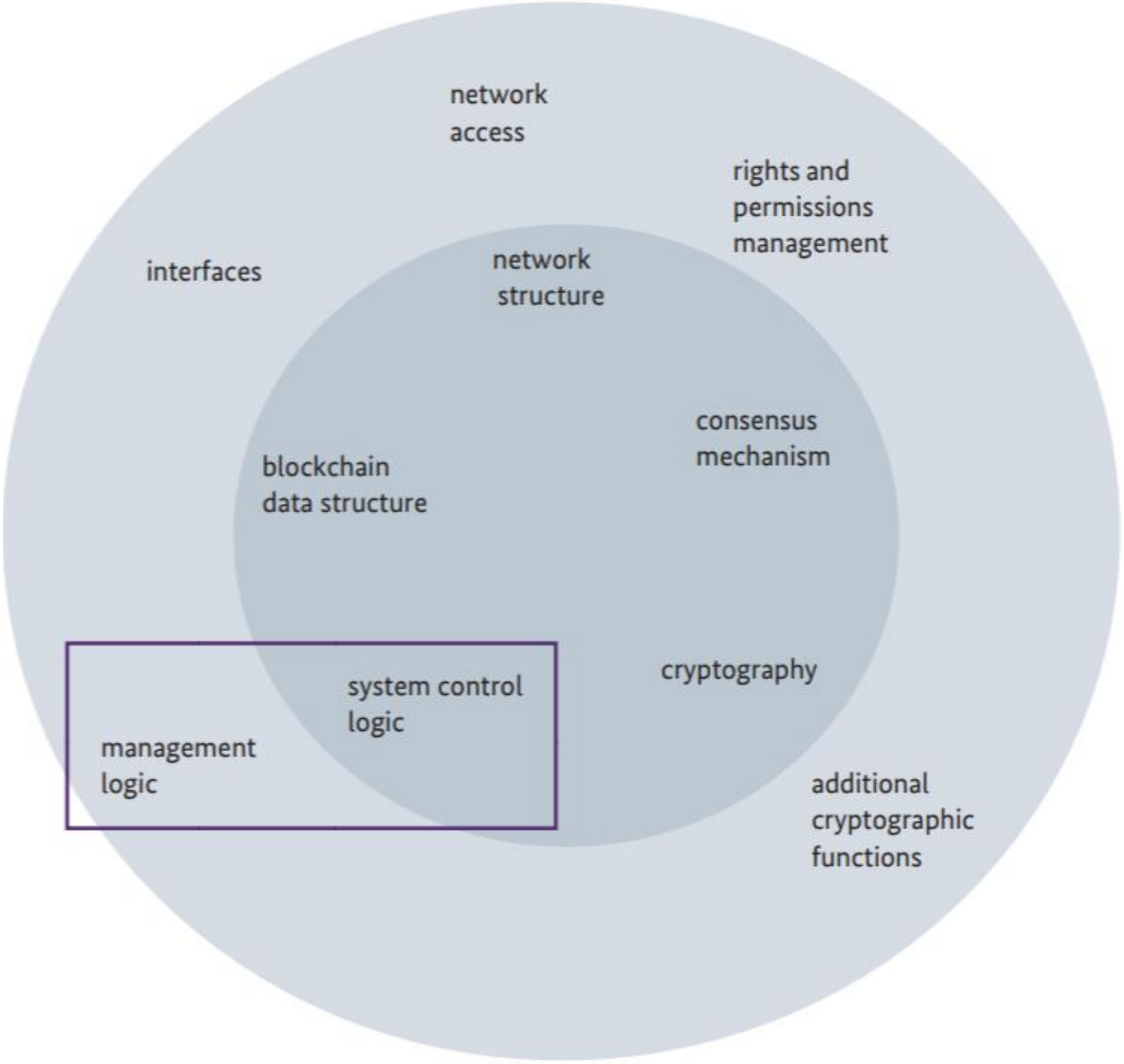
Blockchain
(Review and Advanced Topics)

