Blockchain FinTech and KYC

Bhume Bhumiratana, Ph.D.

Blockchain

TECH

THE NEXT REVOLUTION

BHUME BHUMIRATANA, PH.D.

INTERNET OF MONEY

LOOKS LIKE THIS

IT REQUIRES NO

TRUSTED 3RD PARTY

RECEIVER KNOWS HE CANNOT BE

LIED TO

FINITE AMOUNT

EXISTS

TRANSACTION CAN HAPPEN FROM

ANYWHERE

BETWEEN

ANYONE

CLEARING COMPLETE

ALMOST IMMEDIATELY

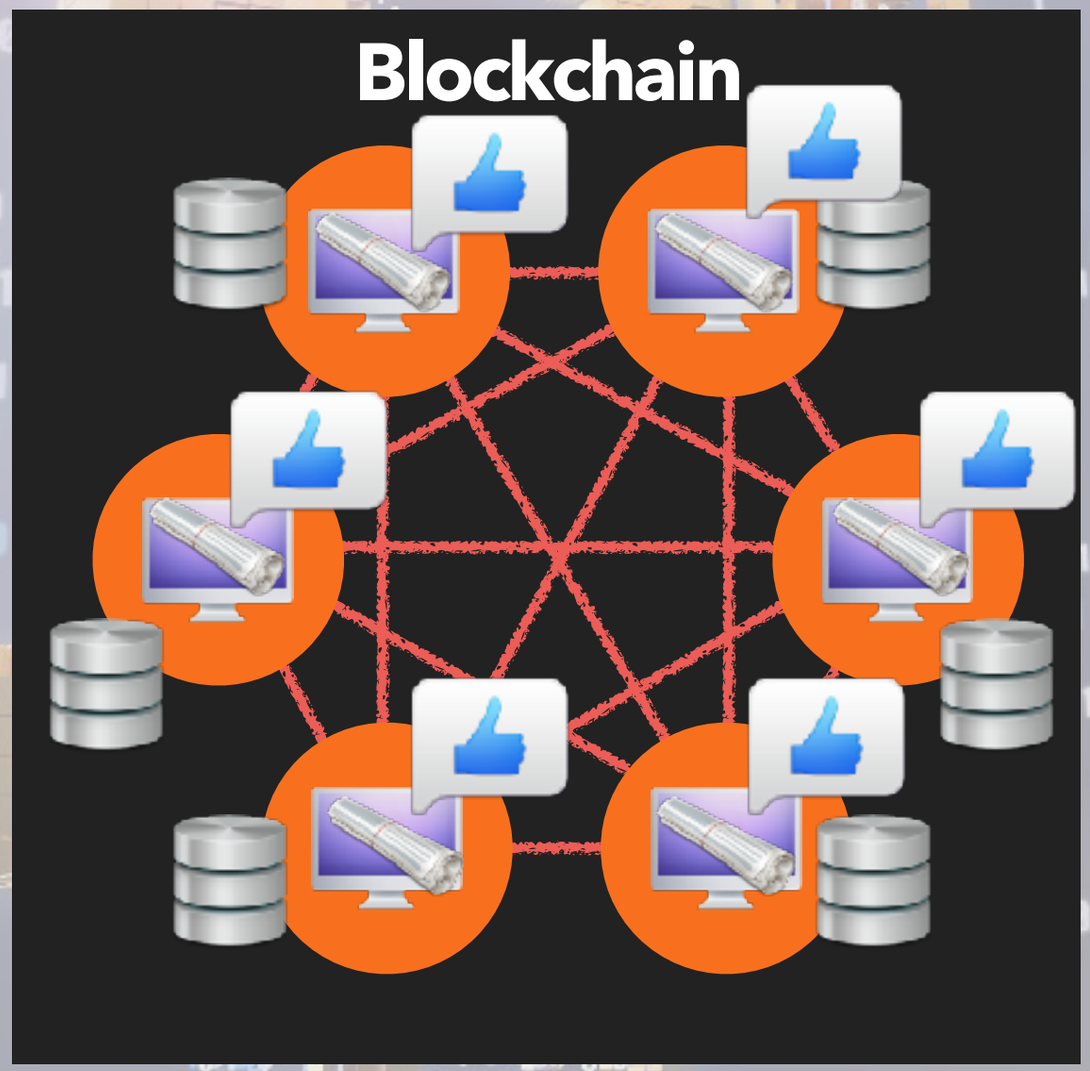
How Is This Possible?

WITH **BLOCKCHAIN** TECHNOLOGY

WHAT IS BLOCKCHAIN?

KEEPING THEM CONSISTENT VIA CONSENSUS

WITH ALGORITHM



WHAT IS BLOCKCHAIN?

