STORAGE DEVELOPER CONFERENCE
SDC 21
BY Developers FOR Developers

Virtual Conference
September 28-29, 2021

A SNIA Event

Applying Blockchain for Digital Identity Management

Abirami Ravichandran
MSys Technologies LLC

ABOUT
MSYS TECHNOLOGIES

PRODUCT ENGINEERING SERVICES AND DIGITAL TRANSFORMATION PARTNER

BAY AREA UNICORNS

rubrik PURESTORAGE® COHESITY Acronis

ENTERPRISES

amazon flex Google bakkt

AWARDS

DOIS

IAOP
2021 Global Outsourcing 100

RED HERRING 100 WINNER ASIA

IE20 INDIA EMERGING TWENTY

'TOP FASTEST GROWING STORAGE COMPANIES' FOR TWO CONSECUTIVE YEARS

Storage.com Newsletter

OUR WW STRENGTH 1000+ AND GROWING

MSYS OFFICES - USA | INDIA | VIETNAM

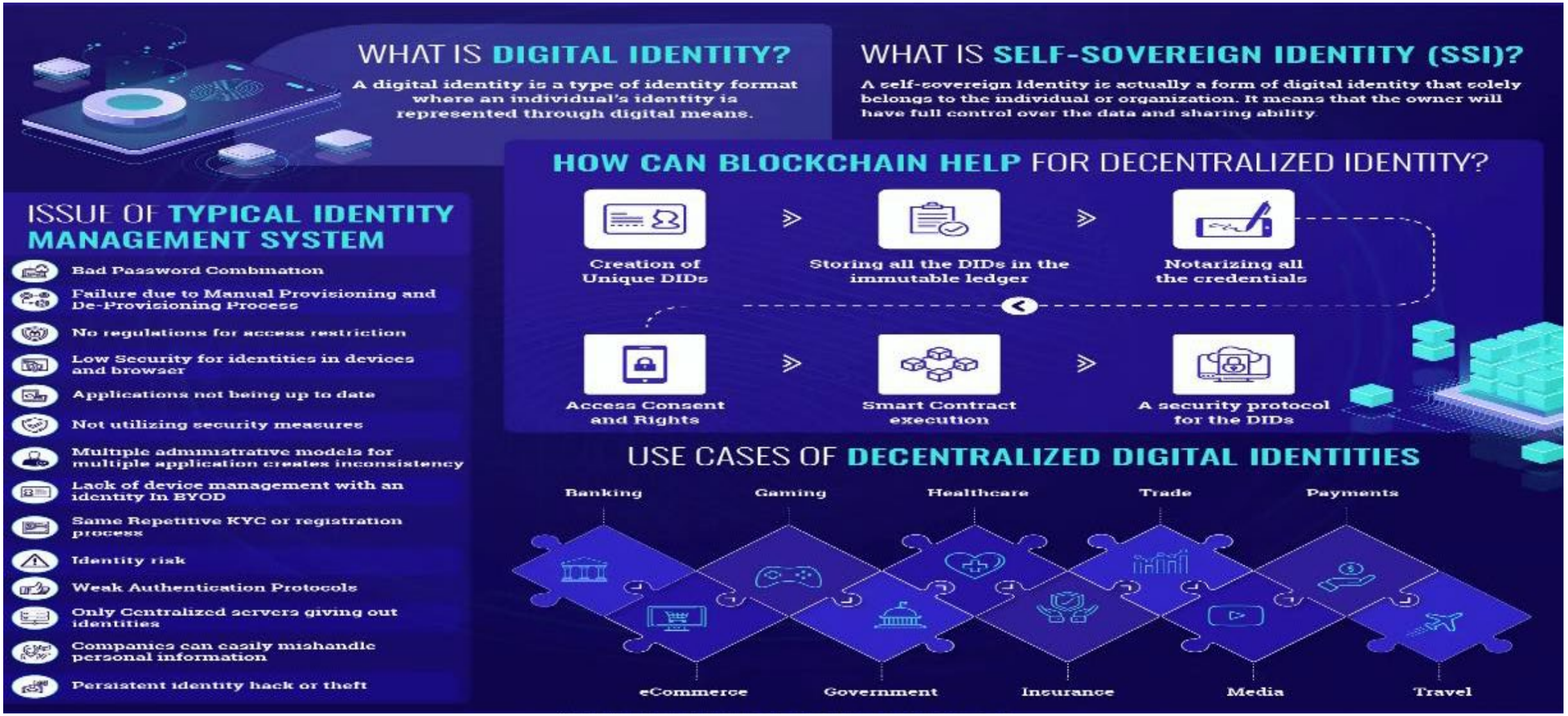
Agenda

- About Digital Identity
- Issues of Typical Identity Management
- Blockchain Adoption Trend and Technology
- How do blockchain technology works
- How can blockchain help digital identity
- Blockchain-based use case
- Legacy Vs Blockchain based on-boarding process
- Current Blockchain Related Projects

Digital Identity

- One of the basic rights of any human being.
- Identity Assets include: A first and last name, The birth date, Nationality, Passport number etc..
- In reality, every human needs to have an identity in order to work in our social environment.