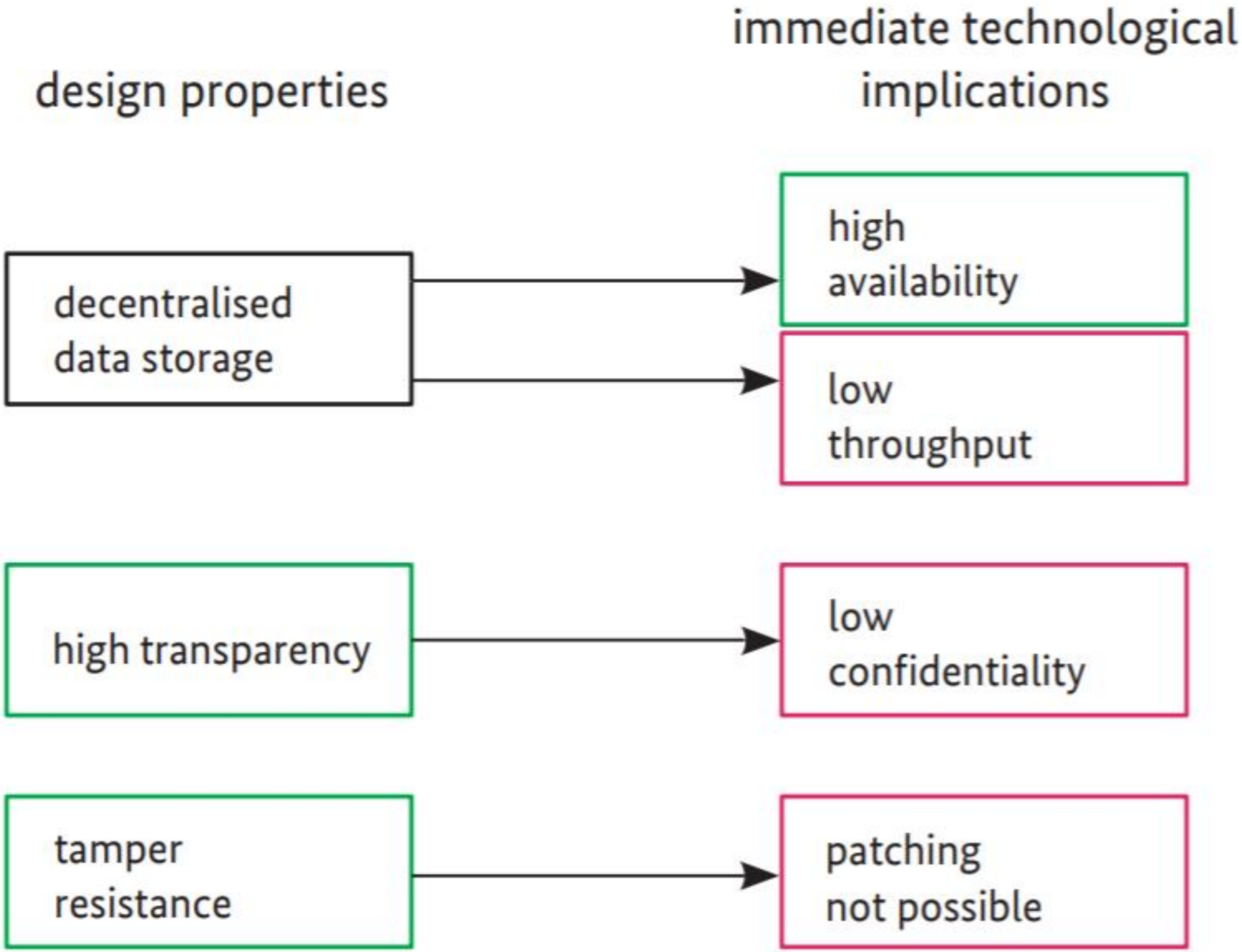
Dhiren Patel

Lecture on 7 Nov 2019

Blockchain components



Introspecting Blockchain



design properties

immediate technological implications

decentralised data storage

high availability

low throughput

high transparency

low confidentiality

tamper resistance

patching not possible

Definitions

- **Block**: A block is a data structure used to communicate incrementally to the nodes of the network transactions and/or changes of states occurring in the time interval since the validation of the last block.
- A block can contain a list of transactions, the binary code of smart contracts, state variables, each organized according to a Merkle tree.
- The header of the block includes the reference of the previous block, the cryptographic footprint of it content *c*, and the proof to be verified.
- For Bitcoin and Ethereum, this is the "nonce" *n* solution of the "PoW" function.
- **Blockchain**: the longest path that links the "genesis block" (root of tree) to a leaf (last block) is called the "blockchain". The blockchain forms a coherent transaction history on which all nodes can, in principle, agree.

