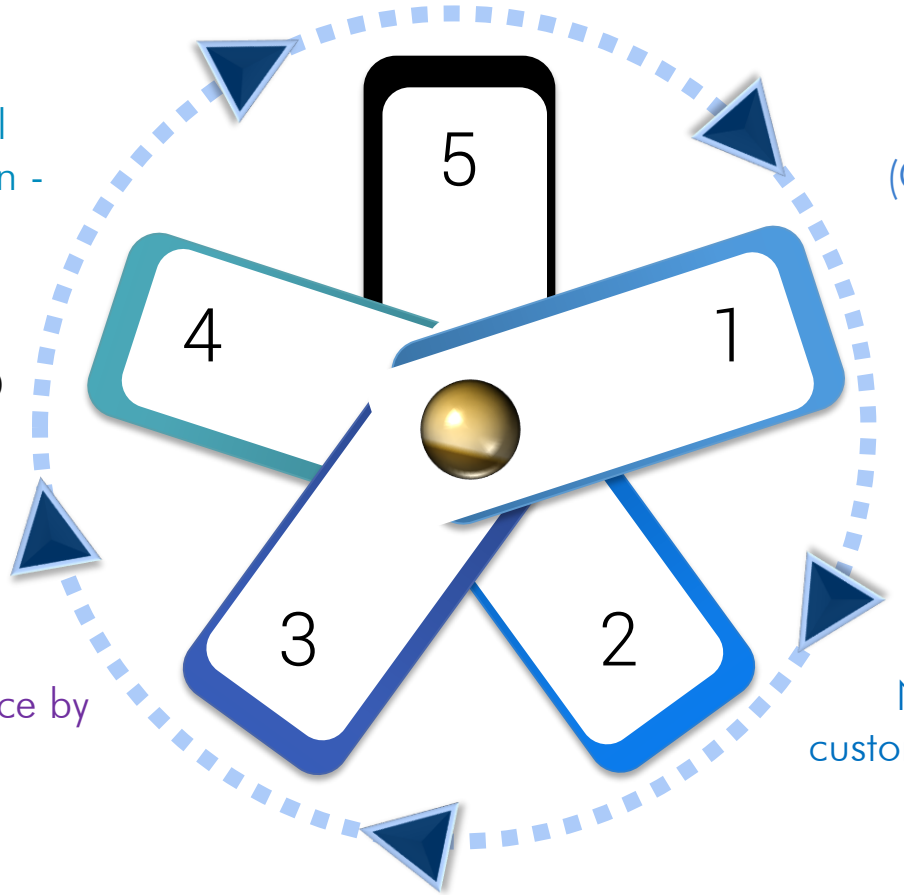
9 789354 933837

Received National Child Award for Exceptional Achievements by Honorable President of India

Registered by National Innovation, Foundation - Government of India

Renamed as Digital ID with Electronic Surveillance System

Honored for special achievements in Science by Government of India



The Idea of Multipurpose ID (Generic Information Tracker) popped-up in 2016

The Idea was presented at India International Science Festival 2016

Prime Minister of India Narendra Modi motivated to customize it for India Vision 2020

9 789354 933837

Our Concern

- ✓ Identity provides a gateway to make access to food, shelter, health, medical care and all such amenities, upon which a citizen has a legitimate right as human being.

Magnitude of the problem

- ✓ Over $ 2.2 billion dollars lost or misused annually in the developing world due to lack of verifiable ‘first-mile’;
- ✓ 65.3 million refugees and displaced people world-wide;
- ✓ 2.5 billion people lack access to banking and credit services;

9 789354 933837

Identity Instruments

✓ In India, there is no single document that serves as National ID [Garg, 2016], yet the following documents are issued for specific purposes that work as ID:

• Aadhaar Card	• Electoral Photo Identity Card (EPIC)
• Indian Passport	• Transfer/Matriculation Certificate
• Overseas Passport	• Freedom Fighter Identity Cards
• Ration Card	• Service Identity Card
• Birth Certificate	• Arms Licenses
• Policy Bond	• Overseas Citizenship of India (OCI)
• PAN Card	• SC/ST/OBC Certificates
• Driving License	• Person of Indian Origin

9 789354 933837

Identity Instruments

• Railway Identity Cards	• Property Documents
• Student Photo ID	• Gas Connection Bill
• Pensioner Photo Card	• Bank/ PO Passbooks
• Unique Disability ID	• Extract of the Service Record
• Photo Credit Card	• Certificate of Identify issued by a Gazetted Officer or SLR
• Marriage Certificate	
• Gazette Notification	• Legal Name Change Certificate

Since citizens are provided with different IDs for different purposes, there is a lack of resemblance in citizen's profile among different data repositories, causing discrepancy and recurrence [Garg, 2017]

9 789354 933837

Problems with Multiple ID

Absence of Single National ID has manifold complications [Garg, 2018]:

- ✓ Procure endless number of IDs, certificates, licenses …… ;
- ✓ Lengthy procedures and official formalities;
- ✓ Periodical renewal, which demands documentation all over again;
- ✓ Wastage of paper, time, money and working days;
- ✓ Long queues, intervention of proxies and agents;
- ✓ Corruption, imposture and suppression of facts;
- ✓ Loss of revenue, due to evasion of tax.

9 789354 933837

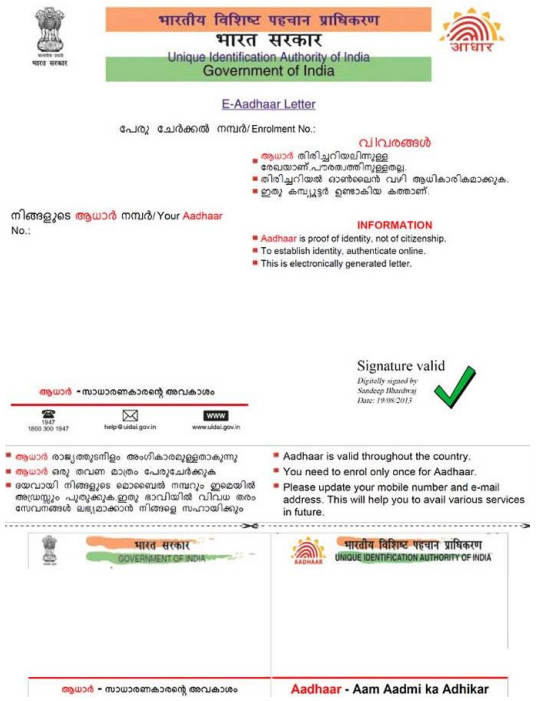
Quest for National Identity

- ✓ For last three decades, there has been a terrific surge of experimentation for identity.
- ✓ Until 1990, Ration Card was a popular tool of Identity.
- ✓ In 1993, the Voter ID or EPIC was implemented.
- ✓ In 2006, the idea of Universal Identity (UID) was proposed by the Department of Information Technology, Government of India.
- ✓ In 2009, Unique Identification Authority of India (UIDAI) was established under the aegis of Planning Commission [Garg, 2019].

9 789354 933837

UID Standards

The data used in UID encompasses Biometrics Data and Demographics Data.


भारतीय विशिष्ट पहचान प्राधिकरण
भारत सरकार
Unique Identification Authority of India
Government of India

E-Aadhaar Letter

പേരു ചേർക്കൽ നമ്പർ/ Enrolment No.:

വിവരങ്ങൾ

- ആധാർ തിരിച്ചറിയലിനുള്ള തെളിവാണ്, പൗരത്വത്തിനുള്ളതല്ല.
- തിരിച്ചറിയൽ ഓൺലൈൻ വഴി ആധികാരികമാക്കുക.
- ഇതു കമ്പ്യൂട്ടർ ഉണ്ടാക്കിയ കത്താണ്.

നിങ്ങളുടെ ആധാർ നമ്പർ/ Your Aadhaar No.:

INFORMATION

- Aadhaar is proof of identity, not of citizenship.
- To establish identity, authenticate online.
- This is electronically generated letter.

Signature valid

ആധാർ - സാധാരണക്കാരന്റെ അവകാശം

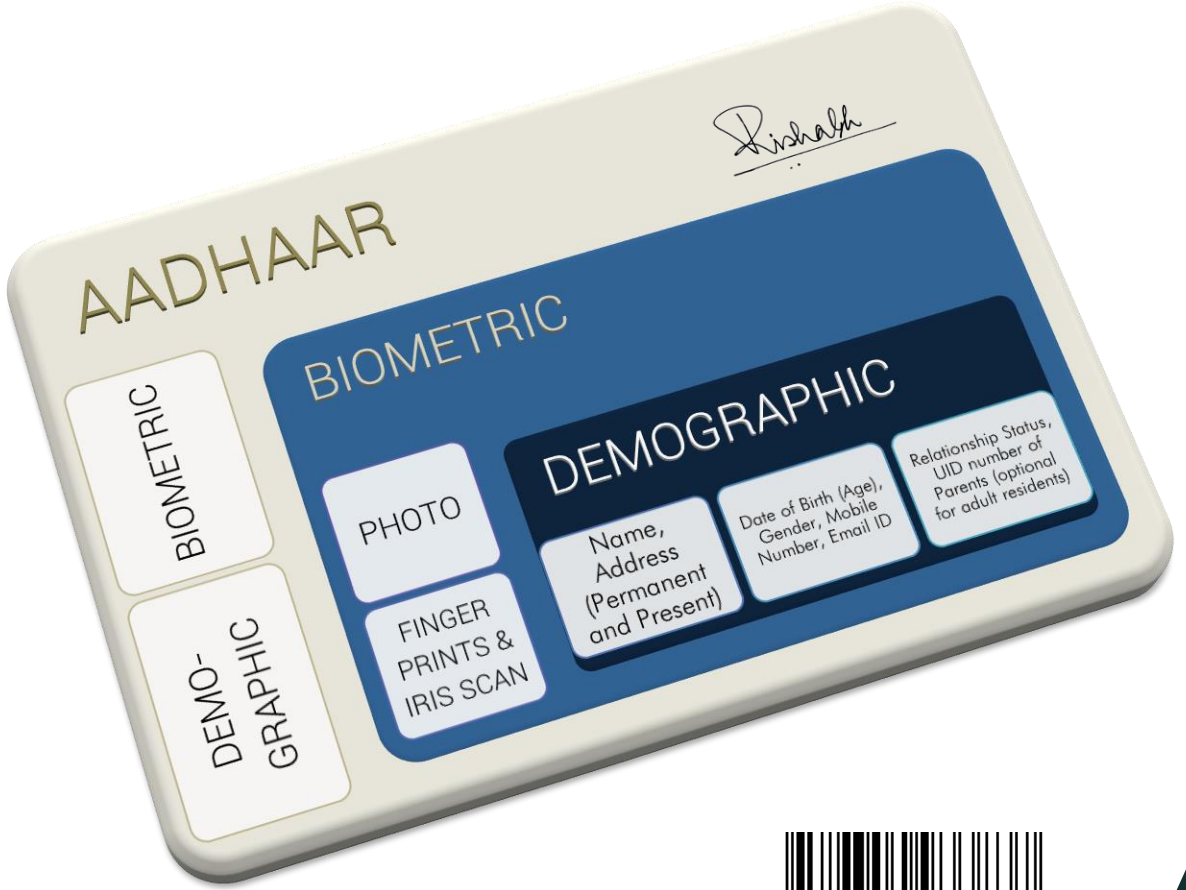
- ആധാർ രാജ്യത്തുടനീളം അംഗീകാരമുള്ളതാകുന്നു
- ആധാർ ഒരു തവണ മാത്രം പേരുചേർക്കുക
- തെയായി നിങ്ങളുടെ മൊബൈൽ നമ്പറും ഇമെയിൽ അഡ്രസ്സും പുതുക്കുക ഇതു ഭാവിയിൽ വിവിധ തരം സേവനങ്ങൾ ലഭ്യമാക്കാൻ നിങ്ങളെ സഹായിക്കും

- Aadhaar is valid throughout the country.
- You need to enrol only once for Aadhaar.
- Please update your mobile number and e-mail address. This will help you to avail various services in future.

भारत सरकार GOVERNMENT OF INDIA

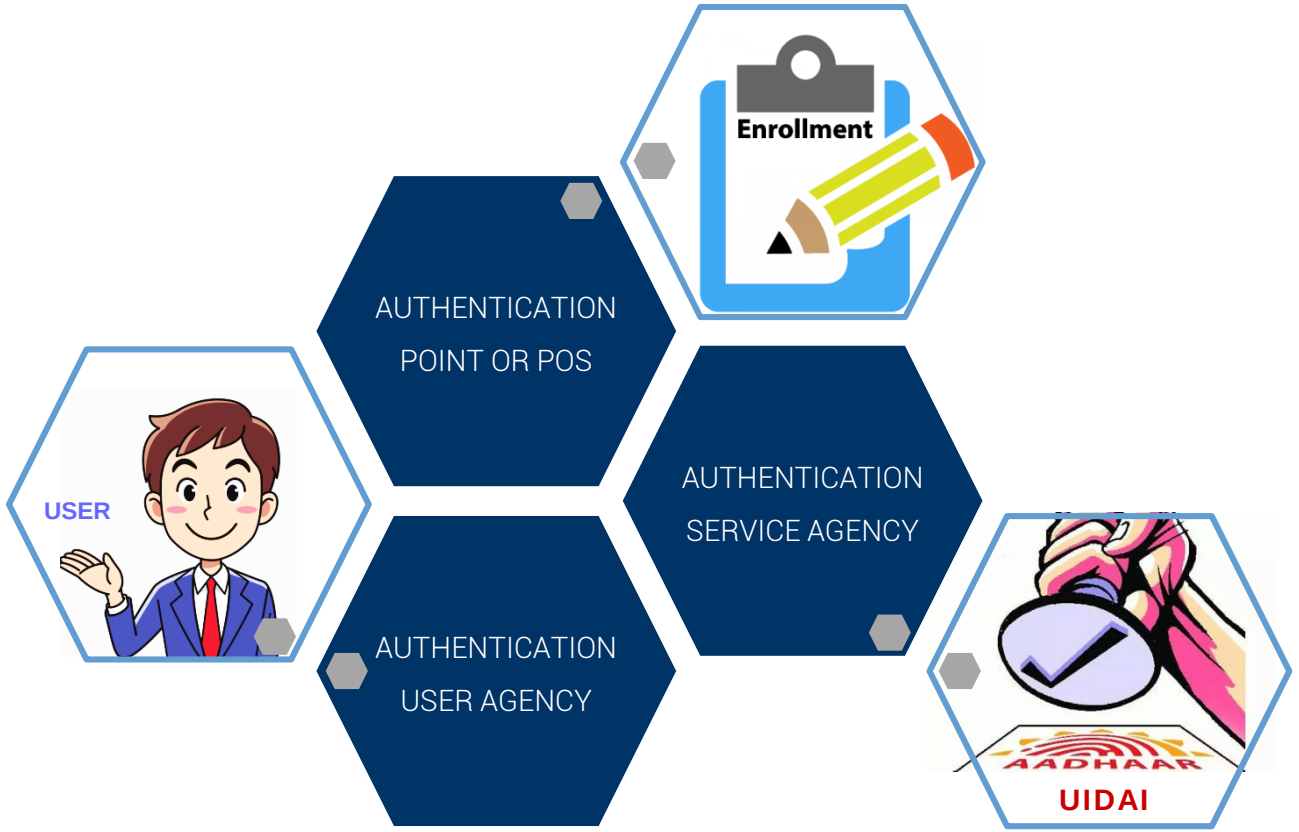
भारतीय विशिष्ट पहचान प्राधिकरण UNIQUE IDENTIFICATION AUTHORITY OF INDIA