Digital Identity



Issue of Typical Identity Management System

- Bad Password Combination
- Failure Due To Manual Provisioning and De-Provisioning Process
- No Regulations for Access Restriction
- Low Security for Identities in Devices and Browser
- Applications Not Being Up To Date
- Multiple Administrative Models for Multiple Application Creates Inconsistency
- Not Utilizing Security Measures Properly

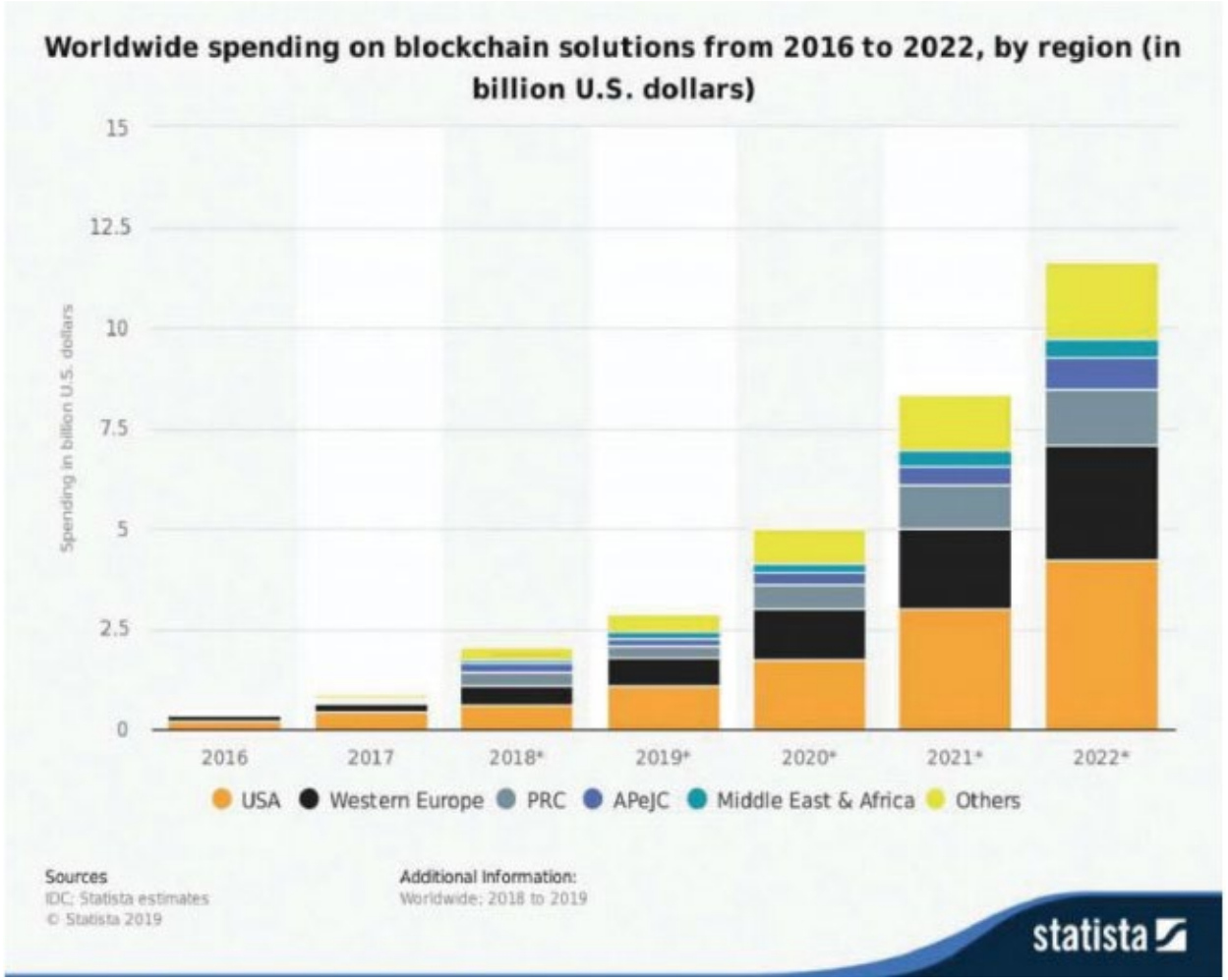
Issue of Typical Identity Management System (Cont'd)