Definitions

- **Consensus**: agreement among nodes that a transaction is valid and that there is a consistent set and a guaranteed ordering of the transactions to be stored in the distributed ledger
- **Consensus mechanism:** rules and procedures by which consensus is reached
- **Immutability**: property of blockchain and distributed ledger systems that ledger records can only be added, but not removed or modified, and are ordered in time
- In a Permissionless blockchain, all the nodes of the network can participate in the consensus mechanism.
- In a Permissioned blockchain, only authenticated and authorized nodes can participate in the consensus.
- **Proof:** Algorithm that provides a short number (a claim) that can be easily verified by others and without all the inputs needed by the algorithm. The output of the verification of a proof is a Boolean ("true" or "false").

Definitions

- **PoW (Proof-of-Work)**: Proof of Work is a mechanism that allows a peer to prove that a certain amount of computing resource has been used over a given period of time
- The Bitcoin's PoW function is expressed with the function:
- **F**d(c, n) → SHA256(SHA256(c|n)) < 2^{224}/d
- It allows keeping data consistent in a setting without authentication of individual parties while at the same time preventing manipulations.
- **Miner**: a miner node is a participant who has the ability to generate and submit a new block to the consensus. It has the necessary resources to perform the computation of the proof. The miner node who generated the most legitimate block according to the rules and procedures of the consensus protocol, is designated "winner"
- **Verifier**: a verifier is a participant who participates in the consensus by voting to designate the most legitimate block to complete the longest chain. It has the right to vote at each time interval corresponding to the generation of a new block.

Definitions

- **Smart Contracts**: A smart contract is a convention between two or more parties, coded in such a way that its execution is guaranteed by the blockchain
- **Tamper resistant**: robust against tampering, modification, removal or damage.
- **Tamper evident**: displays and captures evidence of attempts of tampering, modification, removal or damage.
- **Fork**: update of the rules and procedures by which consensus is reached
  - **Hard fork**: update implementation in the nodes does not provide backward compatibility with the previous implementation
  - **Soft fork**: update implementation into the nodes ensures backward compatibility