ആധാർ - സാധാരണക്കാരന്റെ അവകാശം Aadhaar - Aam Aadmi ka Adhikar



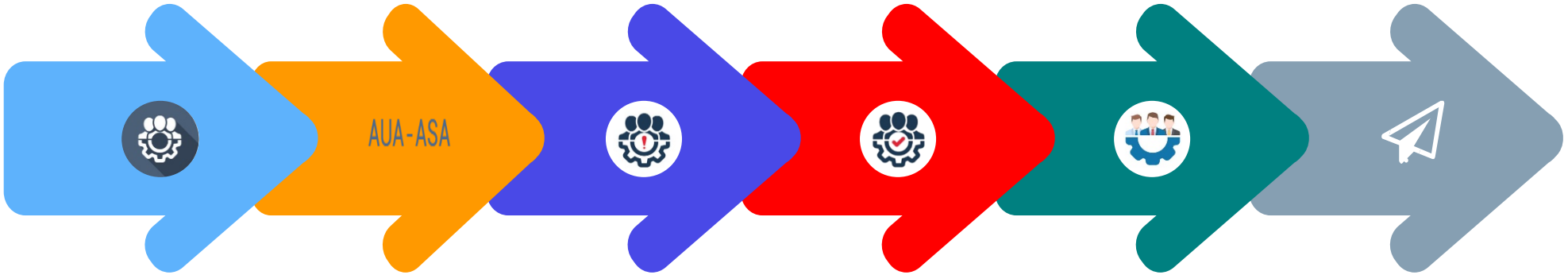
9 789354 933837

UIDAI Ecosystem



9 789354 933837

Process of Authentication



01
Authentication Request

02
AUA/ASA Specific Communication Protocol

03
YES/NO Response

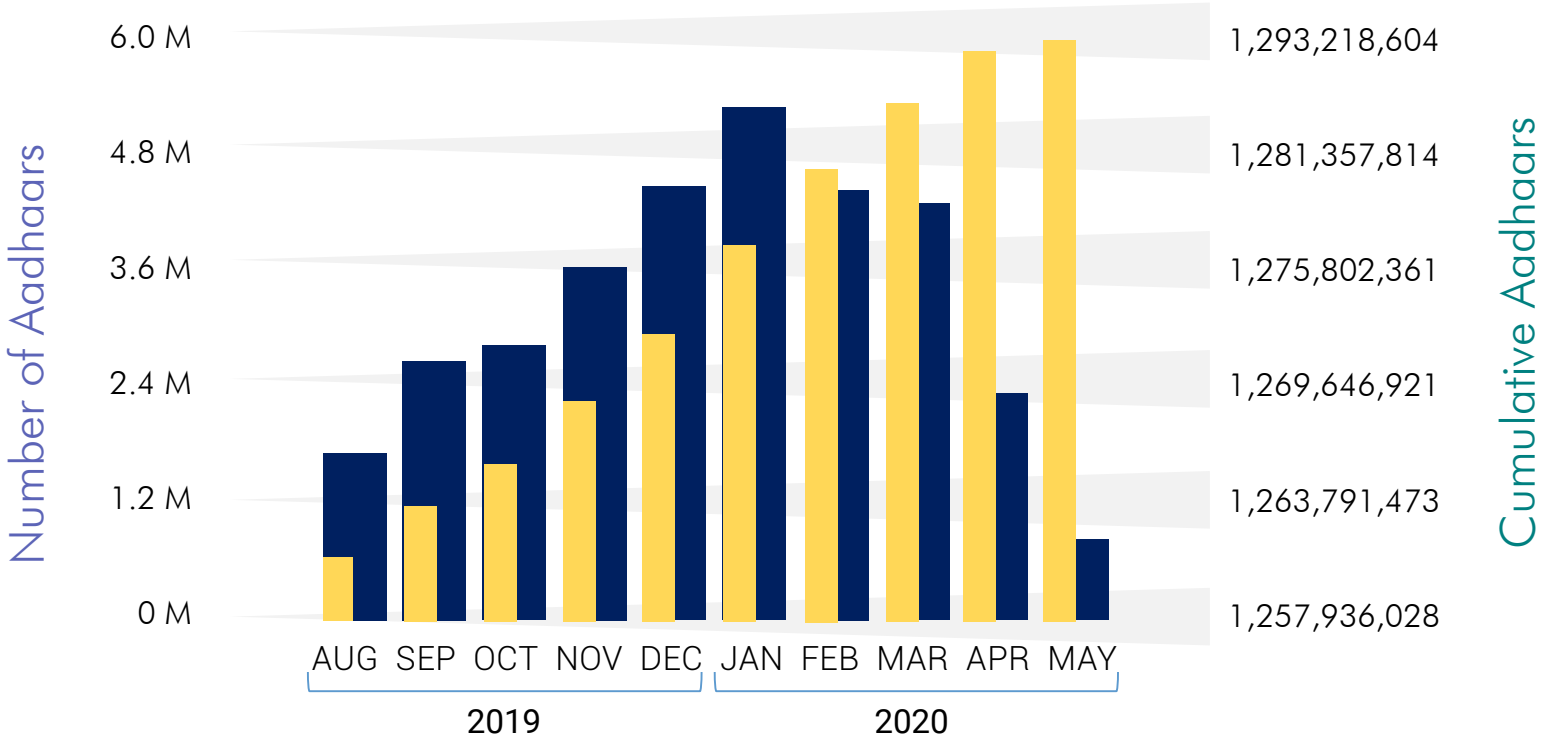
04
Necessary Updates & Confirmation

05
Service delivered

06
Aadhaar Issued

9 789354 933837

Number of UID Generated



9 789354 933837

Saturation Level of UID

Total Population (Projected 2021)
1,392,012,604

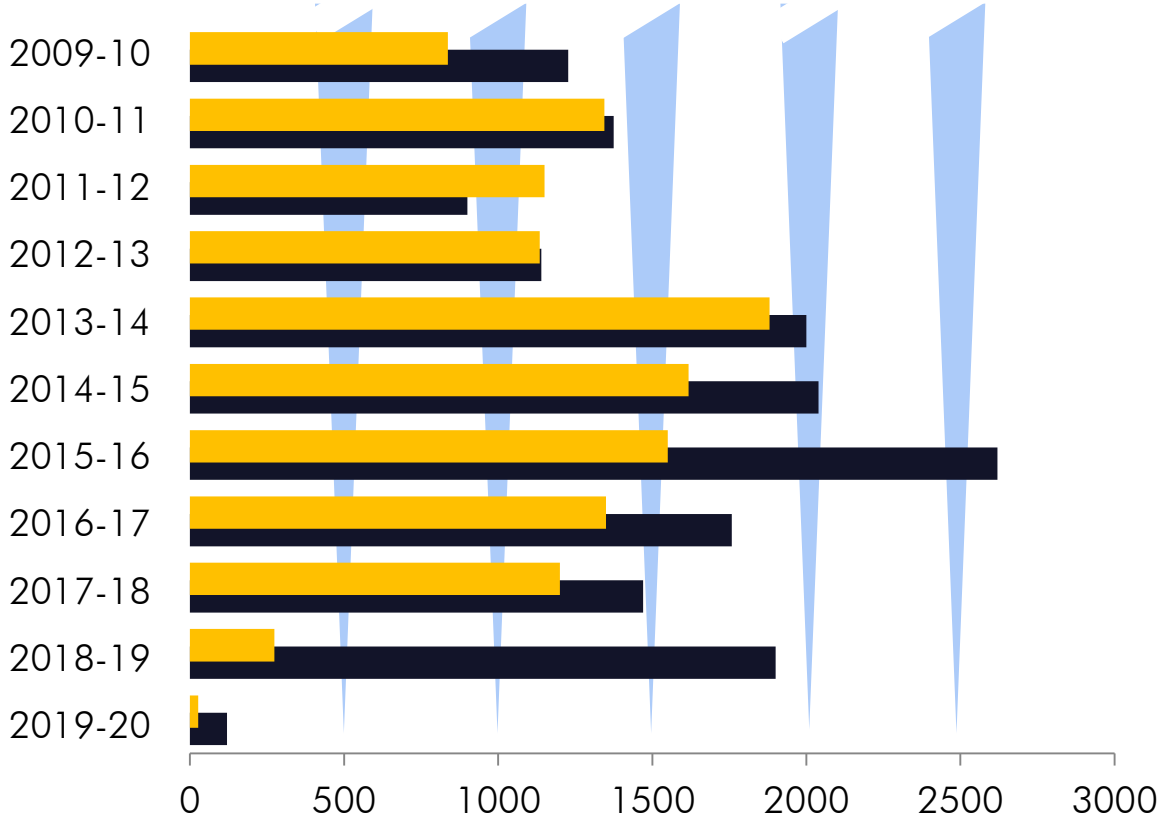
Saturation Percentage
92.90%

Number of Aadhaar Issued
1,293,218,604

Having No Identity
98,794,000 = 7.10%

9 789354 933837

UIDAI Budget & Expenditure (in Crores)



9 789354 933837

UIDAI: Aims & Achievements

UID Number (Aadhaar) was aimed to:

- ✓ achieve social inclusion with more efficient public and private service delivery;
- ✓ reduce the large number of fake / duplicate identities; and
- ✓ to pave the way for direct benefit transfers.

As on 2021-May-22

- ✓ 1,293,218,604 users have been enrolled.
- ✓ A total expenditure of INR 12,962.02 crores have been incurred over the last 12 years [UIDAI 2021].

9 789354 933837

Security Issues

- ✓ UIDAI admitted that 210 government websites unveiled the Aadhaar details on internet [Garg, 2020].
- ✓ Almost 130 million Aadhar numbers, with other sensitive details, are available on internet [First Post, 2020].
- ✓ Jharkhand Directorate of Social Security leaked Aadhaar details of 1.6 million people due to technical glitch.
- ✓ UIDAI banned about 1,000 operators and filed FIRs against 20 individuals for dereliction.
- ✓ Nearly 4.5 billion data records were stolen, or negotiated worldwide during Jan-Jul 2018 (Breach Level Index).

9 789354 933837

Privacy Concerns

- ✓ In other countries, the Information privacy is protected by comprehensive data protection laws:
  - US Privacy Act, 1974;
  - UK Data Protection Act, 1998; and
  - US Computer Matching and Privacy Act, 1988
- ✓ In India, there is no clear legislative or juridical understanding regarding privacy of information.
- ✓ The Supreme Court has derived the right to privacy from Articles 19(1)(a) and Article 21 of the Constitution to desist service providers to make Aadhaar mandatory.

9 789354 933837

Violations

✓ Despite Court's verdict, Government has made Aadhaar compulsory in:

Since Aadhaar inherently carries a lot of personal and private information, it eventually defies the data privacy.

9 789354 933837

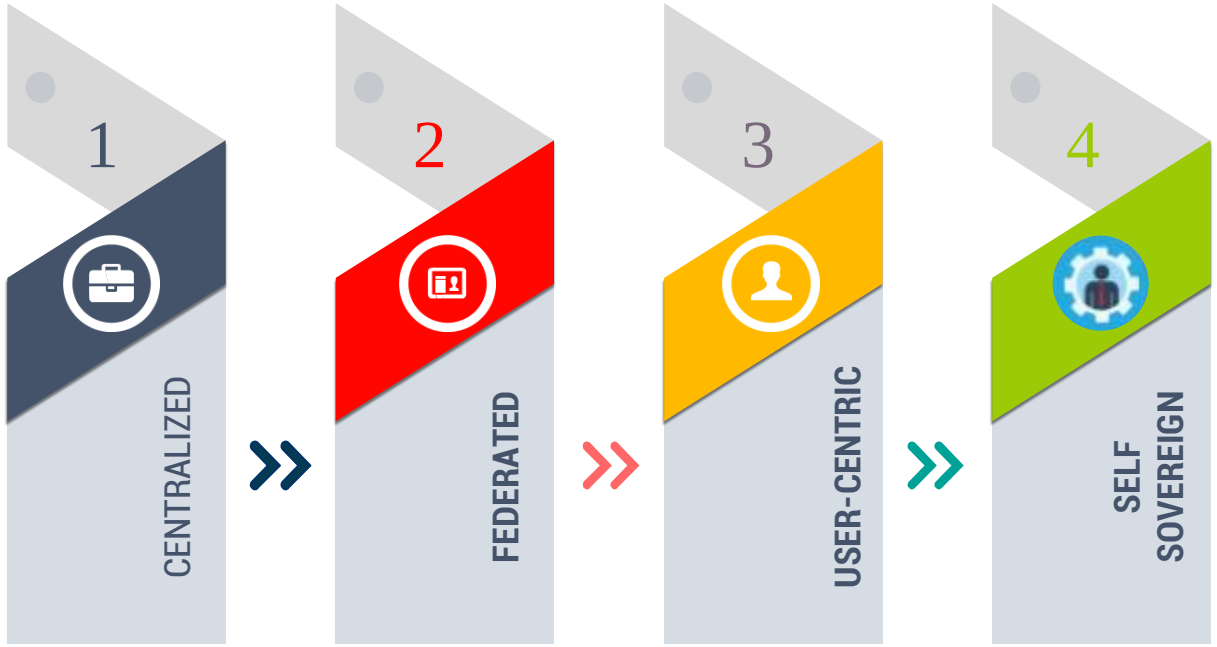
It is not a Failure?