- Lack of Device Management with an Identity in BYOD
- Same Repetitive KYC or Registration Process
- Identity Risk from Online Platforms
- Weak Authentication Protocols
- Only Centralized Servers Giving Out Identities
- Companies Can Easily Mishandle Personal Information
- Persistent Identity Hack or Theft

Blockchain and Decentralized Identity

- No centralized institute issuing or having claim over any kind of identity.
- Added level of security that comes with decentralized ones.
- No third party or any other institute can misuse the digital identity anymore.
- Blockchain technology - Great solution for decentralized identity.

Blockchain Adoption Trend



- **Forecast:** Value of Blockchain for businesses will exceed **$3.1 Trillion** by 2030.
- Below graph depicts the global spending on Blockchain solutions in recent years and projected through 2022.

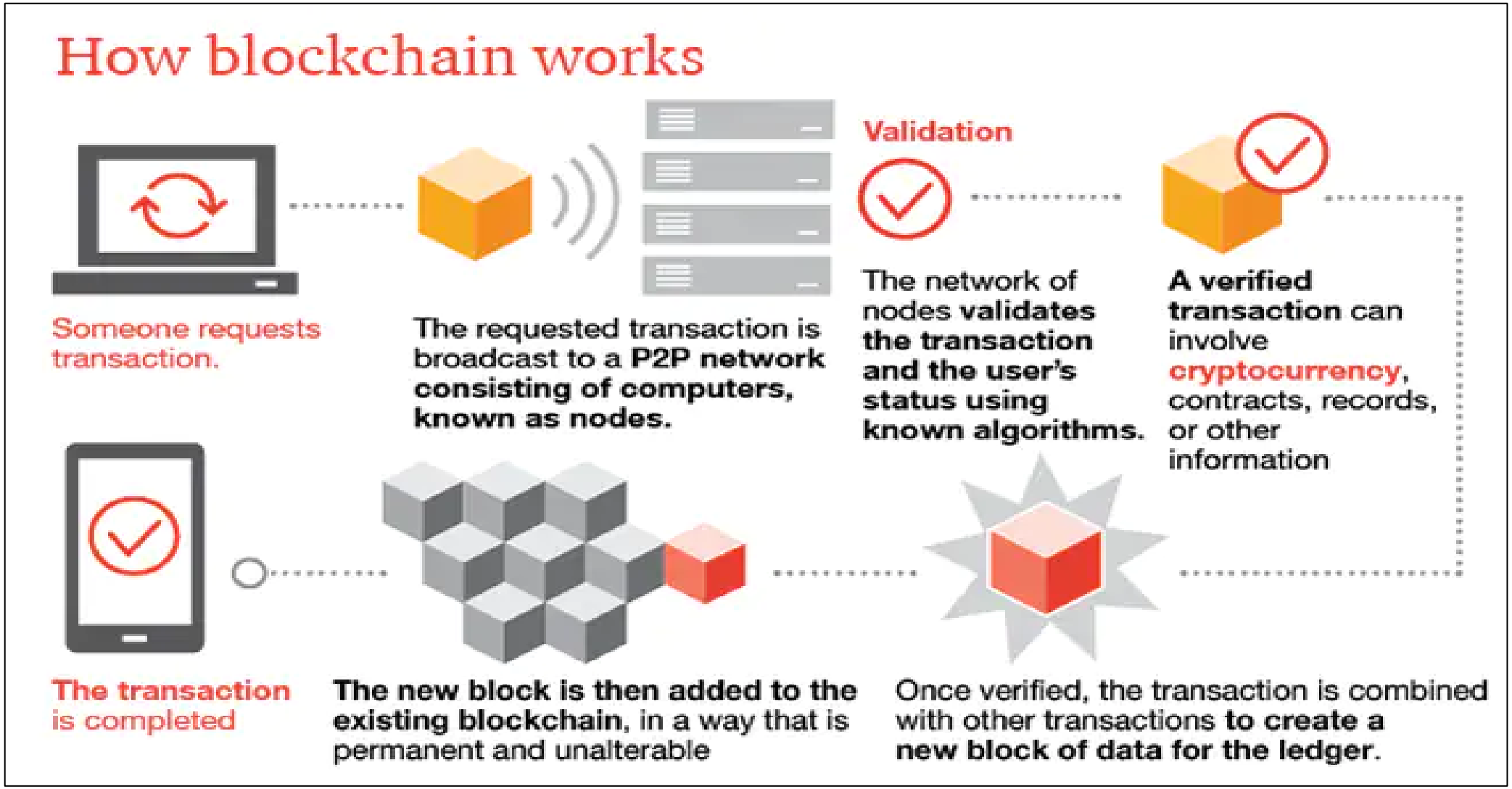
Blockchain Technology

- A distributed ledger system that promotes decentralization, transparency, and data integrity.