Definitions

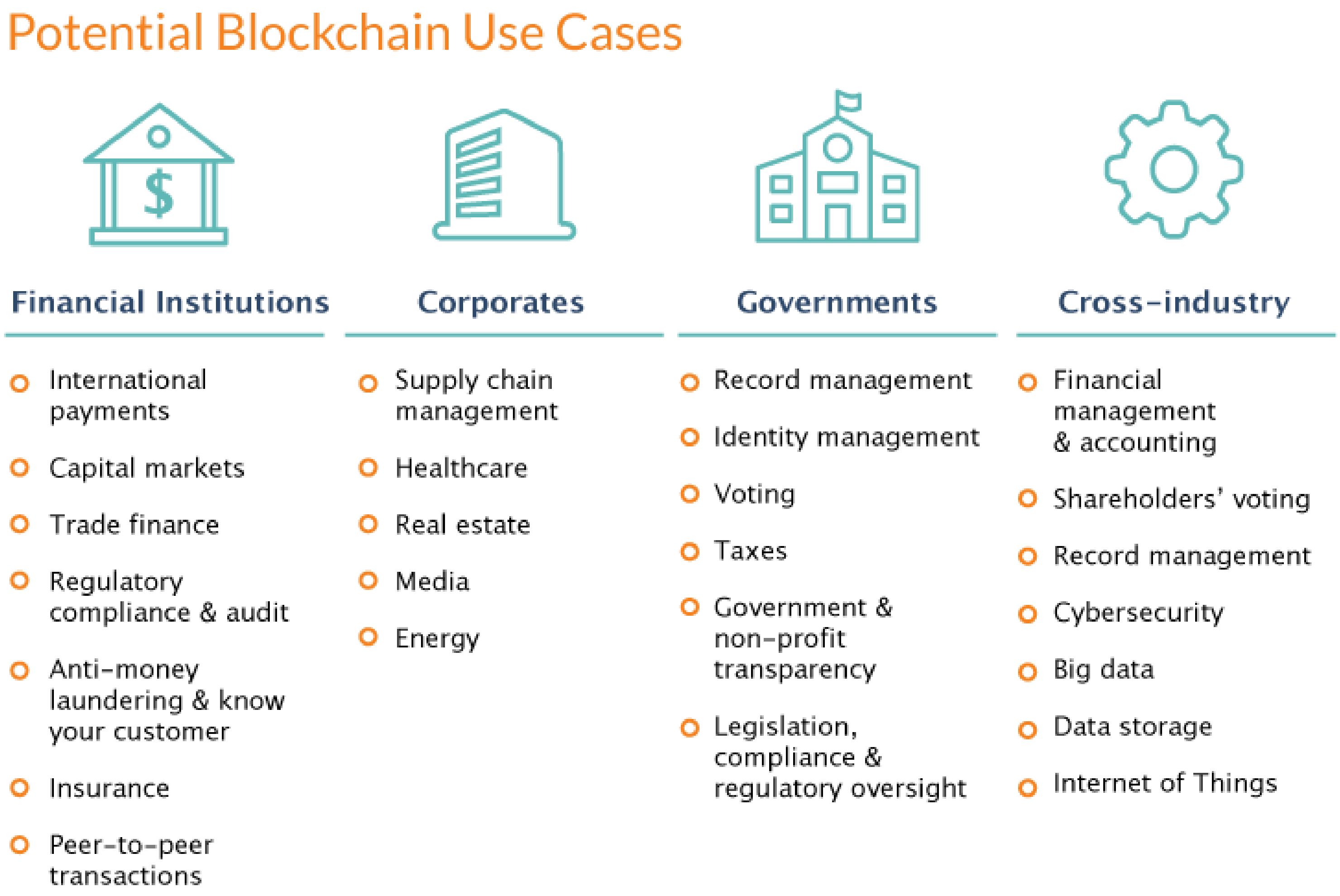
- **Liveness property** is one which states that something must happen. An example of a liveness property is the statement that a program will terminate if its input is correct.
- **Safety property** is one which states that something will not happen. For example, the partial correctness of a single process program is a safety property. It states that if the program is started with the correct input, then it cannot stop if it does not produce the correct output.
- **Consistency**: All nodes in the system see exactly the same data at the same time.
- **Availability:** Ensures that the system is operational: All queries receive an answer within the allocated time

- Blockchains offer benefits as compared to databases in terms of resilience against misuse and availability.
- Blockchains exhibit disadvantages as compared to databases in terms of confidentiality and efficiency.

Definitions

- Integrity - assuring the completeness and accuracy of data
- Authenticity - guaranteeing that a communication partner (a person or an IT component or application) is who he claims to be
- Availability - of services, applications, data - that users can always use them as intended
- Confidentiality - protection against unauthorised disclosure of information
- Anonymity - data or actions of the entity cannot be linked

Blockchain Use cases
(revisiting and new)



Potential Blockchain Use Cases

Financial Institutions

- International payments
- Capital markets
- Trade finance
- Regulatory compliance & audit
- Anti-money laundering & know your customer
- Insurance
- Peer-to-peer transactions

Corporates

- Supply chain management
- Healthcare
- Real estate
- Media
- Energy

Governments

- Record management
- Identity management
- Voting
- Taxes
- Government & non-profit transparency
- Legislation, compliance & regulatory oversight

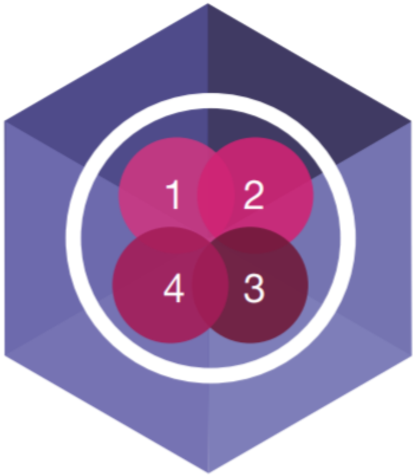
Cross-industry

- Financial management & accounting
- Shareholders' voting
- Record management
- Cybersecurity
- Big data
- Data storage
- Internet of Things