NETWORK OF COMPUTERS THAT **COOPERATES** TO MAINTAIN SETS OF **FACTS** TOGETHER AS THEY **GROW** KEEPING THEM CONSISTENT VIA **CONSENSUS** WITH **ALGORITHM** THAT AUTOMATICALLY **REPAIRS** FROM MISTAKES AND ERRORS

WHERE EACH FACT IS **VALIDATED** BY ALL **PARTICIPANTS** AS THEY ARE GENERATED

AS A RESULT, THE SYSTEM CAN BE **TRUSTED** WITHOUT TRUSTING **ANYONE** IN THE NETWORK

SO LONG AS YOU CAN TRUST IN THE **ALGORITHM**

NETWORK OF COOPERATING COMPUTERS

THAT MAINTAIN FACTS

FACTS

THAT CANNOT BE ALTERED

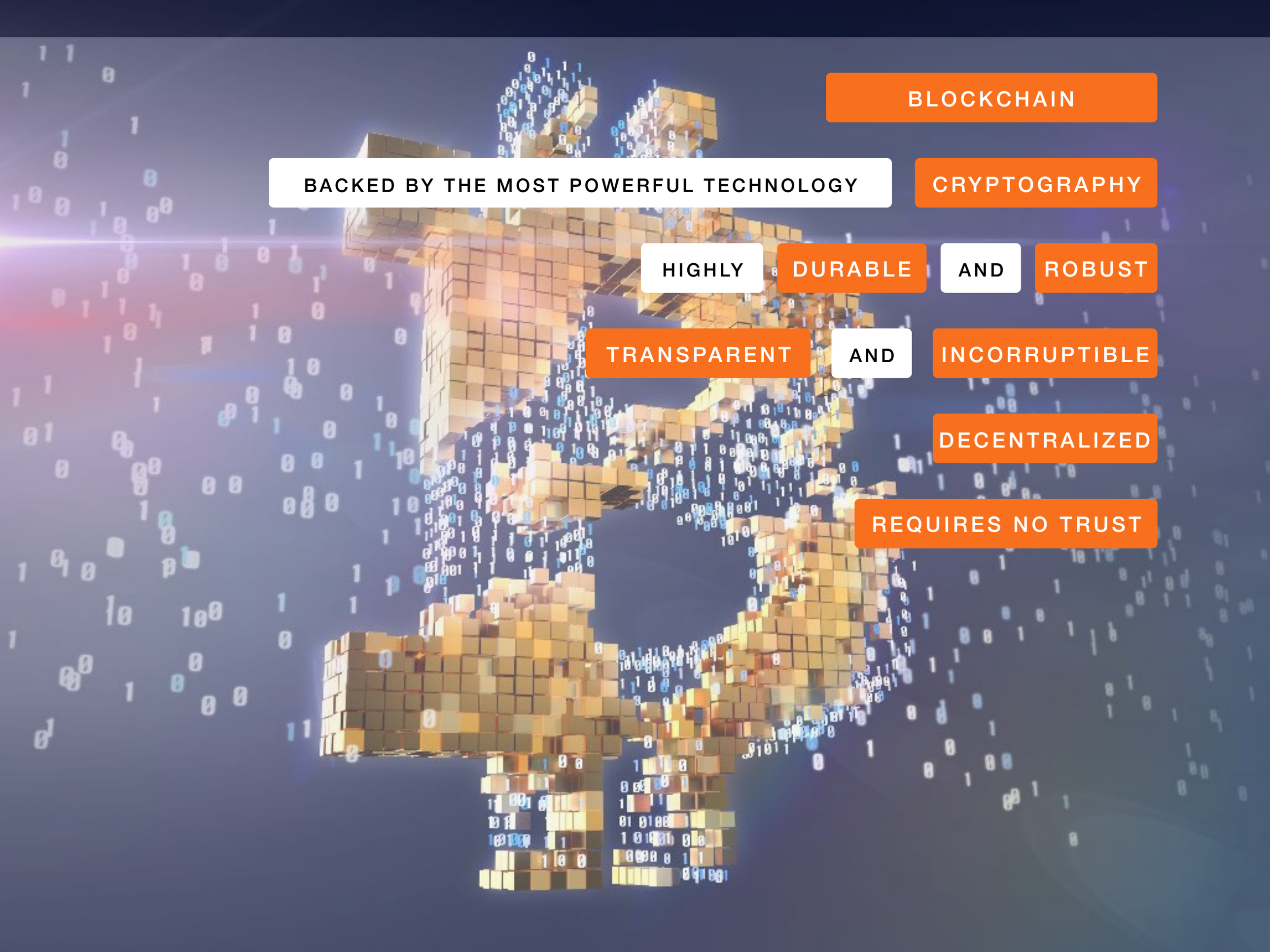
PARTICIPANTS CANNOT BE

LIED TO

BLOCKCHAIN

FULLY TRANSPARENT

ALWAYS AVAILABLE


BACKED BY THE MOST POWERFUL TECHNOLOGY
BLOCKCHAIN
CRYPTOGRAPHY
HIGHLY
DURABLE
AND
ROBUST
TRANSPARENT
AND
INCORRUPTIBLE
DECENTRALIZED
REQUIRES NO TRUST


BLOCKCHAIN
CAN BE USED FOR MORE THAN JUST
MONEY
AKA
CRYPTOCURRENCY
SMART CONTRACT
SHARING ECONOMY AND APPLICATIONS
CROWDFUNDING
GOVERNANCE
SUPPLY CHAIN
PROVENANCE
AUDIT
DATA STORAGE
MARKETS
TRADE
TRADE FINANCE
INTERNET OF THINGS
SMART GRID
SMART CITY
IDENTITY
KYC
FRAUD PROTECTION
ANTI MONEY LAUNDERING
LAND TITLES
...