- Multiple blocks that are connected in a chain-like a format.
- Block - data along cryptographic hash ID with transactional data and timestamps .
  Chain - represents the linking structure.
- Stay Forever! - any data that would go in the block can never get deleted or altered.
- Peer-to-Peer network.

Blockchain Technology : How Does It Work?

- Blockchain stores all the information in a ledger system.
- Any kind of data exchanges is called “**transactions**.”
- Every single user on the network is called “nodes,” and they get a copy of the updated ledger.
- First of all, a user will request for a transaction in the network.
- It will be broadcasted to all the nodes in the network.
- The nodes use an algorithm to validate the information.
- Once the block gets validated, the block will get a spot on the chain.
- At the same time, the transaction we did will be executed as well.

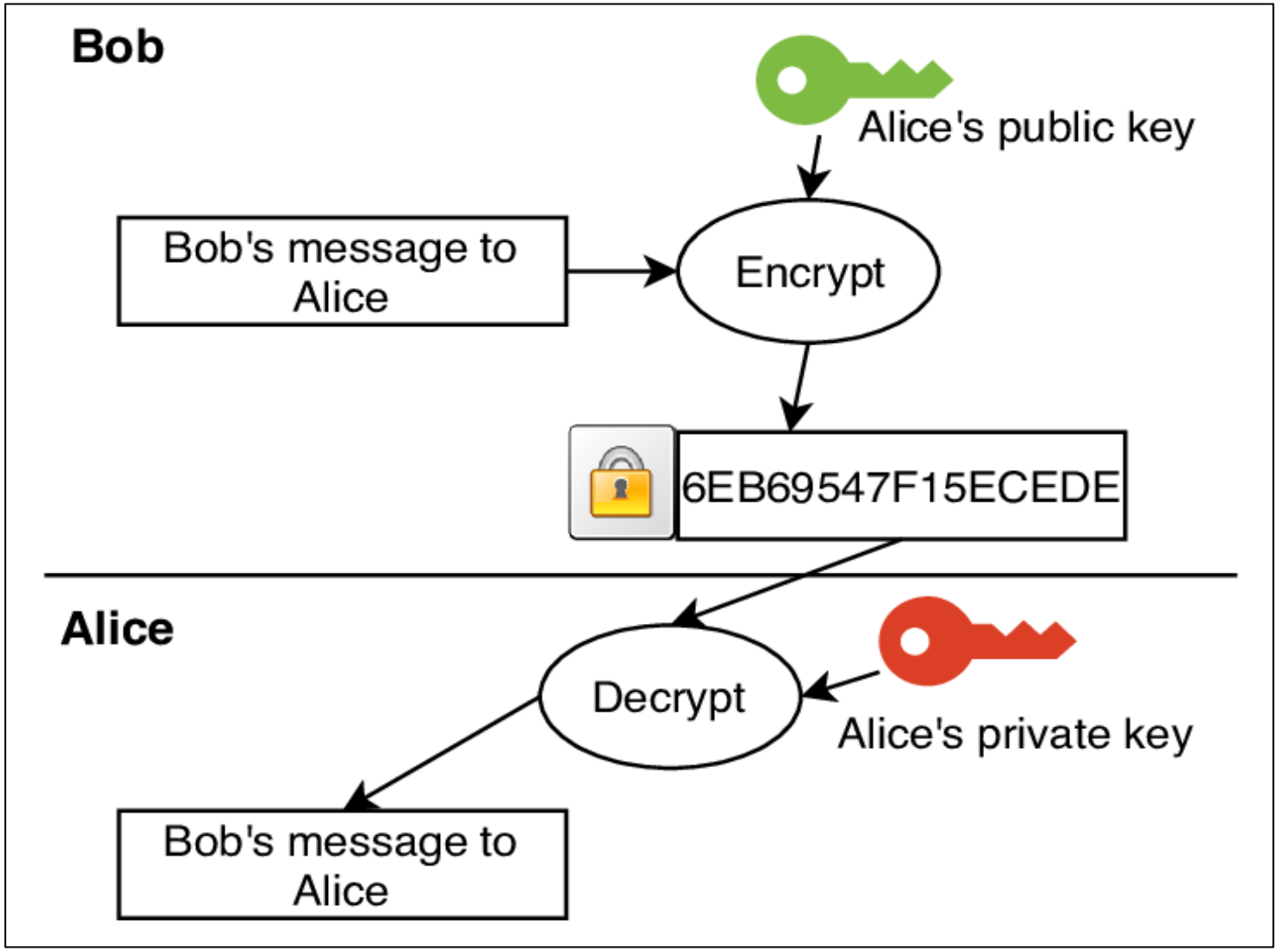
Blockchain Technology : How Does It Work?