Blockchain (Built Businesses)

Improving contract management (legally enforceable smart contracts)

Enabling more transparency (in Supply Chains)



Enabling the infrastructure to combine circular economy (Building Information Management and IoT)

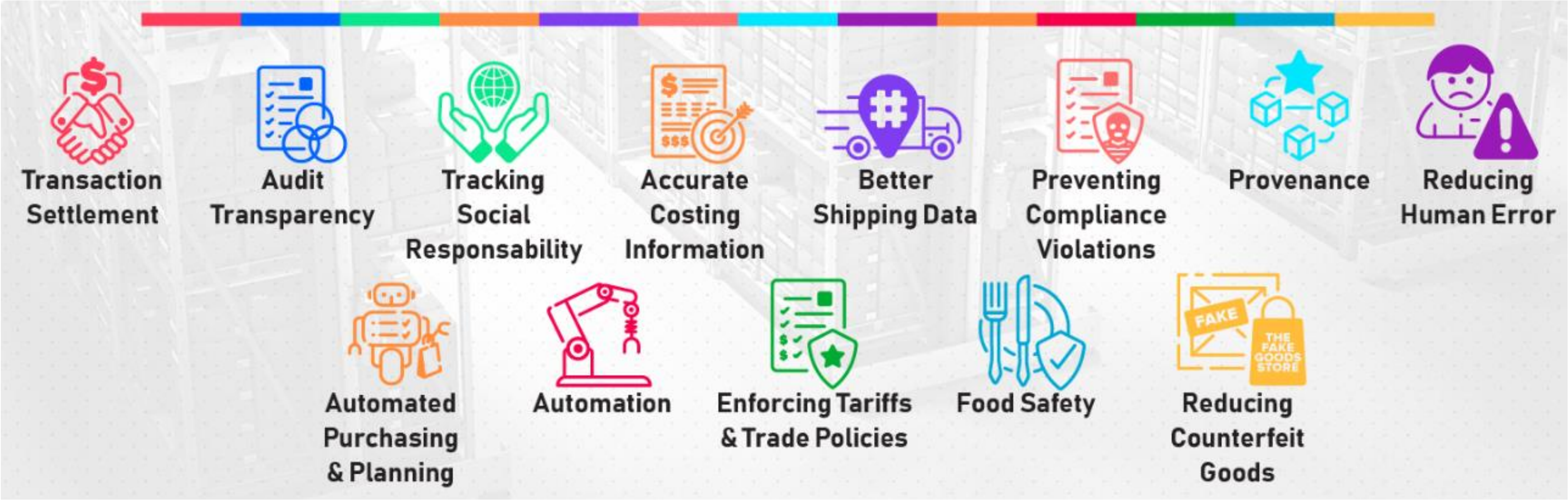
Tamper-proof exchange (of value and information)

Use Case: Supply Chain

- Global supply chains are inefficient, poorly tracked, and sometimes exploitative.
- E.g. Paperwork can account for substantial cost of container transport, and products are frequently mis-labeled.
- Create a shared IT infrastructure that streamlines workflows for stakeholders along the supply chain.
- Blockchain platform can facilitate accurate asset tracking, enable enhanced licensing of services, products, and software, and ultimately improves transparency into the provenance of consumer goods, from sourcing all the way to the point of consumption.

Food Safety
Automotive Industry
Pharma Supply Chain
Seafood Verification

Supply Chain Management through Blockchain (and AI)


Transaction Settlement
Audit Transparency
Tracking Social Responsability
Accurate Costing Information
Better Shipping Data
Preventing Compliance Violations
Provenance
Reducing Human Error
Automated Purchasing & Planning
Automation
Enforcing Tariffs & Trade Policies
Food Safety
Reducing Counterfeit Goods
FAKE
THE FAKE GOODS STORE

Use case: Banking and Finance

- Banking and financial services struggle with outdated operational processes, slow payment settlements, limited transparency, and security vulnerabilities.
- Blockchain technology can solve these problems with accountable and transparent governance systems, improved incentive alignment between stakeholders, secure technology infrastructure, and efficient business models.
- In addition, blockchain allows the digitization of financial instruments, which brings greater liquidity, lower costs of capital, reduced counterparty risk, and access to a broader investor and capital base.