- ✓ Despite an expenditure of ≥12,962 Cr INR, 98 million marginalized residents, who are in dire need of access to limited benefits provided by the State, are still living dispossessed [Garg, 2021].
- ✓ Aadhaar, which was imagined as a general proof of identity and address could not hold ground because various existing forms of identity still continue.
- ✓ The use of biometrics has numerous drawbacks. It is inherently fallible for large scale and the results are often probabilistic.
- ✓ Linking of Aadhaar to social schemes has ironically created more barriers for the poor and deprived.
- ✓ In Sep 2013, the Supreme Court of India challenged the constitutional validity of Aadhaar. In light of the Court's verdict, Aadhaar lost its ground.

9 789354 933837

Now, What's the Way-out?

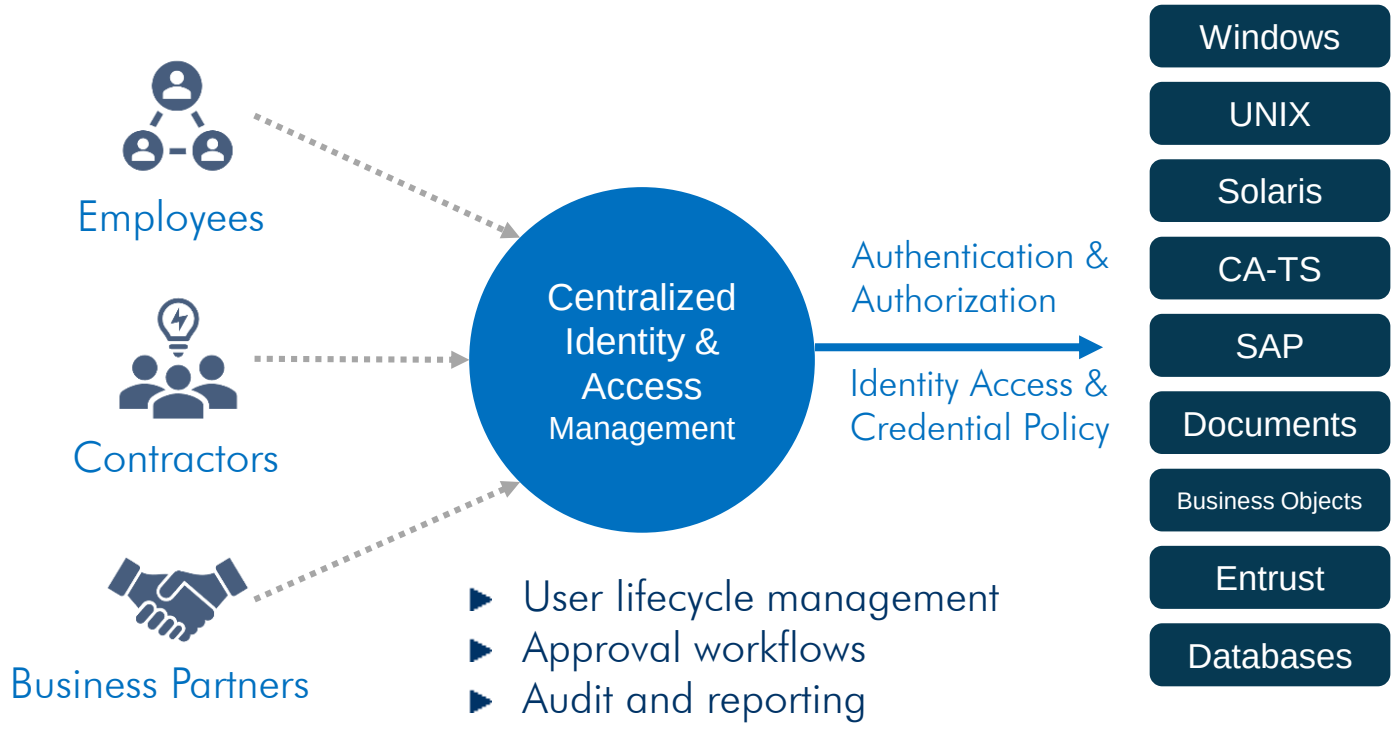
- ✓ In order to have secure and private identity, the only solution is digitization.
- ✓ Over the years, the online identity have advanced through four major stages:



9 789354 933837

Centralized Identity

✓ Controlled by a single authority, each user needs a new digital identity credential for every new organization.



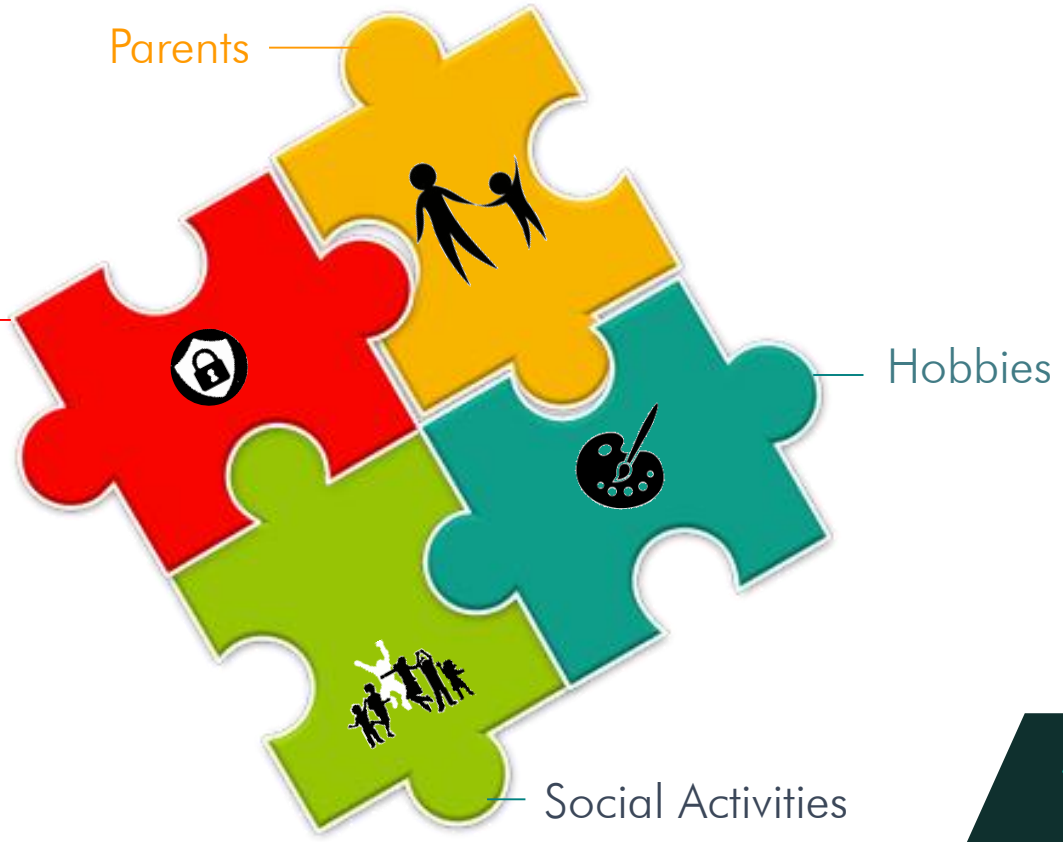
9 789354 933837

Federated Identity

- ✓ Controlled by multiple federated authorities, which allow users to utilize the same identity on multiple sites.

User-centric Identity

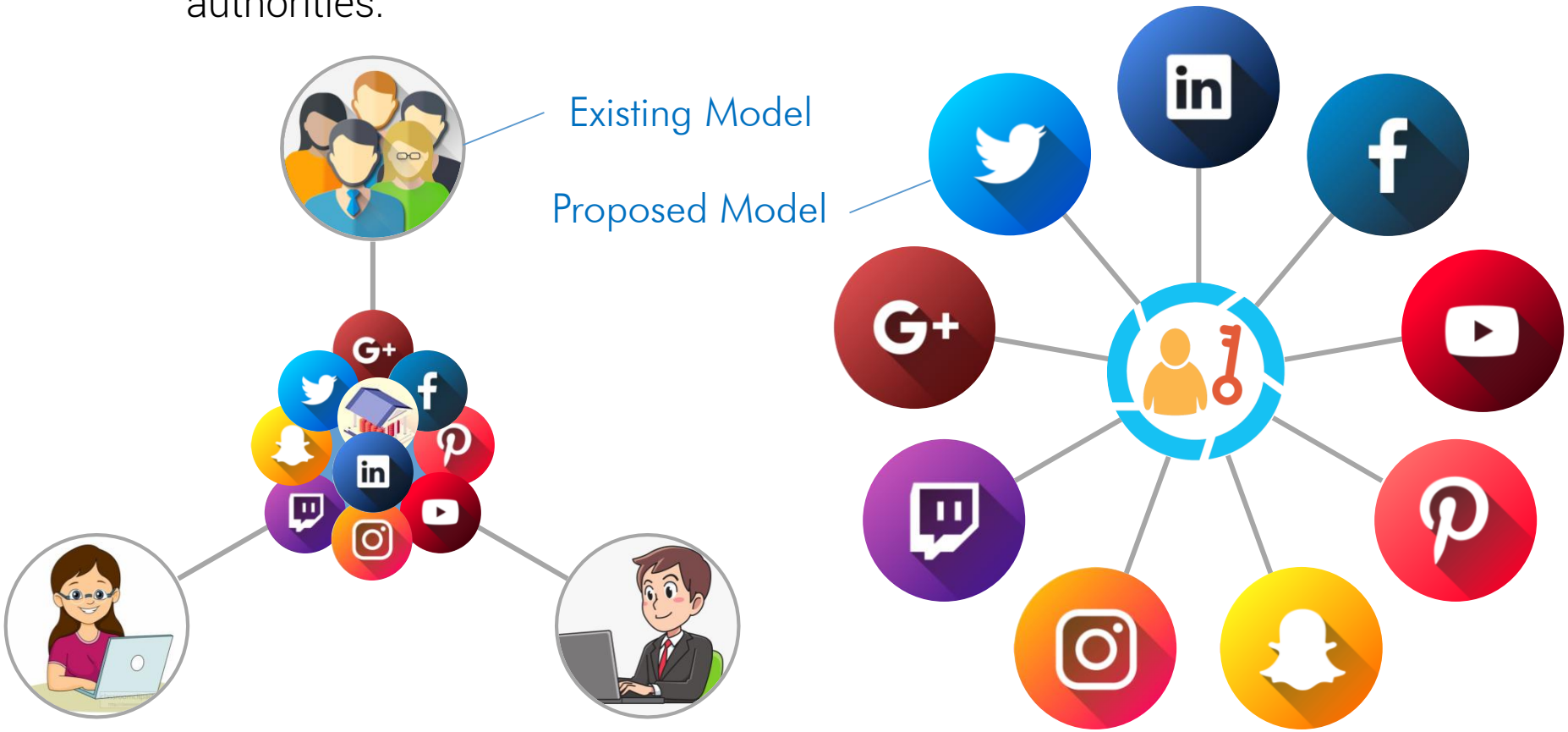
- ✓ Controlled by an individual, across multiple authorities, without requiring a federation.
- ✓ A user can theoretically register his own Open ID, for private but lawful activities, which he can use autonomously.



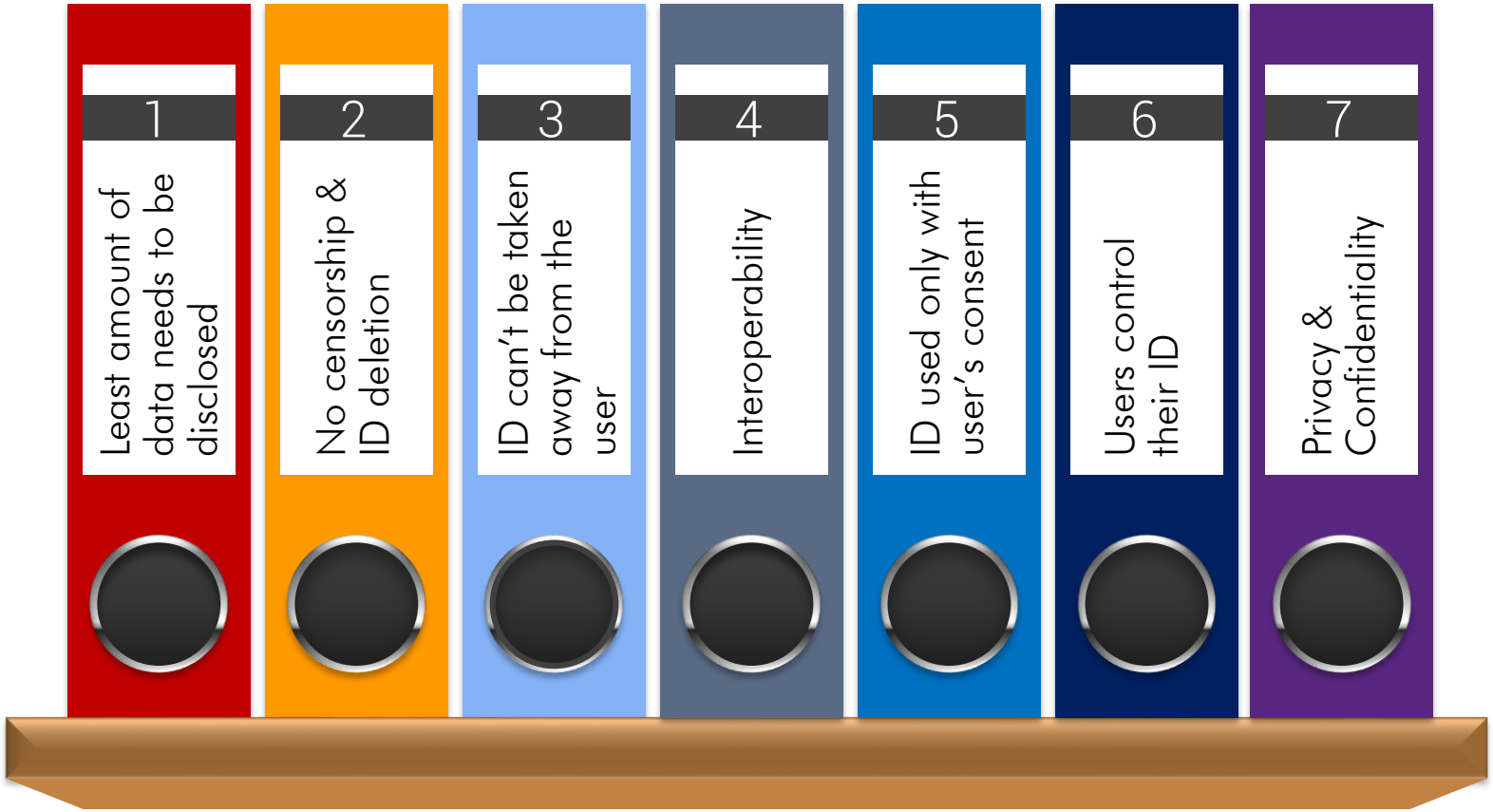
9 789354 933837

Self-Sovereign Identity

- ✓ The user is central to the administration of identity, across any number of authorities.