Digital Identity Blockchain: How Can Blockchain Help?

- **Creating DIDs** : DID's can be created from Blockchain addresses (Which are unique); Owners can generate it themselves.
- **Registry for All DIDs** : ID's Information get stored on immutable ledger storage.
- **Credential Notarization**: Putting Seals on ID; A timestamp and moreover, offer an electronic seal.
- **Consent and Access Rights(SSI)**: User can control.
- **Using Smart Contract Features**: Identity as a proof can be used in smart contracts triggering the data exchange securely and transparently system along the way.

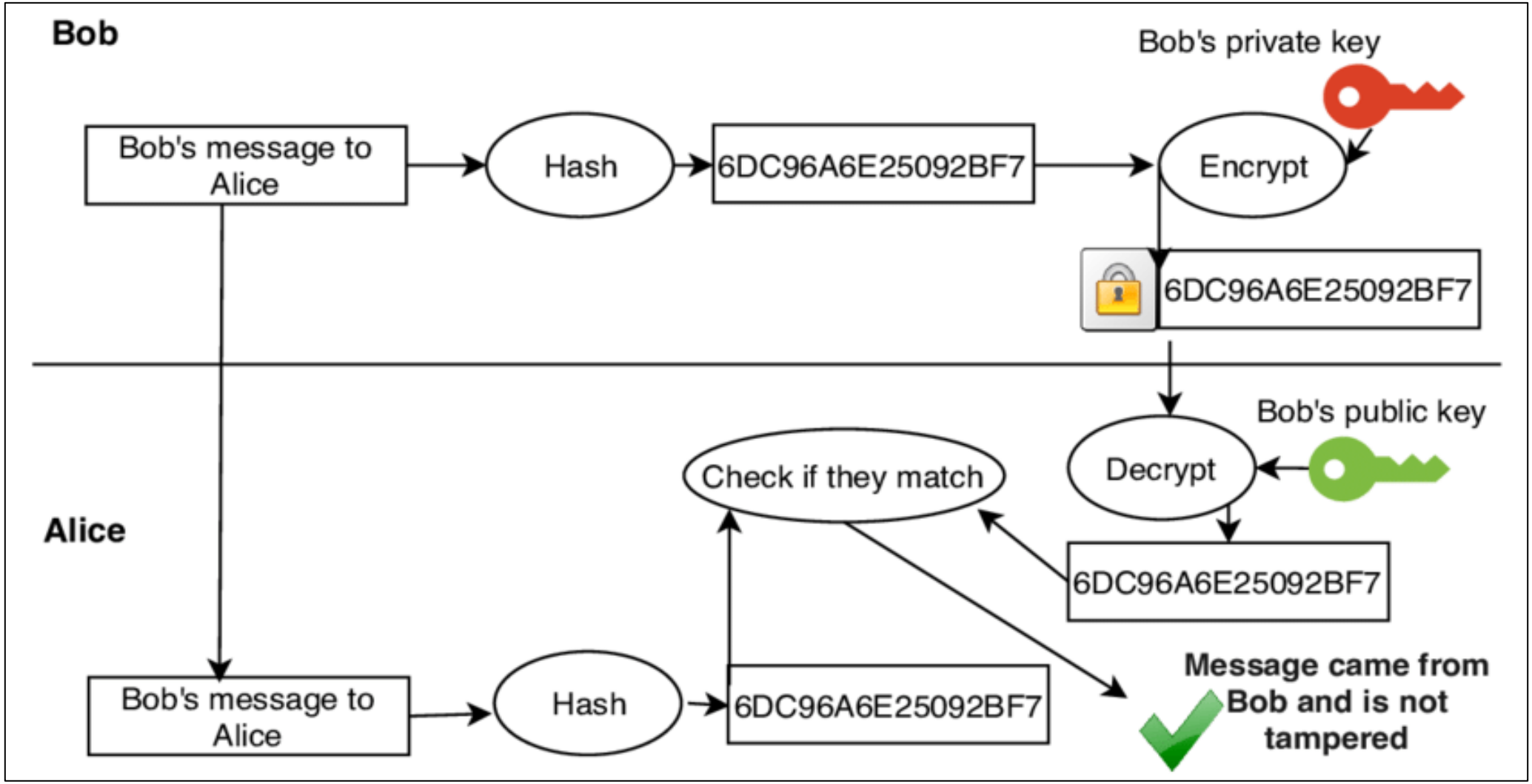
Public-key Cryptography



Hashing

- Mathematical mechanism of generating a fixed size value from input data.
- In Blockchain, hashing is utilized in hashing transactions and block data.
- Bitcoin system uses **SHA256** hashing algorithm, which was originally designed by United States National Security Agency (NSA).
- SHA256 is also being used for decades in many sectors and services that requires solid security, such as in financial services, and it has proven to be secure.