Blockchain in Banking and Finance

Interbank Transactions

Remittance

Smart Contract Enforcement

Crypto Banking

Record Sharing & Storage

Clearing & Settlement

Loan Syndication

Regulatory Technology

KYC/AML

Regulatory Reporting

Trade Finance

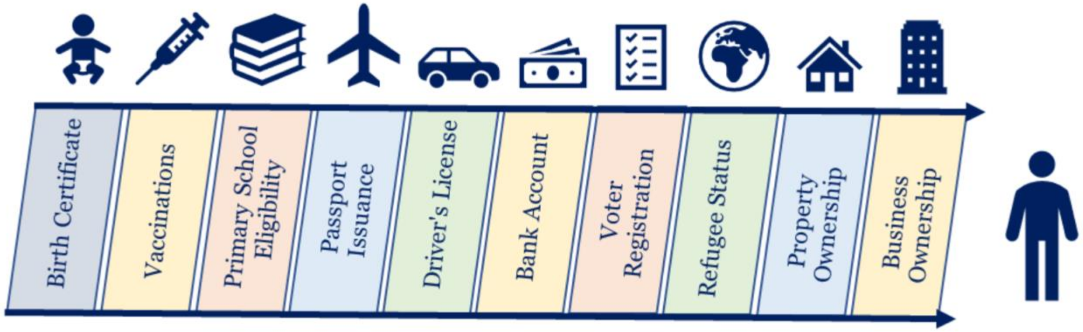
Data Security

Increasing Transparency

Serving The Unbanked

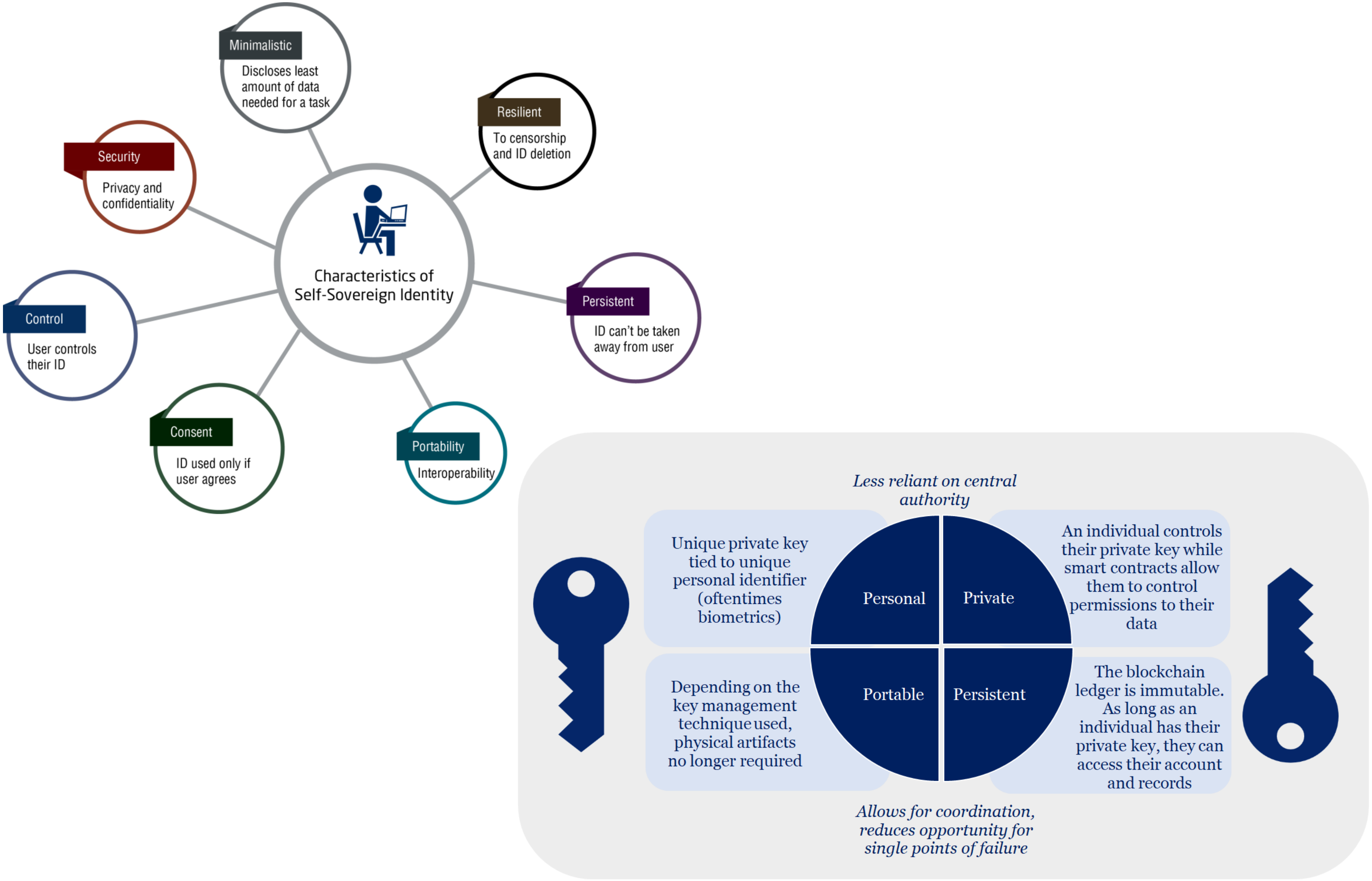
Use case: Digital Identity

- it becomes increasingly difficult to store and manage user and non-user identities securely.



- Digital identity theft negatively impacting millions of individuals. Individuals do fail to have full control over their online identities.
- A blockchain-based digital identity management system provides a unified, interoperable, and tamper-proof infrastructure with key benefits to enterprises, users, and IoT management systems.