Blockchain Use case in Financial Industry

Use Case

- Cross-border payments
- Share trading
- Smartcontract
- Identity Management
- Loyalty and Rewards

Cross-Border Payment

Cross-Border Payment

- Benefit
  - Faster and more affordable
- Barrier
  - Regulation
- How
  - Remittance + Foreign Exchange
  - Cryptocurrency Exchange

Trading

Trading

- Removing the middleman
    - Stock Exchange
    - Clearing and Settlement
- Potential Limitation
    - Scalability
    - Speed

Smart Contract

Smart Contracts

- Benefits
  - Secure and automated processing of contracts
  - Transparent, and precise (code)
- Use case
  - Insurance
  - Real estate, trade finance
- Obstacle
  - Maturity of technology
  - Security Risk

Identity Management

Identity Management

- Benefit
  - Transparent
  - Sovereign control
  - Security
- Challenge
  - Adoptions/Deployments
  - Key Management/Theft

Loyalty and Rewards

Loyalty and Rewards

- Benefit
- Transparency and Traceability
- 24/7 feedback of value, Real-time reward
- No middleman, tradable/exchange-able rewards

Other use case

- Trade Finance
- Regulatory Compliance & Audit
- Insurance
- P2P transaction and Lending

Use Case: eKYC

Know Your Customer (KYC)

"Methods to confirm identity of customer prior to establishing business relationship"

4 steps of KYC:

1. Identification

Customers present their own identity to declare the intent to conduct business with the organization (e.g. bank account opening). Identification can be achieved in 2 major approaches

1. **Face to Face**: the customers present themselves with government issued document such as ID card or passport
2. **Non-Face to Face**: the customers present their identity by declaring the information about their identity (e.g. providing first and last name, citizen ID number)

2. Verification

Process where business verify the customer's identity to ensure the customer is who they claim they are. Verification can be achieve in 2 major approaches

1. **Face to Face**: Verify authenticity of the provided document

2. **Non-Face to Face**: Verify authenticity of the provided information such as checking with authority

3. Authentication

After customers and business establish relationships, they establish a more convenient and reliable method of confirming transactions in the future.

1. **Face to Face:** e.g. Book bank + signature, ATM card + PIN
2. **Non-Face to Face:** e.g. Username+Password, Token

Note: The authentication is often strengthened by using Multi-Factor Authentication such as SMS-OTP

4. Due Diligence

Process where business must continuously conduct the due diligence and building customer profile to confirm the customer's authority to do transaction such as checking against UN sanction and PEP list, beneficial owner and controller.