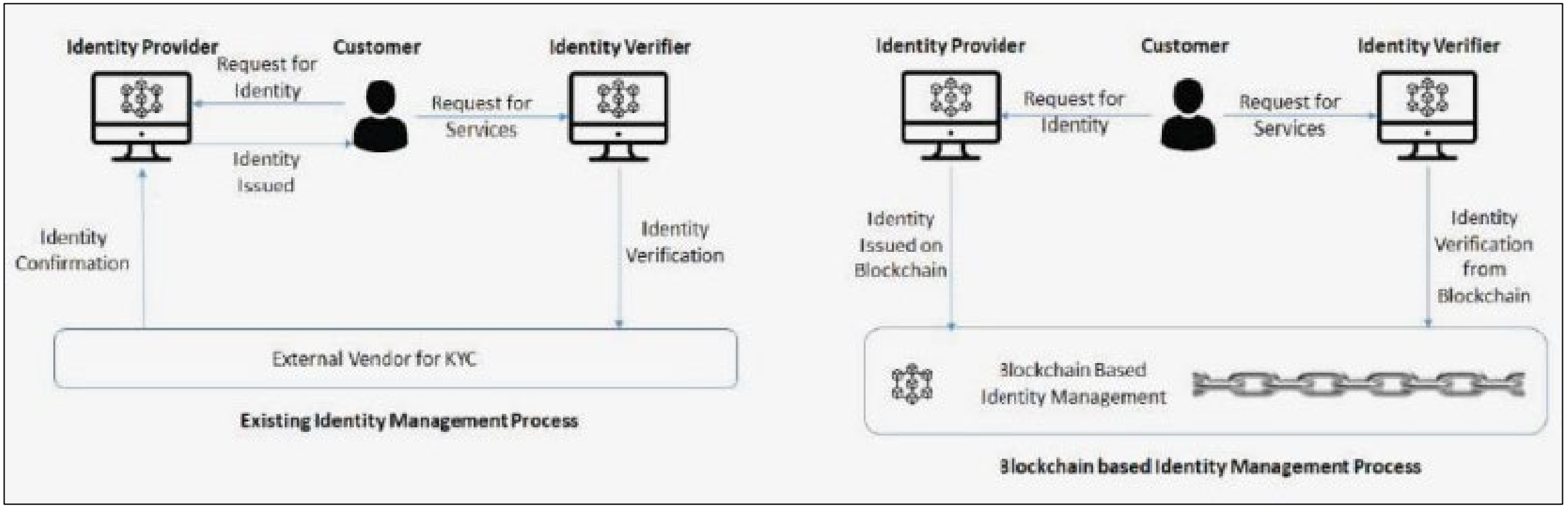
Digital Signature



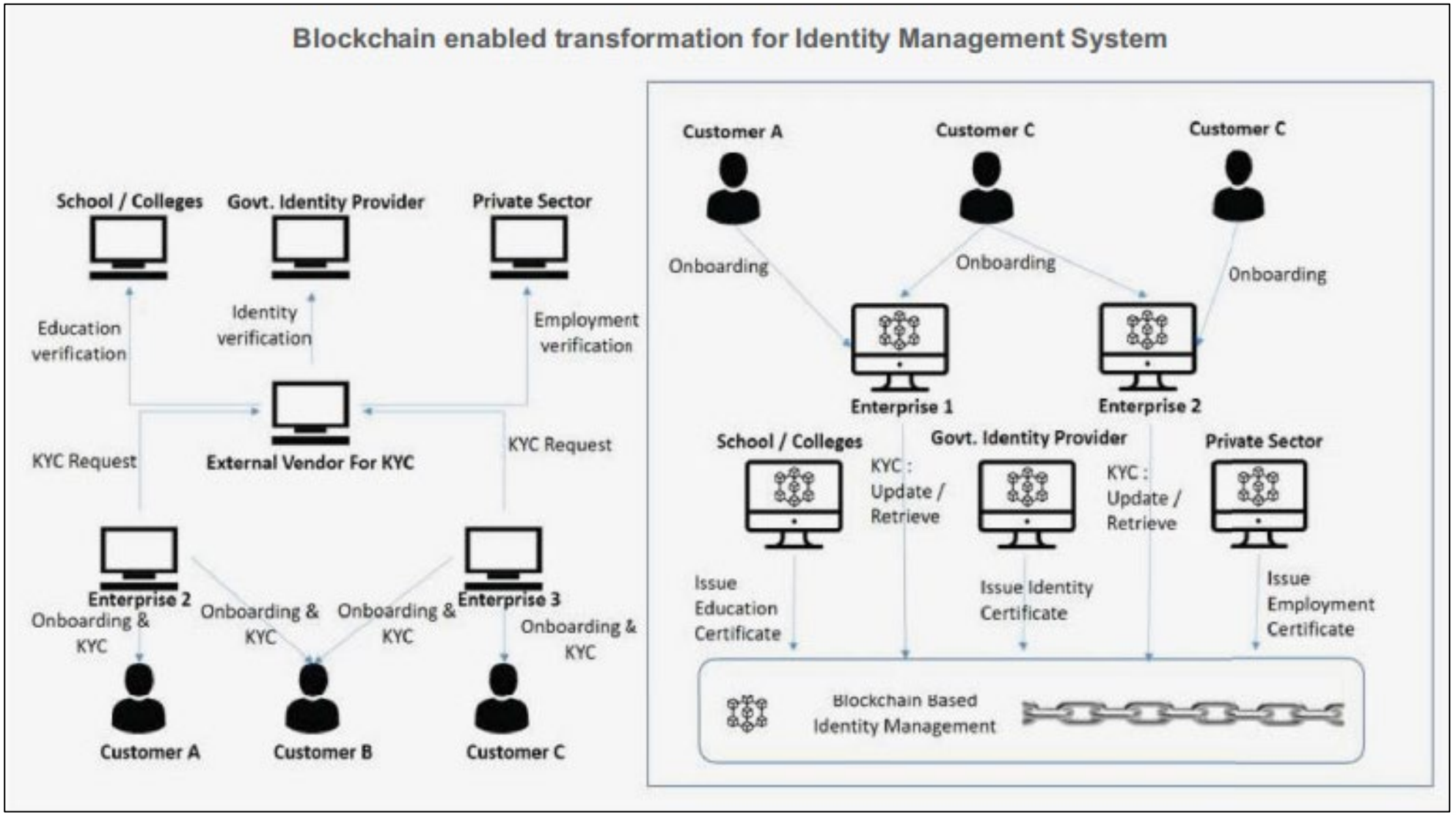
What is stored on Blockchain?

- No private data is stored on the Blockchain ledger in our system.
- Even encrypted and hashed versions of private data are not stored as the encrypted data on Blockchain
- Thereby, Blockchain is mainly utilized to lookup decentralized identifiers and identity owners.

Existing Versus Blockchain based ID Management Process



BlockChain based Use Case



On-boarding Process

Legacy on-boarding process	Blockchain based on-boarding process
• Customer raise request for on-boarding in enterprise • Enterprise raises background verification request to External KYC vendor for:- 1. Education with School / Colleges 2. Identity with Government Identity Provider 3. Employment with Private sector • Upon successful verification, External KYC vendor share the status with enterprise • Based on the verification status, enterprise on-board customers in their systems	• **Join the network:** Enterprise, School Government Identity Provider, and private sector join the Blockchain network • **Issue education certificate:** School issues educational certificates which get stored in Blockchain-based user's wallet • **Issue identity certificate:** Government identity provider issues identity certificates again stored in Blockchain-based user's wallet • **Issue Employment Certificate:** Private sector issues employment certificates which get stored in Blockchain-based user's wallet • **Onboarding Request:** Customer raise request for on-boarding in enterprise • **Request for Documents:** Enterprise raise a request to share the required certificates • **Documents Sharing:** Customer shares the required documents with the specific enterprise for the given duration • **Certificate verification:** Enterprises perform the certificates verification from Blockchain network and on-board customers in their systems