Characteristics of Self-Sovereign Identity



How can SSI become a reality?

- ✓ Identity meta-data can be hashed and stored on a chain-code.
- ✓ Information could be available when and when people need it.
- ✓ Identity data can be safely & securely recorded and accessed by authorized parties.
- ✓ Trusted partners would provide a secure and immutable network for creating opportunities for the bottom of the pyramid.
- ✓ A distributed ledger across a trust network would prove helpful during critical life events & civic crisis like COVID-19.

But, what is it .....?

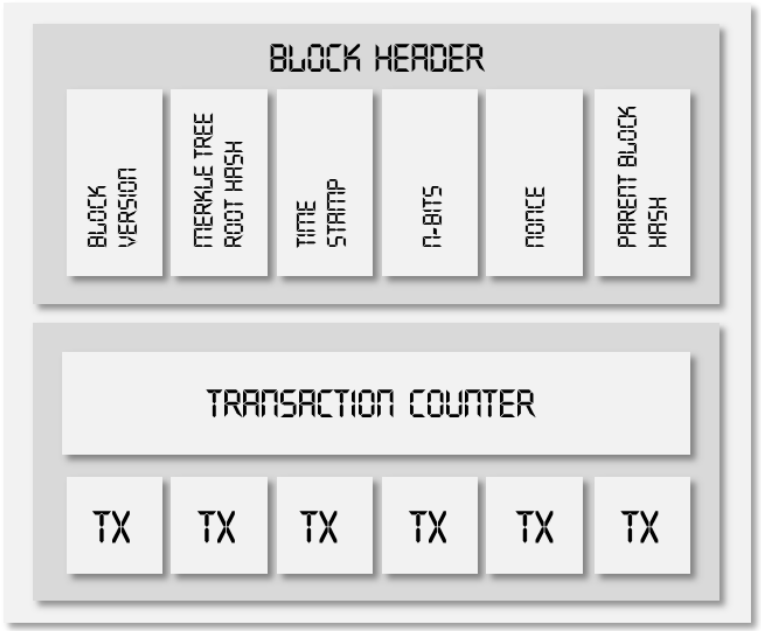
9 789354 933837

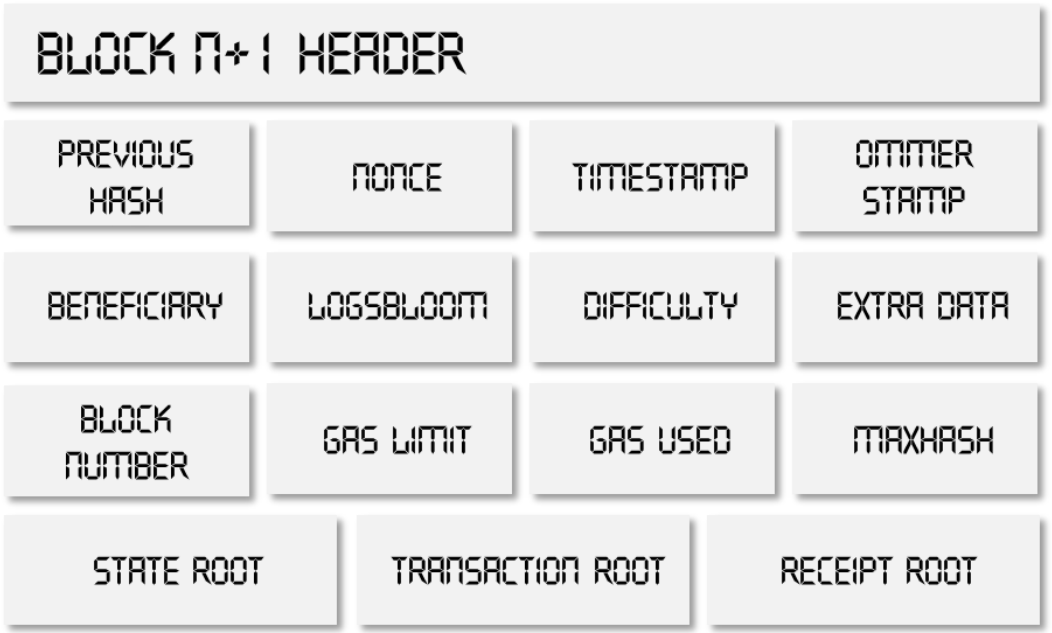
……. It's Blockchain

- ✓ The term blockchain is commonly used to refer to a public or permission-less distributed ledger.
- ✓ The blockchain, that maintains a continuously growing list of records or transactions, provides ledger and smart contract (chain-code) services to applications.
- ✓ In a decentralized identity framework, security becomes the responsibility of the user, who may determine his or her own security measures.
- ✓ Block-chain powered decentralized identity solutions compel hackers to target discrete data stores, which is expensive and cumbersome.

9 789354 933837

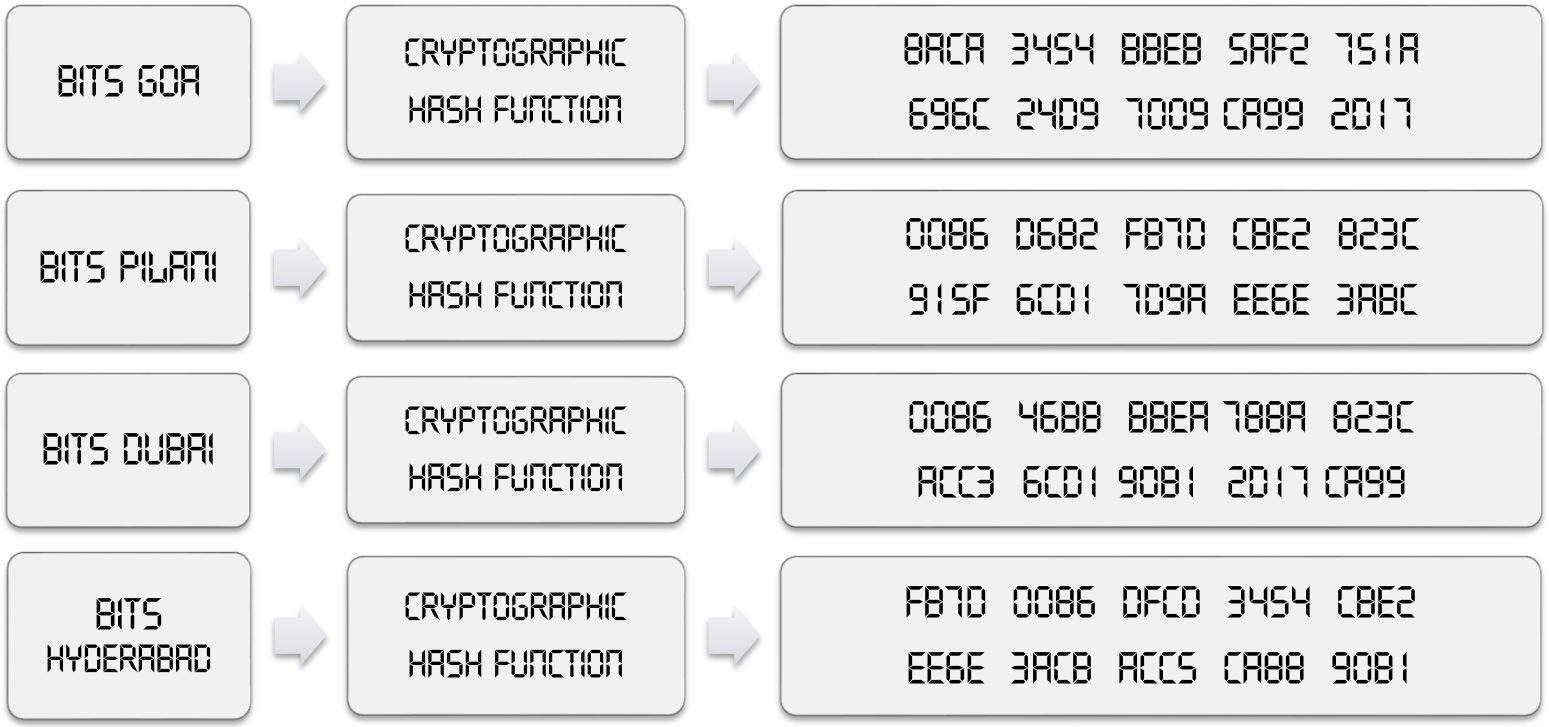
Block : Its Components





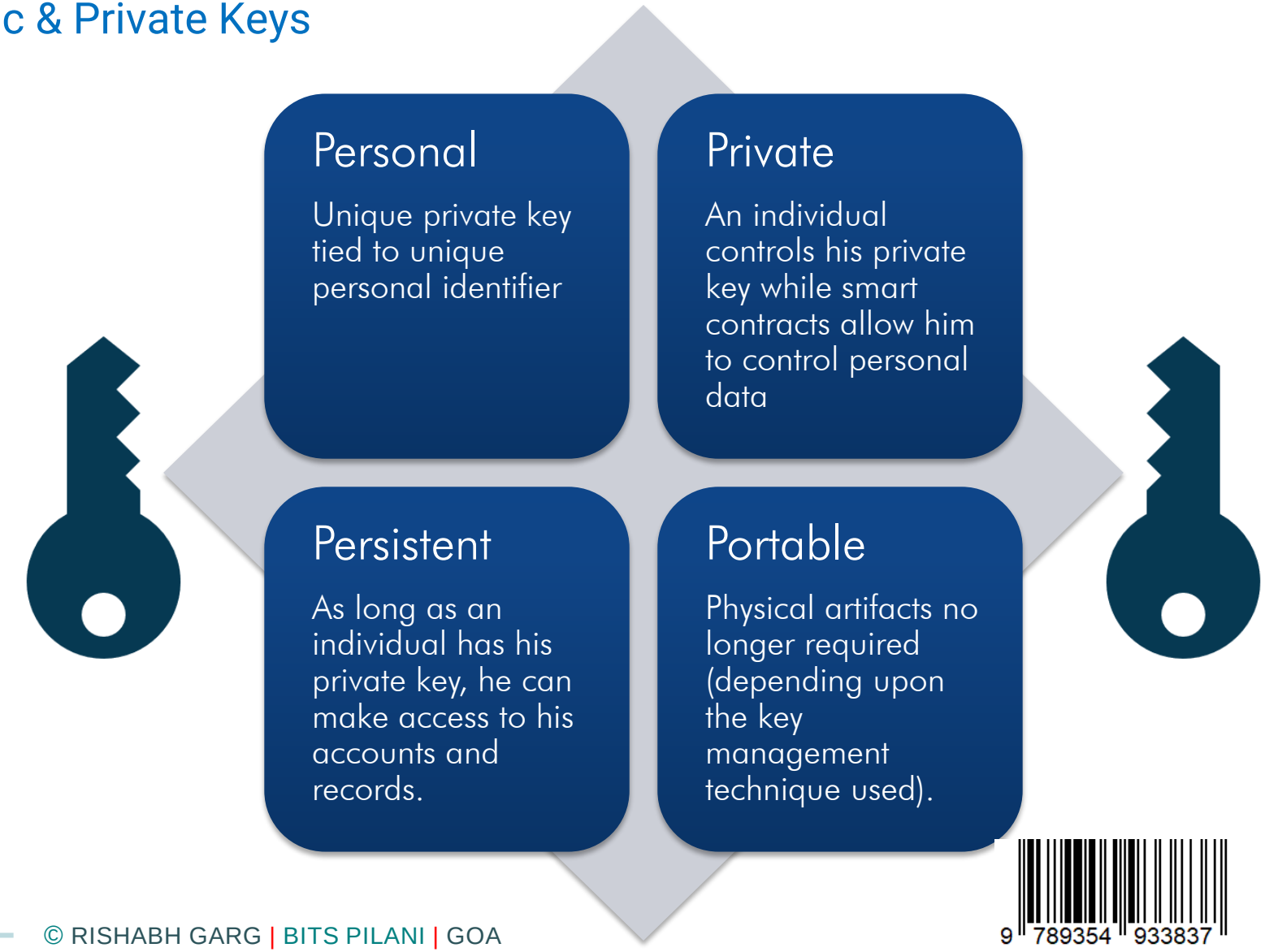
9 789354 933837

Hash as a Mathematical Algorithm



9 789354 933837

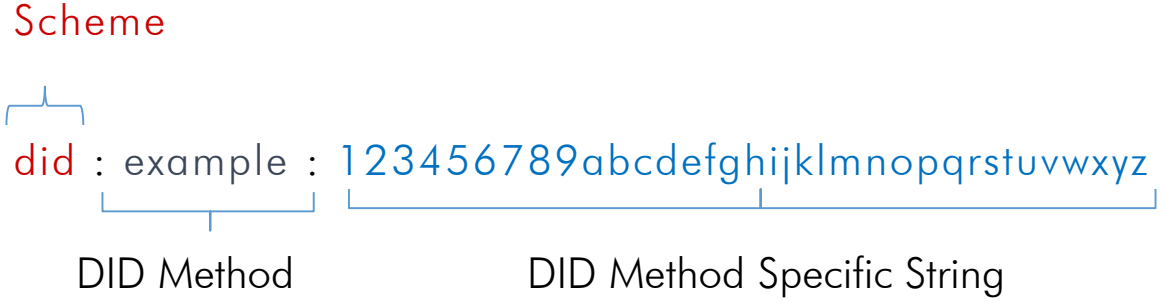
Public & Private Keys



9 789354 933837

Decentralized Identifiers (DID)

- ✓ Recent advancements in block-chain technology allow every public key to have its own address, which is known as DID.
- ✓ A DID is stored on the public ledger along with DID document containing the public key, any specific credentials, which the identity owner wishes to share, and the network addresses for interaction.