How it work

1. Profile creation

Each user is given a persistent identity on the blockchain

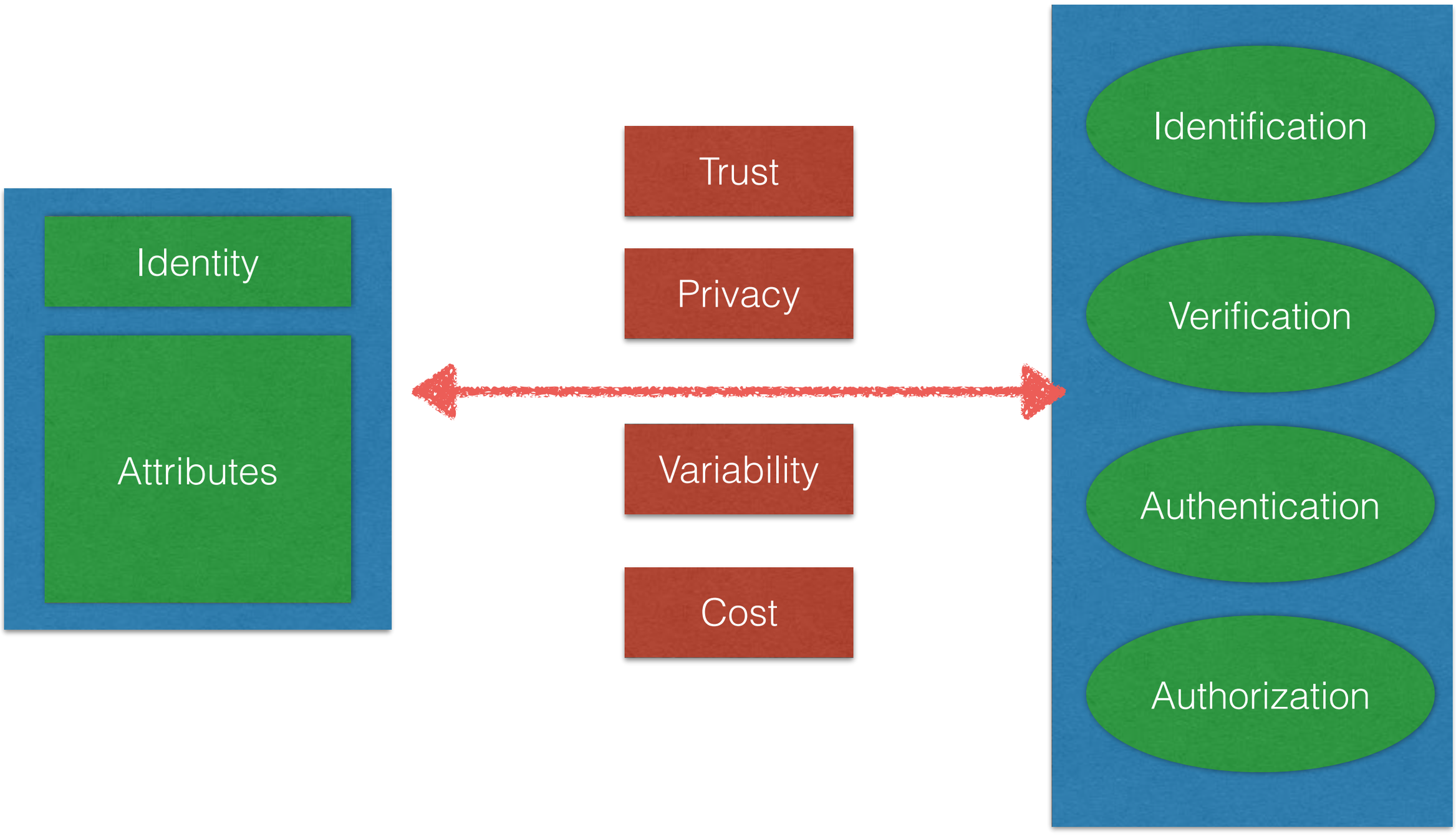
2. Verification

Government system or Certified business verifies claim of identity (can be either F2F or Non-F2F) of the user, and leave a non-repudiation, non-forgeable, immutable proof of verification on the blockchain

3. Use

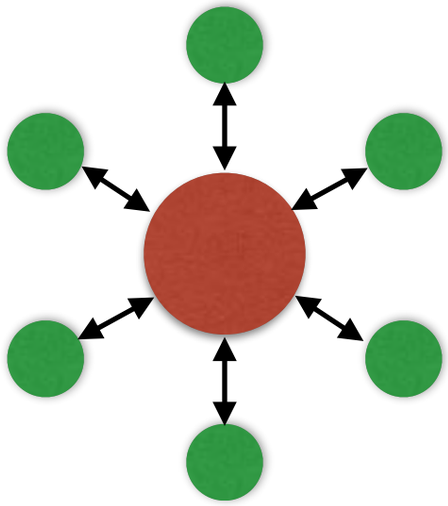
When a business wants to confirm a user identity, user provides proof of ownership of identity on the blockchain. The business, then, can confirm the proof directly on the blockchain, in a non-forgeable way

eKYC

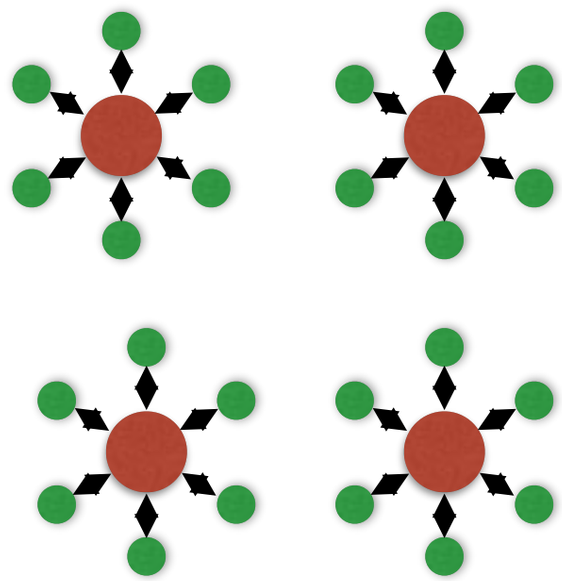

Identity
Attributes
Trust
Privacy
Variability
Cost
Identification
Verification
Authentication
Authorization