Limitations and Benefits

Limitations of Legacy on-boarding process	Benefits of Blockchain based on-boarding process
• **Expensive**: Duplicate KYC cost for the same customer which was verified by one reputed organization. • **Time Consuming**: Lack of direct communication between enterprises and various departments the verification process takes longer time to on-board customers. • **Lack of Transparency:** Due to lack of direct communication between enterprises and various departments/units, there is a lack of transparency in the information. • **Lack of Trust:** If the same customer's KYC was completed from one enterprise then also another enterprise performs the KYC again. • **Lack of Control:** Customers don't have control on 1. How the information was shared with other departments/units. 2. Don't have control to revoke the permission to access their identities details if required.	• **Less Expensive**: Bringing certificate issuer and verifier on the same platform helps to remove the external party from the process which helps to save the huge cost for verification • **On-boarding Acceleration:** By segregating external KYC vendors from the on-boarding process and bringing Identity issuer and verifier on the same platform helps to on-board customers quicker on the system. • **Trust & Transparency:** Distributed & decentralized data ledger helps to bring trust & transparency in the system • **Customer-centric control:** Customer-centric and aims to provide control to the customer and let him/her decide 1. With whom he/she wants to share information? 2. What would be the duration for which he/she wants to share information? 3. Ability to revoke permission to use his/her information

Related Projects

Related Works	Explanation
Hyperledger (2015)	• It is an initiative by The Linux Foundation that aims to create common open source Blockchain frameworks and tools that anyone can use freely.
Hyperledger Fabric	• Hyperledger Fabric is a Blockchain foundation for creating private permissioned Blockchain applications with a modular design. • Identities are essential in Hyperledger Fabric, since apart from asset ownership, resource and access permissions management are also determined by actors' identities. • Another distinctive feature of Hyperledger Fabric is that it allows private channels that can be used for permissioned private data sharing.
Hyperledger Indy	• Hyperledger Indy is a public permissioned distributed ledger project. • It supports data minimization and enables identity owners to store their identity based records. • Applications don't need to store individuals' personal data, instead they store a link to the identity.

Related Projects (Cont'd)

Related Works	Explanation
Sovrin(2015)	• A live distributed ledger built for decentralized identity that uses Hyperledger Indy's codebase. • It uses a public Blockchain since it is designed to provide a self-sovereign digital identity for all.
ShoCard(2015)	• Identity details are stored in a digital file called "ShoCard," which is owned by the identity owner and usually stored on the owner's mobile device. • Identity owners have a public-private key pair for controlling their identity. • ShoCard system architecture consists of a Blockchain layer which includes multiple public and private Blockchain networks built on top of the Blockchain layer

Related Projects (Cont'd)

Related Works	Explanation
Secure Key(2019)	• SecureKey and Canada's major financial institutions launched blockchain-based network **Verified. Me** in Canada • SecureKey architecture enables privacy with a **triple-blind identity sharing,** in that the data provider never knows the service a consumer is accessing, and the data requestor does not have to know the exact credential provider other than knowing the business type of the credential provider.

Conclusion

Blockchain based Digital Identity management systems help enterprises and customers in following perspectives:

- Security
- Data Control
- Identity Traceability
- Trust & Transparency
- Accelerated onboarding
- Eliminate fraud
- Cost Effective
- Single Identity

References

- https://www.researchgate.net/publication/333993279_Towards_a_Blockchain_based_digital_identity_verification_record_attestation_and_record_sharing_system
- https://101blockchains.com/digital-identity/
- https://www.coforgetech.com/resource-library/white-papers/digital-building-digital-identity-management-system-blockchain

About Speaker

Abirami is a Devops Engineer with 5+ years of hands-on experience in building and supporting web SaaS solutions based on Linux/Unix platform in a cloud especially on AWS and GCP. In her previous stints, she worked on Configuration and Management of Web and Application servers including Apache, Nginx , Tomcat JBOSS and Wildfly. She has distinguished experience on different Version Control systems, Continuous Integration, Continuous Testing and Continuous Monitoring Tools. She helped to choose the best tools and technologies which best fit the business needs. She has also been an active member of the Organisation internal GDPR committee and trains employees on Data , Source code security and Privacy. She has been the operations team head and contact for SSAE audits held on the organization.

At MSys, she is responsible for automating and supporting CI/CD in product development. She is employed by Python for Automation. And also using Jenkins for automation Jobs and writes Ansible Playbook for configuration Management. She is having close coordination with the development team such that the application is in line with performance according to the customer's expectation.

Please take a moment to rate this session.

Your feedback is important to us.

Thank you