9 789354 933837

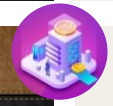
Evolution of Blockchain

2009-11

- Satoshi Nakamoto released Bitcoin paper
- The 1st Bitcoin online purchase BTC 10,000 taken place

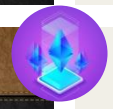
2012-14

- Ethereum released
- Blockchain technology R3; Ripple blockchain introduced



2015-17

- Linux Foundation introduced Hyper-ledger
- JP Morgan launched Quorum blockchain



2018

- 15% financial companies used blockchain
- 95% of companies willing to invest in blockchain

2019

- Blockchain as a service industry started flourishing
- Security Tokens replaced ICOs

2020

- Introduced the concept of GlobalID leveraging Blockchain Technology (Rishabh Garg, 2020).

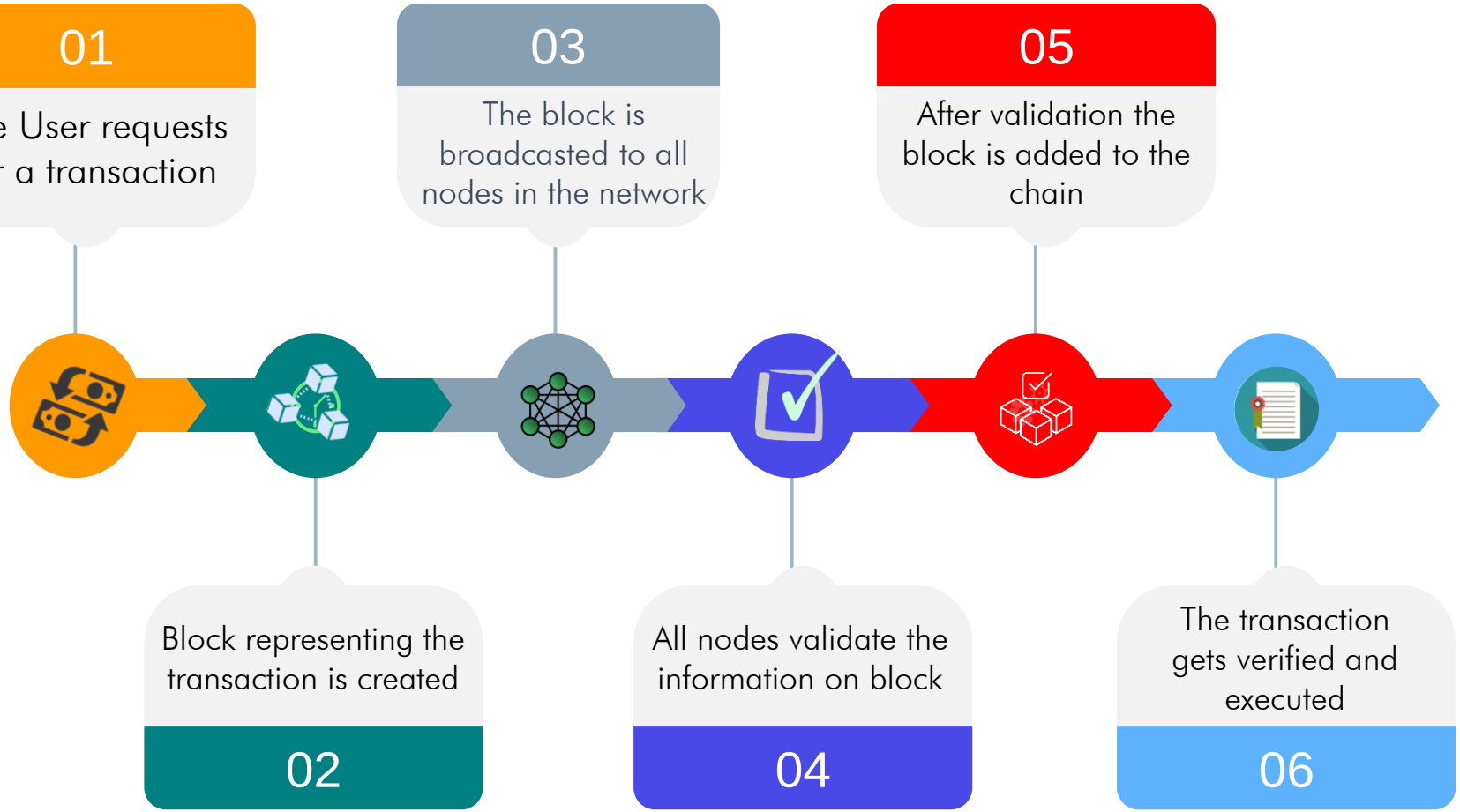
Blockchain Models

Based on its applications, blockchain is delineated as Blockchain 1.0, 2.0 and 3.0.

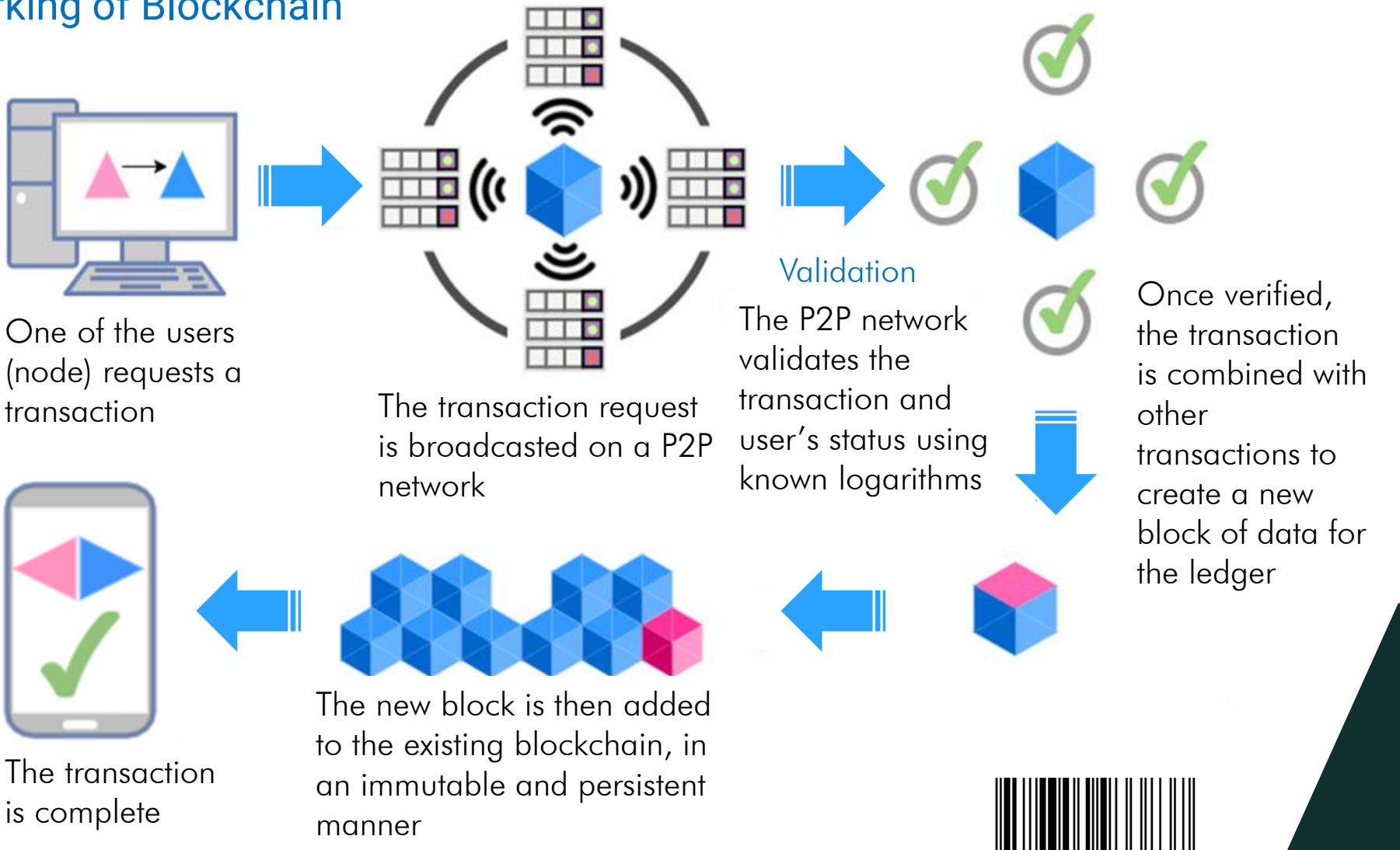
- ✓ Blockchain 1.0 was restricted to cryptocurrency (bitcoin), for small payments, foreign exchange and money laundering.
- ✓ Blockchain 2.0 comprised smart-contracts, decentralized applications for banking, stock trading, credit system, supply-chain management, payment clearing, etc.
- ✓ Blockchain 3.0 is suitable for areas like education, health, science, transportation, logistics and finance.

9 789354 933837

Working of Blockchain



Working of Blockchain



One of the users (node) requests a transaction

The transaction request is broadcasted on a P2P network

Validation

The P2P network validates the transaction and user's status using known logarithms

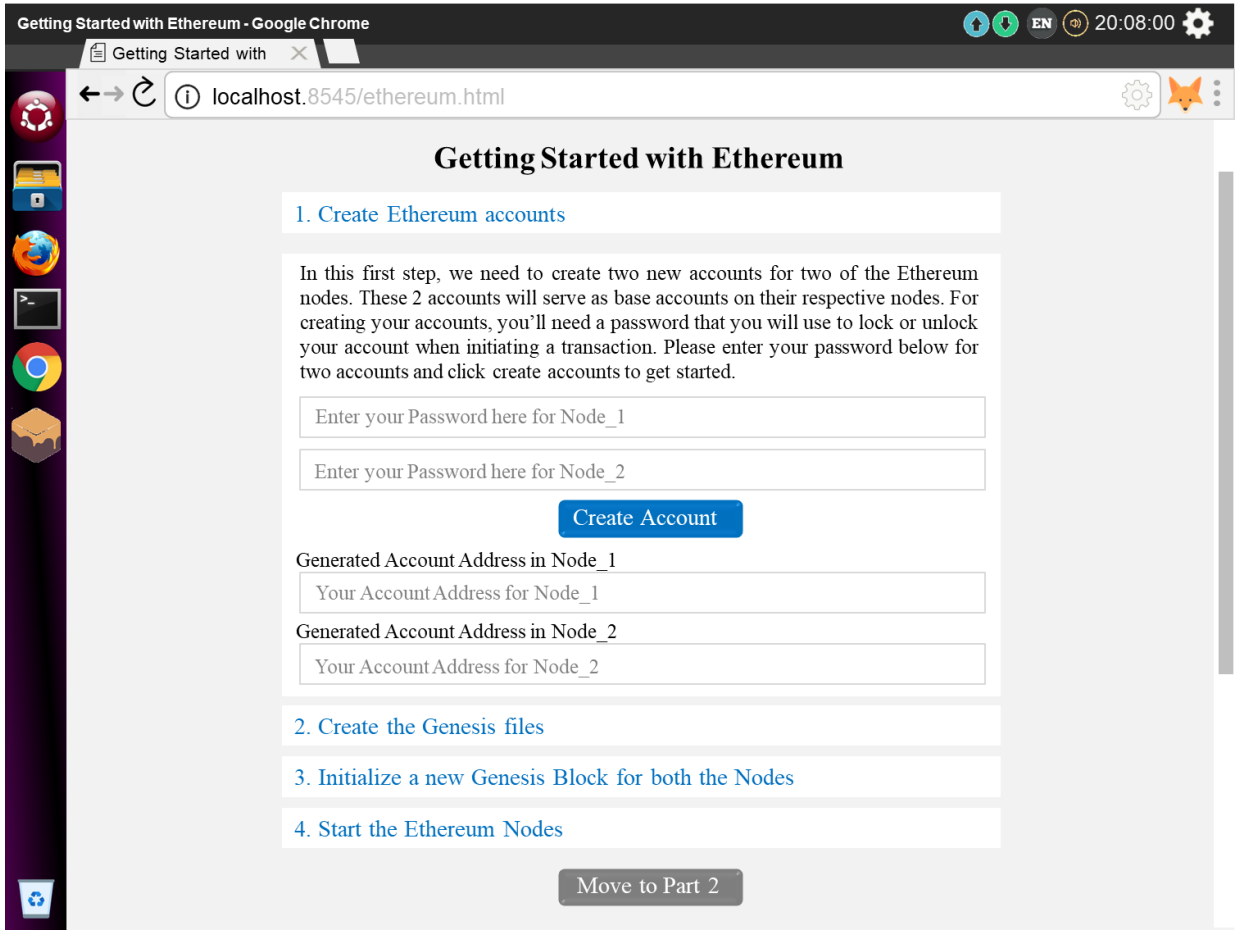
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger

The new block is then added to the existing blockchain, in an immutable and persistent manner