National/Shared E-KYC Models

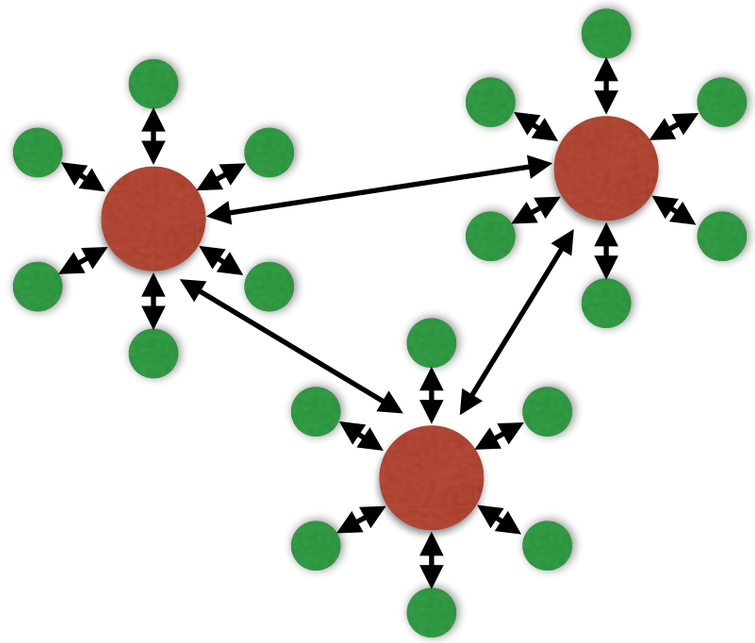
Centralized



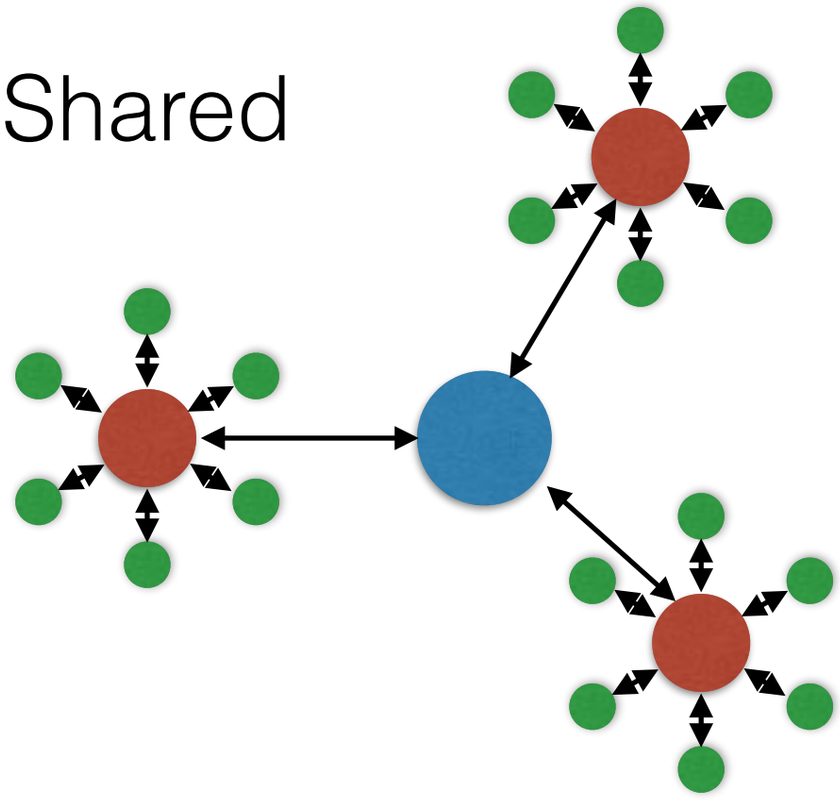
Separated



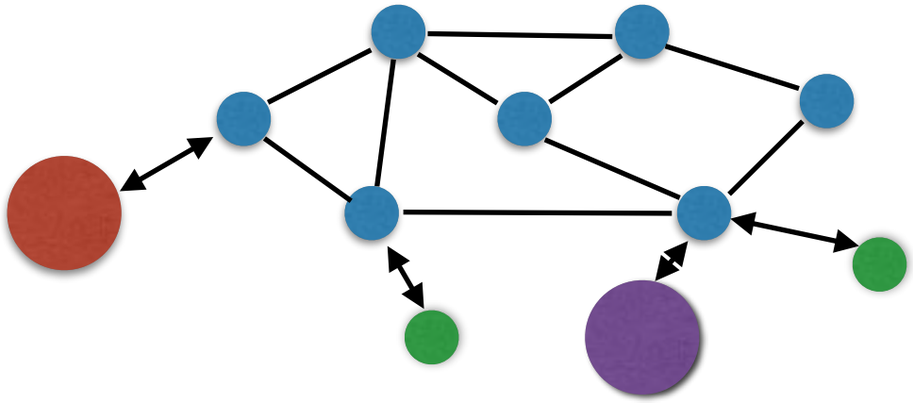
Federated



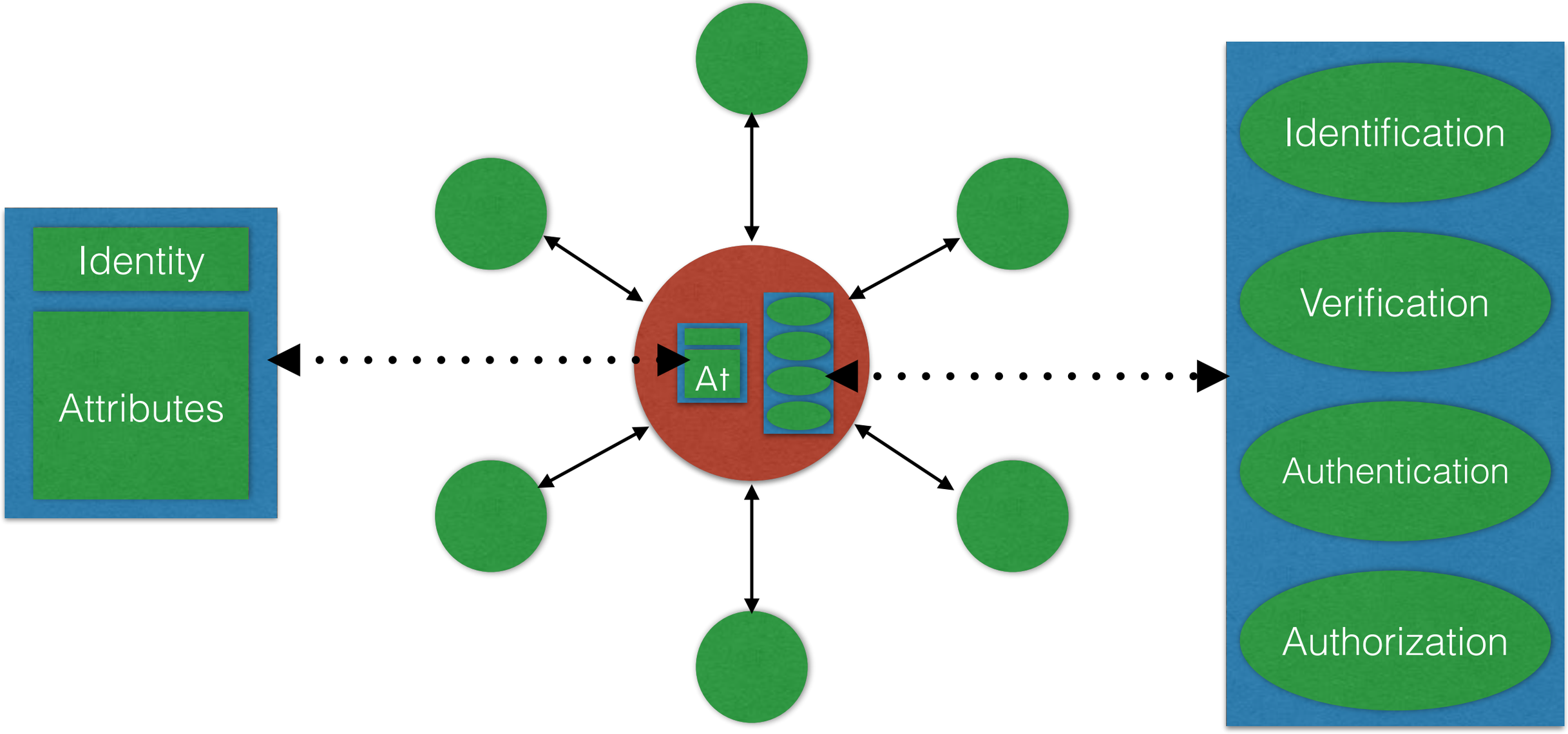
Shared



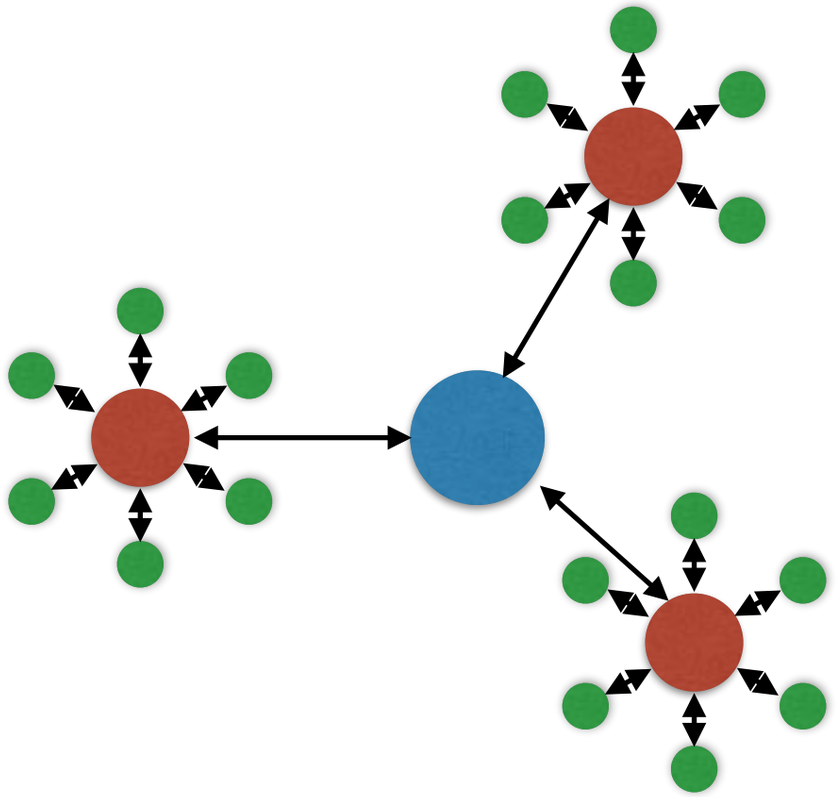
Distributed



Centralized/Decentralized/ Federated



Shared



Attributes

Identity

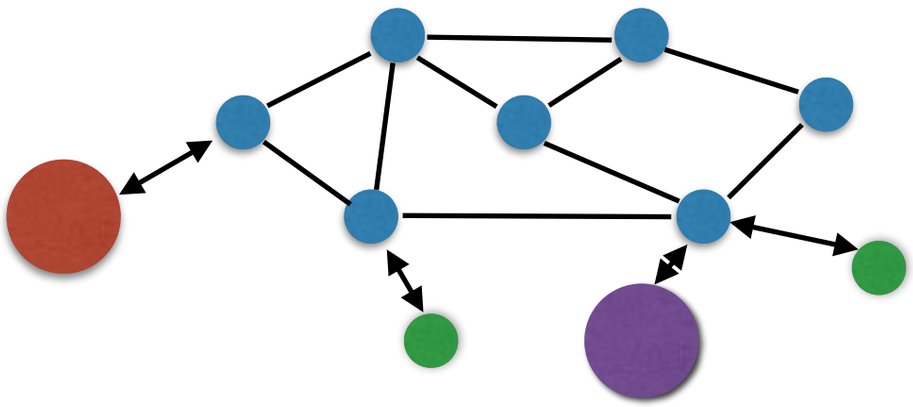
Identification

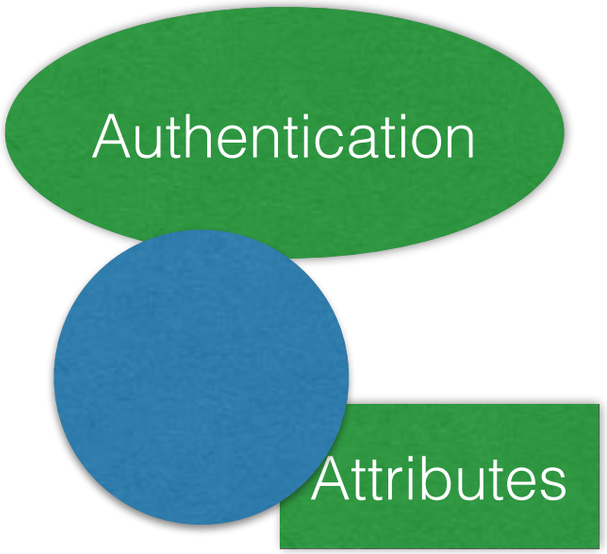
Authentication

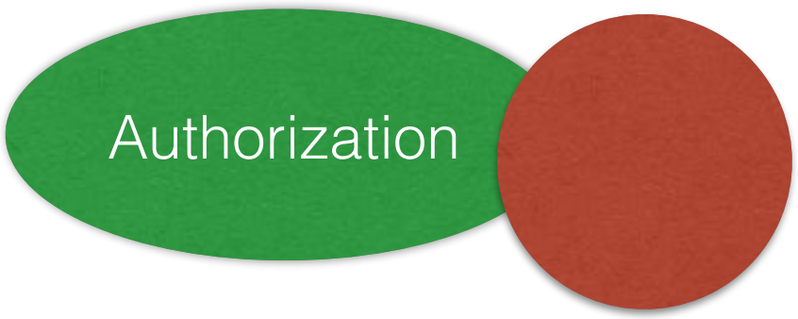
Verification

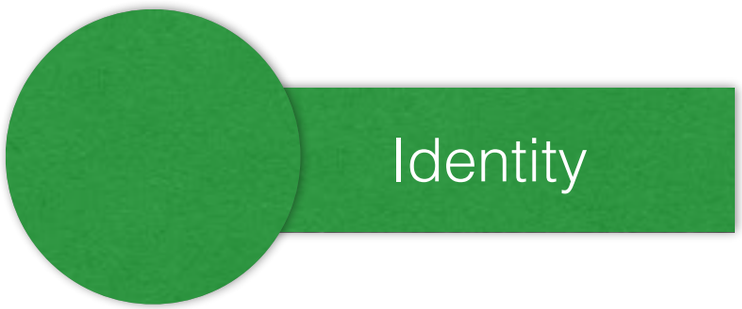
Authorization

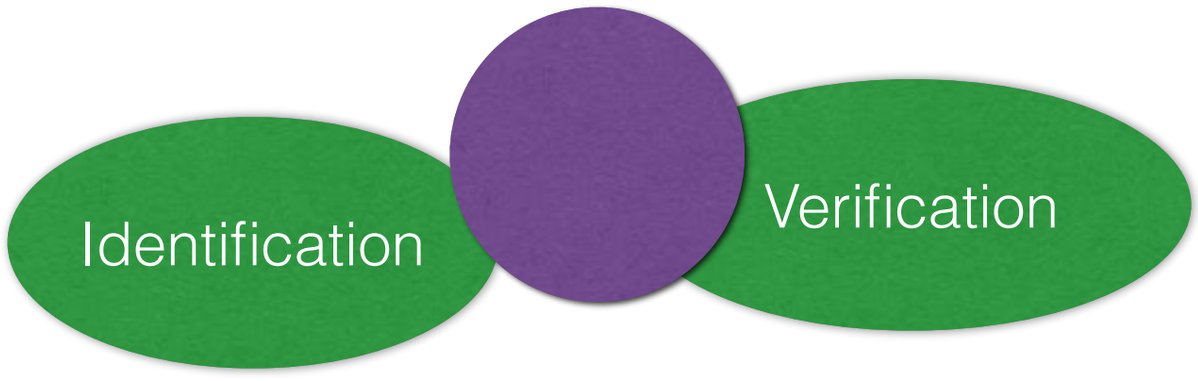
Distributed











Advantages of using Identity Blockchain for eKYC

1. **Immutability:** Identity data and related data cannot be forged or modified. Thus, identity data and related data is foolproof and built-in fraud protection
2. **Integrity:** Business which runs on the blockchain identity platform will have confidence that the data is up to date and verified
3. **Transparency:** The blockchain automatically collects proof for auditing
4. **Provide Anti-Fraud/Identity theft via transparency control** For example, if the customer is a victim of identity theft, the customer can see the log on the platform to check whether there is an unauthorized use of customer's profile to open new account. The platform will collect the evidence that there is usage of the identity that the customer can check for himself; the platform provides the chance for faster detection.
5. **Lower Infrastructure/Operation Cost**
6. **Scalable:** The blockchain platform is decentralized, meaning the customers do not need to rely on other platform to get access. Everyone can become a part of the system and control his data without needs to depend on centralized infrastructure. It distributes the cost to the organization that has the most to gain from usage. No centralized data means lesser risks on the reliability of the intermediaries.

Security by design

Key Risks

- Fraud
- Identity Theft
- Cybersecurity
- Giving/Lending Identity (e.g. nominee)

Fraud & Identity Theft (1/2)

- **Blockchain's transparency helps reduce fraud and theft**: If the user is the victim of the identity theft. Once the criminal uses the unauthorized identity, the user which is the owner can detect the unauthorized usage and may be able to prevent the crime or notify the authority of the fraudulent activity to minimize the damage

- **State-of-the-art Authentication (Public Key Cryptography):** In case the user verify and authenticate the transaction using the device or technology with public-key Cryptography and use the high standard Key management device (e.g. FIPS 140-2 level 3 or higher), the identity theft or fraudulent will be unlikely or exhausting because the criminal must gain access to such device. The user will be aware of the breach if he finds that the device is missing. Moreover, if the device is locked with PIN or biometric lock, the criminal needs to obtain or forge the biometric data in order to use take over the identity. Mission Impossible!