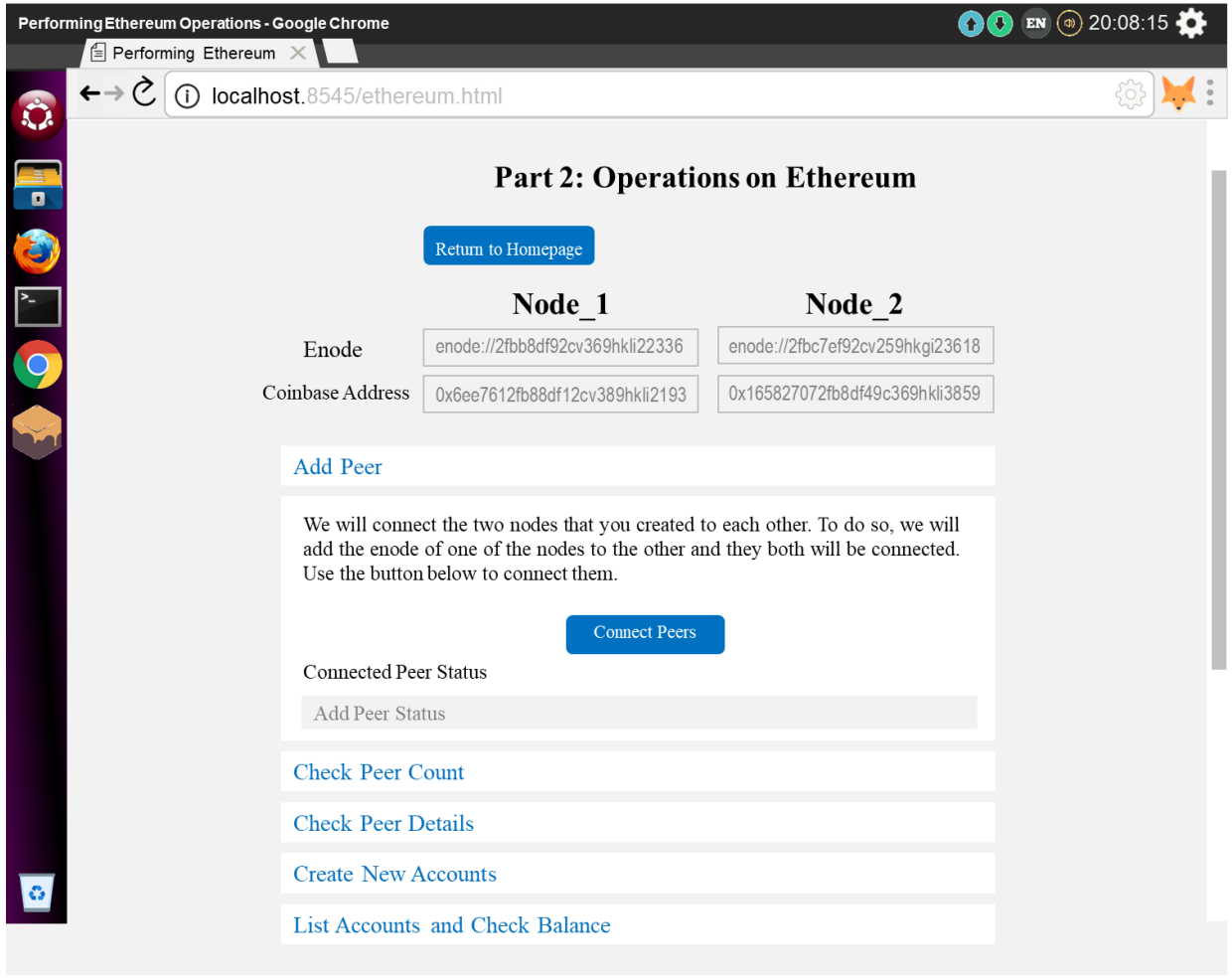
The transaction is complete

9 789354 933837

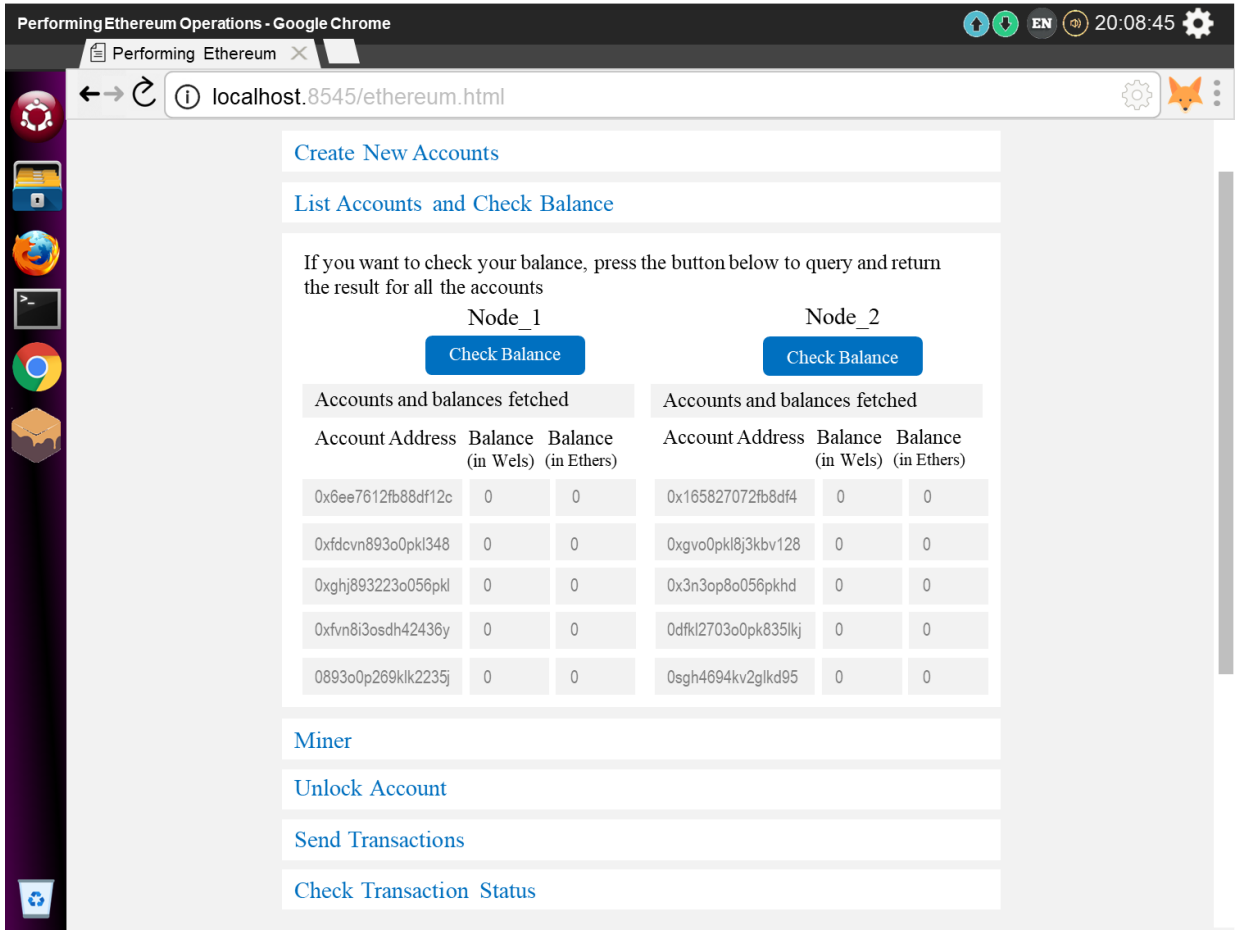
Creating Blockchain Account



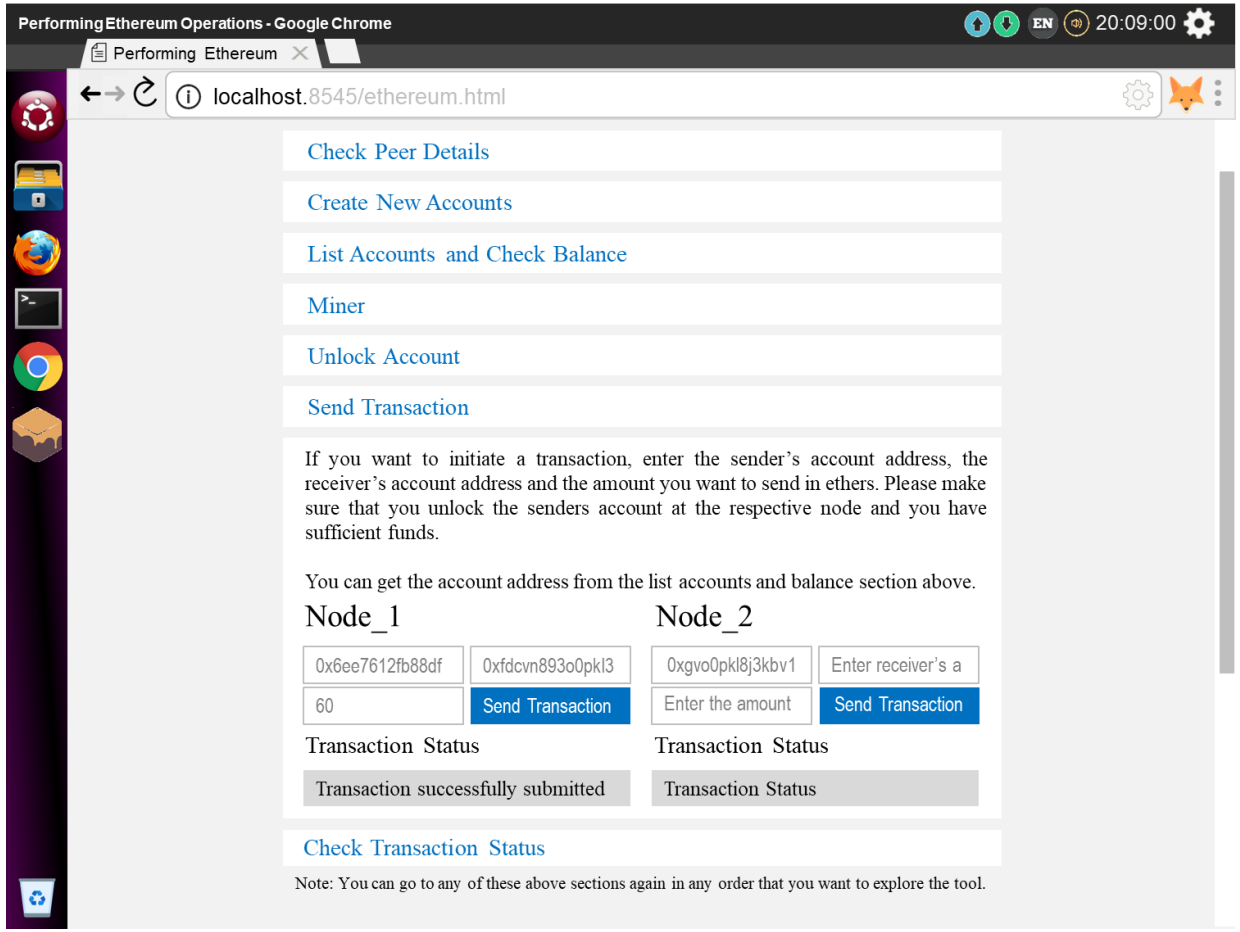
Adding Peers to Blockchain



Checking Accounts



Performing Ethereum Operations



Input & Output UTXOs References

Blockchain.com Wallet Exchange Explorer Buy Bitcoin Trade

Inputs 0

HEX ASM

Index	0	Details	Output
Address	1AKEnMqiDihdpMmSYX1Q9KGxVScfghjMh	Value	0.17396625 BTC
Pkscript	OP_DUP OP_HASH160 662c1fc19cc2bba73988cfc907549f589c369961 OP_EQUALVERIFY OP_CHECKSIG		
Sigscript	3054022100ac3ff1ca25ed15bfd5ac0e1417affcfgh456fjgdfb56g529j7612g4t'pukt564ytugewfdffghj542fdsafs2085001 02379c8ba33e7fe5s6g4hjty21khkftyd5410a2523		
Witness	N/A		

Outputs

Index	0	Details	Unspent
Address	3N1m2P85yGXUQM2drHS5gaYrQu8h351Cdy	Value	0.05835490 BTC
Pkscript	OP_DUP OP_HASH160 deedfb4ac67184f1ab8ea28dde06a1c53491a87 OP_EQUALVERIFY OP_CHECKSIG		

9 789354 933837

Advantages of Blockchain IAM

Typical IAM	Comparative characters	Blockchain IAM
Honeypots - treasure of information is likely to be attacked by hackers		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.		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.	Centralization 	Transactions are immutable by nature, they can be used to both store and retrieve data that needs to be regulated by various compliance standards.

Key characteristics of Blockchain

DISTRIBUTED

A group of nodes, or servers maintain the entries without any central authority.

PERMISSIONED

In a permissioned blockchain, only appointed nodes are authorized to validate transactions.

SECURE

The database is immutable and irreversible. Transactions, once made cannot be revised or tampered with.

TRUSTED

Distributed nature of the network requires half of the computer nodes to reach a consensus, to enable transaction to occur.

AUTOMATED

Transactions occur automatically; the conflicting or double transactions do not occur.

9 789354 933837

Comparisons among different 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 a 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 large number of nodes on public blockchain network).	High (with fewer validators, the system is more efficient).	High (with fewer validators, the system is more efficient).