Fraud & Identity Theft (2/2)

- **Plugable Identificaton**: The identity platform that runs on blockchain is open for variety of method for verification and authentication in order to allow the user to choose the best suitable technology for each individual needs which provides different level of security. Some people with demand for higher security than layman will have the tailored choices while people with little needs for high level security will not have to go through pain of securing higher than needed complicated method.
- **Smart-Contract based identity** The platform is flexible to build the application on-top, e.g., the tailored made special condition. The user may require that multiple devices must be used to verify or authenticate the transaction. In doing such that, it will increase the security for such user and reduce the risk of losing a single device.

Cybersecurity

- Blockchain technology is known for high level of security, and resilient to attack. The most vulnerable point in the system is the external systems that connects to the blockchain.

- The Blockchain Identity Platform is designed to be **“Permissioned Blockchain.”** To connect to the Platform, an external system must be thoroughly tested and strictly audited before it is allowed to connect to the Platform. External system’s owner is obligated to maintain the highest security measure of its own system.

- Once the Platform administrator spots the security breach or suspicious behavior from any blockchain node in the ecosystem, it can be immediately isolated from the Platform in order to mitigate the risk and to maintain the highest level of system and information security for the rest of the blockchain ecosystem.

Nominee and other abuse of online identity

- Addressing the issue of abusing the identity and being nominee for other people is typically difficult because of the voluntary/consensual nature of the actor
- This issue is hard to detect and prevent if the owner of the identity consents. However, the blockchain based identity can reduce the incentive to do so because of the higher risk of getting caught (with Transaction Transparency and Non-Repudiation of identification) and enhance ability to prove intent.
- Since the transaction in the blockchain system is transparent to the actor, the activity can later be examined, and the confirmation of identity usage is non-refutable. The nominee cannot refuse that he did not lend the identity or abuse the identity because the usage needs the user confirmation and all transactions are kept in the hash/log on the blockchain. With greater and wider usage, the blockchain identity platform will become apparently fortified. The user cannot deny the transaction and claiming that his identity was stolen if he let the transaction continues when has the chance to notify the authority. The behavior of abuse can be used to prove his malicious intent.