Comparisons among Typical Consensus Algorithms

Property	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Node identity management	Open	Open	Permissioned	Open	Open	Permissioned
Energy saving	No	Partial	Yes	Partial	Yes	Yes
Tolerated power Of adversary	<25% computing power	<51% stake	<33.3% faulty replicas	<51% validators	<20% faulty nodes in UNL	<33.3% byzantine voting power
Example	Bitcoin [Nakamoto, 2008]	Peercoin [King & Nadal, 2012]	Hyperledger Fabric [HPL, 2015]	Bitshares	Ripple [Schwartz et.al., 2014]	Tendermint [Kwon, 2014]

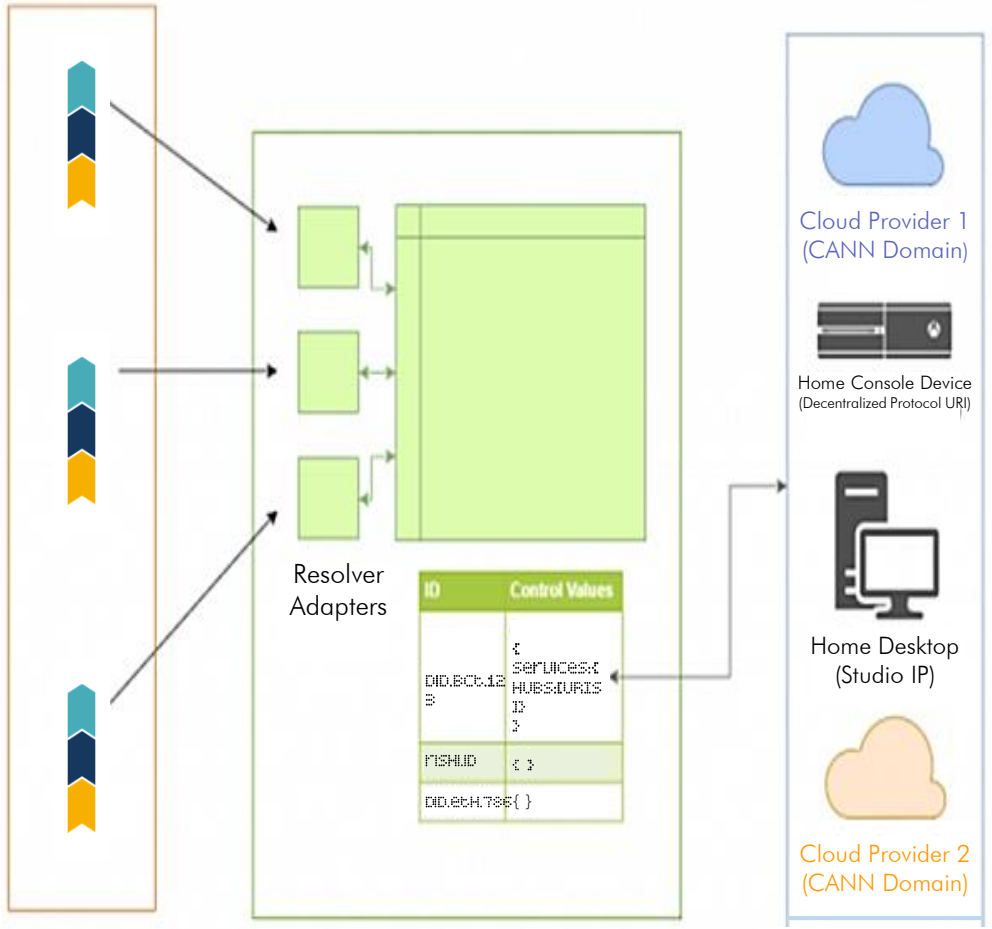
9 789354 933837

Challenges DLT needs to overcome

Privacy Issues	Limited Evidence of Global Impact	Conflict with Traditional Approaches	Data Protection & Security	Uncertain Cyber Regulations	Immature Technology

9 789354 933837

DLT to Record Citizen Data



Devices are associated with Identity Hubs through device specific public keys

App Associated Devices

Master ID
(Private Key)

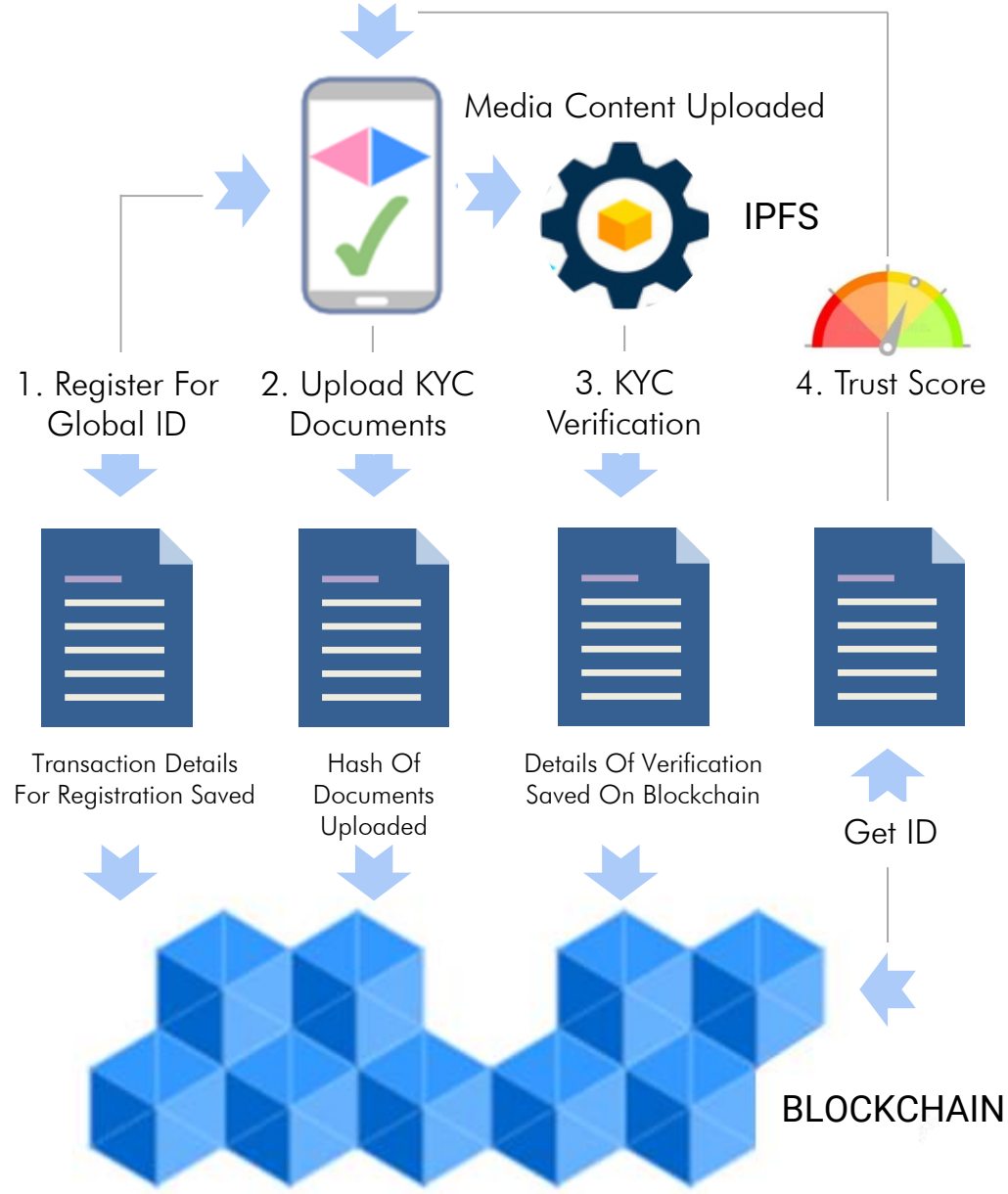
Blockchain

Decentralized Identifier - DID

IPFS

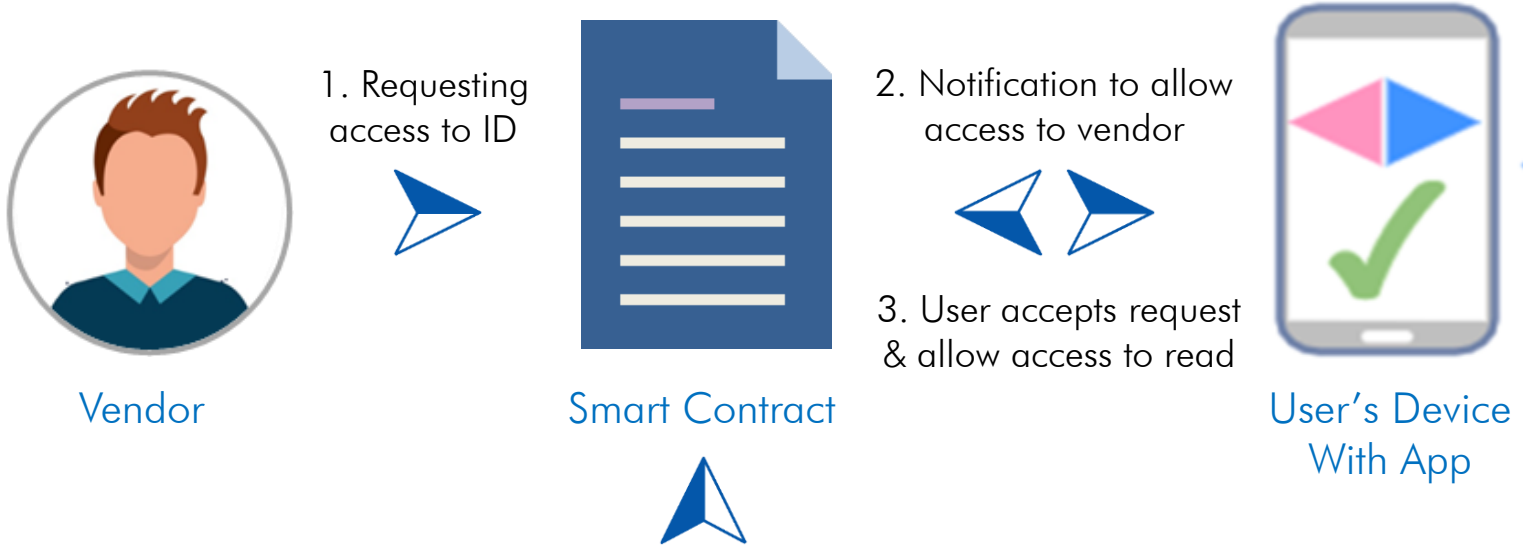
9 789354 933837

Identity Access Management (IAM)



9 789354 933837

Identity Access through Blockchain



9 789354 933837

Functional Mechanism

Step 1: Installation of Mobile App

- ✓ An individual will have to download the mobile app from play store or app store to fetch his identity.
- ✓ 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 which will help organizations to send or to get the access to user's identification documents.

9 789354 933837

Functional Mechanism

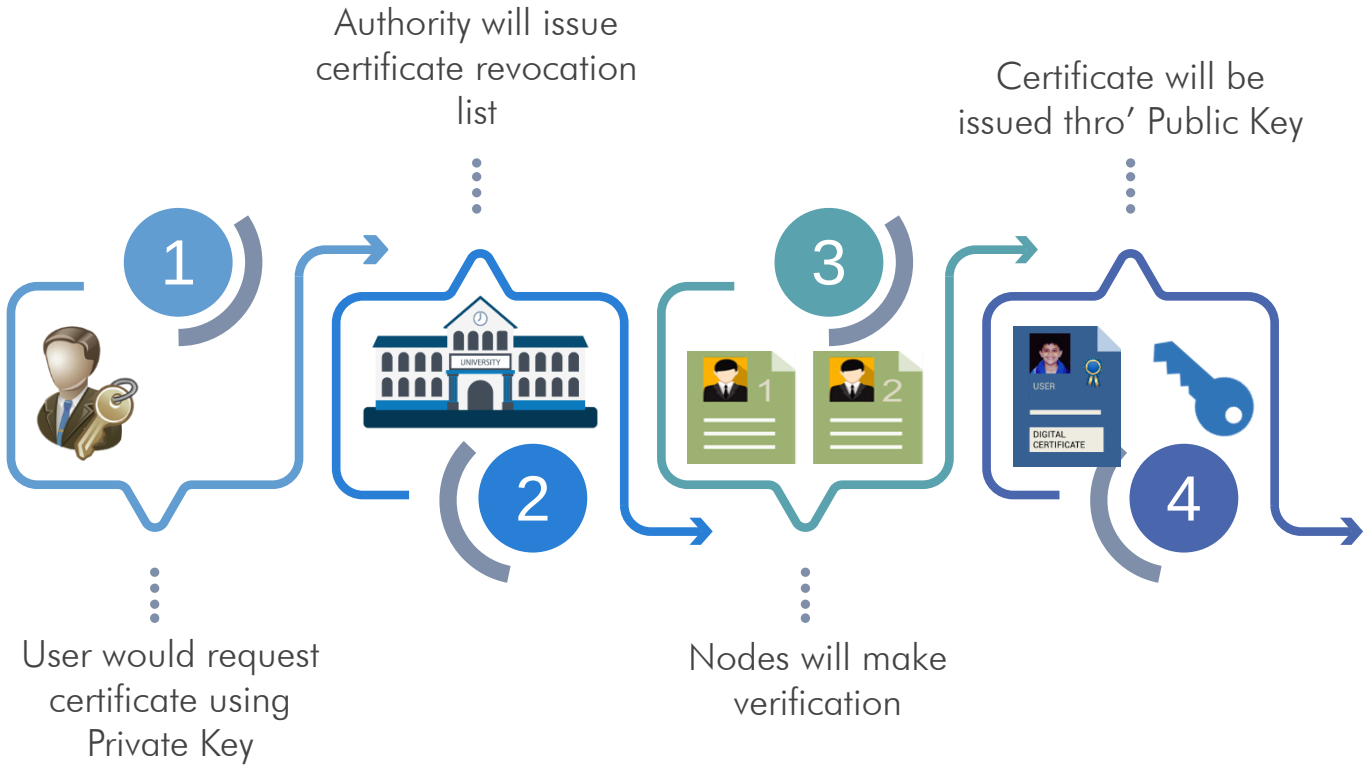
Step 2: Uploading the documents

- ✓ On having the unique ID number, the user will fetch the government issued IDs through the app and save them in the IPFS / Private Ledger.
- ✓ The app will extract the personal information from these ID's.
- ✓ The user will now have the ownership of his own data. It would help users to decide what information is to be shared with organizations?
- ✓ Without the user's consents, no information can be shared with any identity seekers.

9 789354 933837

Functional Mechanism

Issue / Endorsement of Document



9 789354 933837

Functional Mechanism

Step 3: Government or Third-party Access

- ✓ A government organization can send a notification to the user (owning the identity) to make an access to specific details for authentication.
- ✓ The authority 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 any user's data except the transactions made between the identity holder and third-party.

9 789354 933837

Functional Mechanism

Step 4: Trust Score

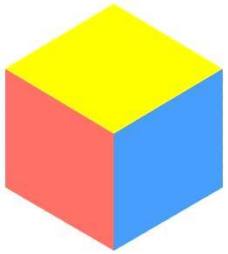
- ✓ Smart contracts can generate a trust score for a user from the information provided by him for creating a self-sovereign identity.
- ✓ Higher the trust score, higher will be the trustworthiness of an individual.
- ✓ This can help organizations validate user's identity on real-time basis.
- ✓ It can save time, money and provide an insight to user's credibility.

9 789354 933837

Generation of Trust Score

Low Trust Score

- 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.



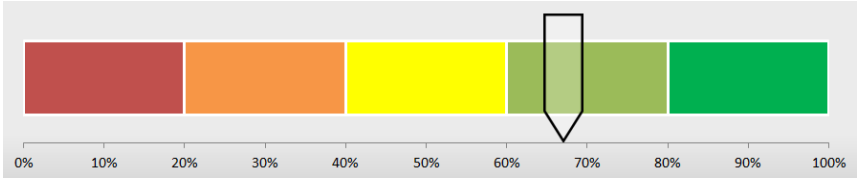
Blockchain

User

High Trust Score

- 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.

Trust Score Scale



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

User Optimized Features of Blockchain

- ✓ Each registered user on Blockchain IAM system will get a UID.
- ✓ UID consists of personal identity information, in encrypted format, stored on his device, backed by IPFS.
- ✓ User can share his UID with any government organization to authenticate himself through the Blockchain IAM.
- ✓ Blockchain IAM system does not store any user's data. It uses Smart Contracts to share the PII, and hence data manipulation is impossible.
- ✓ No transaction can occur without the explicit consent of the user that adds security to IAM.

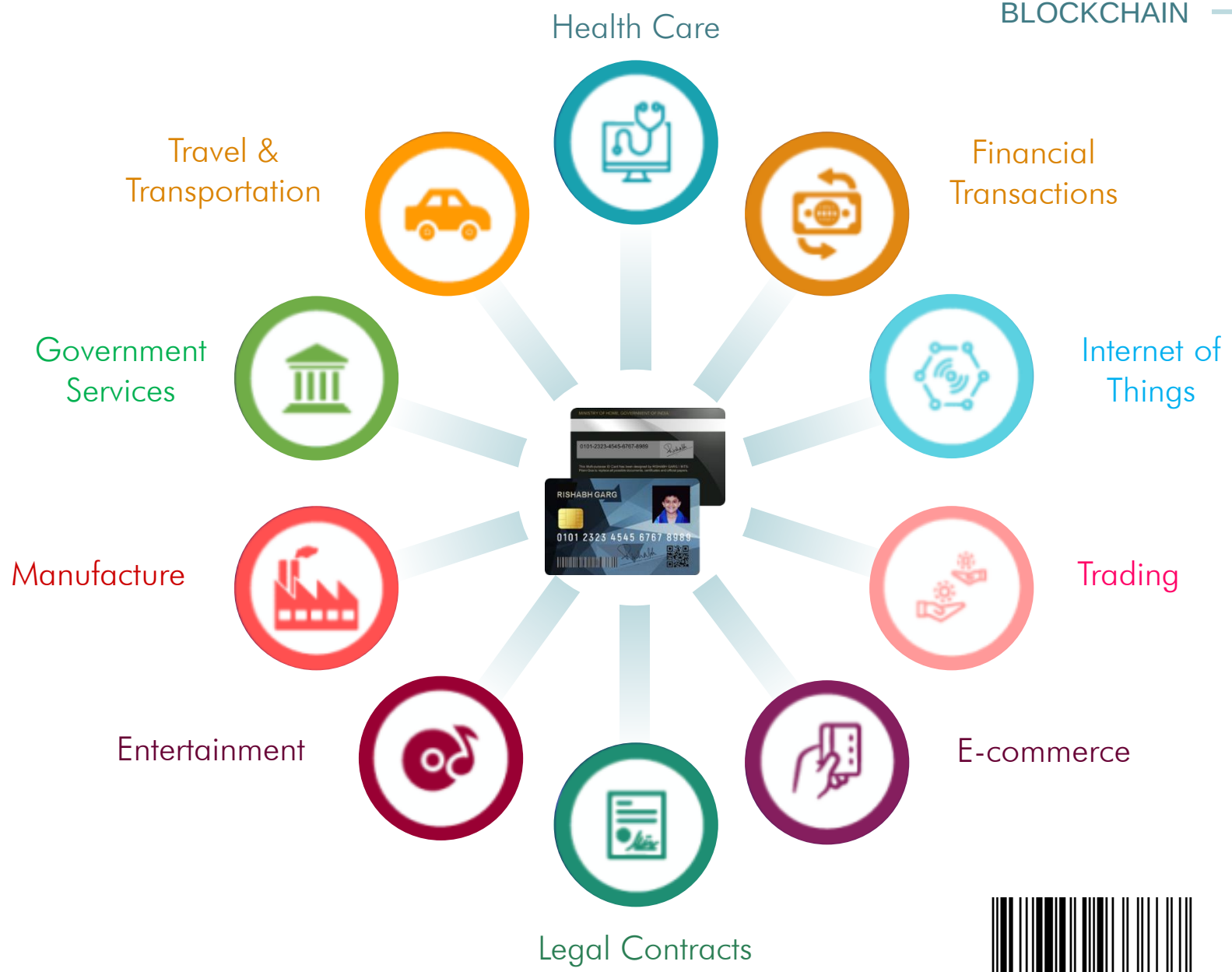
9 789354 933837

User Optimized Features …….

- ✓ Decentralization enables the distribution of information on every node in the network, reducing the chances of SPOF.
- ✓ Irrespective of geographical boundaries, the users can get their identity verified across the globe.
- ✓ Blockchain 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.

9 789354 933837

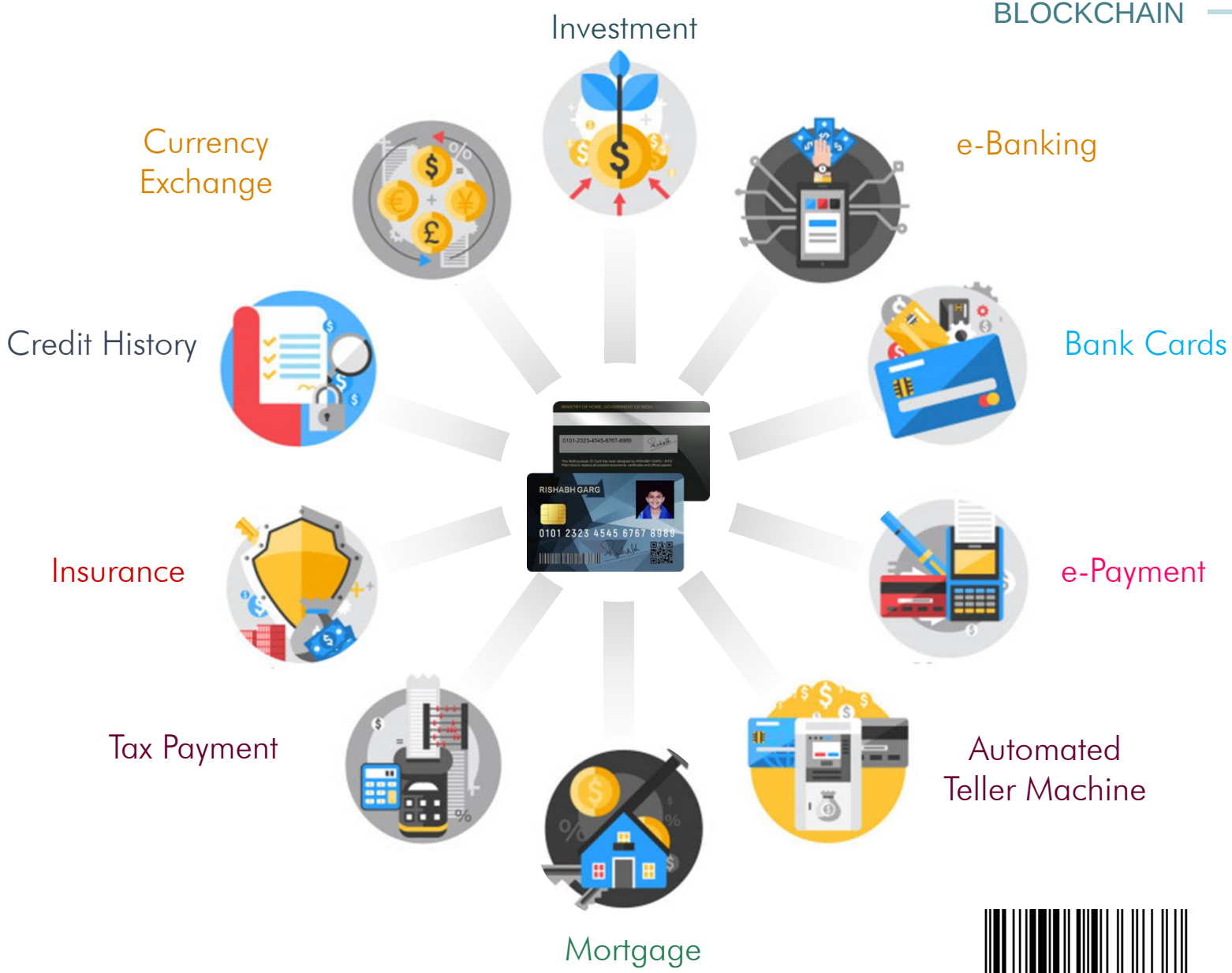
Applications of Blockchain



9 789354 933837

Applications of Blockchain in Government Sector

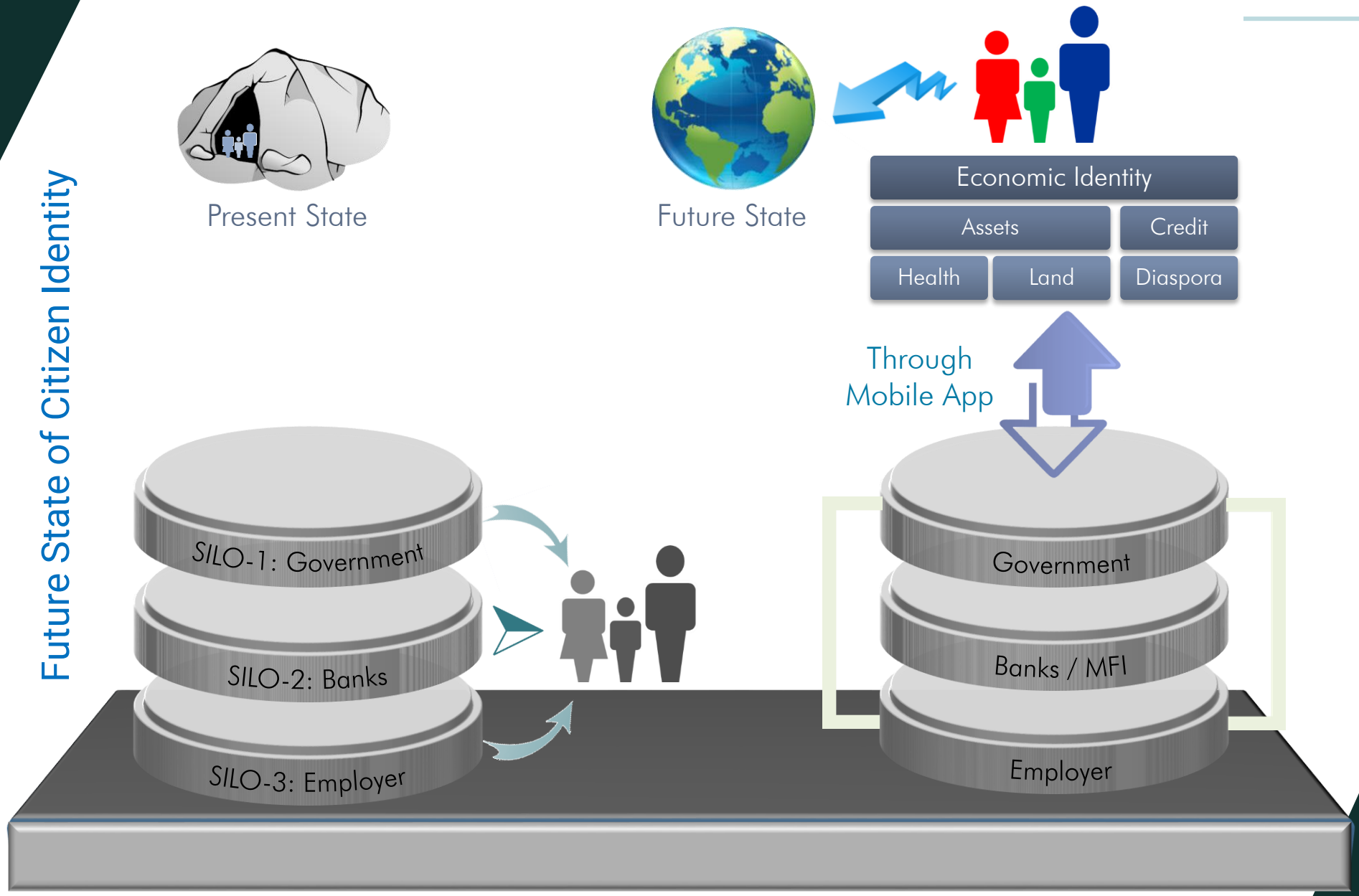
Applications of Blockchain in Finance



9 789354 933837

One World - One Identity

Future State of Citizen Identity



References

- Garg, R. Decentralized Applications for Global Networking. Book under peer review process, 2021.
- Garg, R. Blockchain based Decentralized Applications for Multiple Administrative Domain Networking. Engineering Research Project, BITS - Pilani, KK Birla Goa Campus IN, 2021: 01-69.
- Garg, R. Decentralized Transaction Mechanism based on Smart Contracts (in press) 2021.
- Garg, R. Interplanetary File System for Education and e-Verification (in press) 2021.
- Garg, R. Ethereum based Smart Contracts for Banking & Finance (in press) 2021.
- Garg, R. Self Sovereign Identity using Decentralized Identifiers. Research Oriented Project, 2020: 01-67.
- Garg, R. Digital Identity and Access Management through Distributed Ledger Technology. Open Self-Paced Project, 2020.
- Garg, R. Multipurpose ID: One Nation - One Identity, Indian Society for Technical Education (ISTE) Annual Convention - National Conference on Recent Advances in Energy, Science & Technology, 2019 (39).
- Garg, R. 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, 2018.
- Garg, R. Digital ID with Electronic Surveillance System. Innovation registered with National Innovation Foundation - Autonomous Body of Department of Science & Technology, Government of India, 2018.
- Garg, R. Hi-Tech ID with Digital Tracking System, National Conference on Application of ICT for Built Environment, 2017.
- Garg, R. Generic Information Tracker. 2nd India International Science Festival, New Delhi, 2016.