Identity Management



Characteristics of Self-Sovereign Identity

Minimalistic
Discloses least amount of data needed for a task

Resilient
To censorship and ID deletion

Security
Privacy and confidentiality

Persistent
ID can't be taken away from user

Control
User controls their ID

Consent
ID used only if user agrees

Portability
Interoperability

Less reliant on central authority

Unique private key tied to unique personal identifier (oftentimes biometrics)

Personal

Private

An individual controls their private key while smart contracts allow them to control permissions to their data

Depending on the key management technique used, physical artifacts no longer required

Portable

Persistent

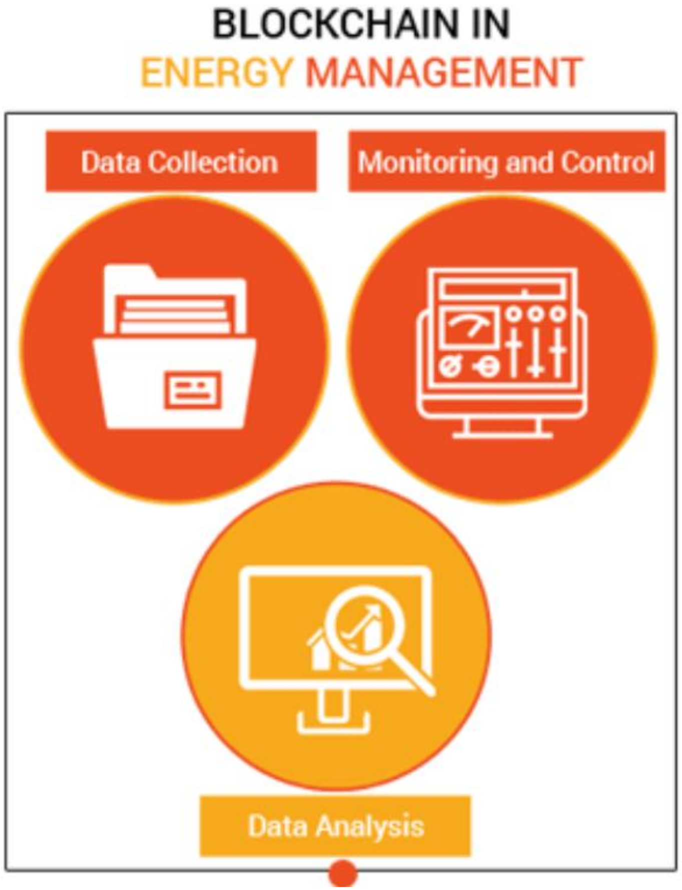
The blockchain ledger is immutable. As long as an individual has their private key, they can access their account and records

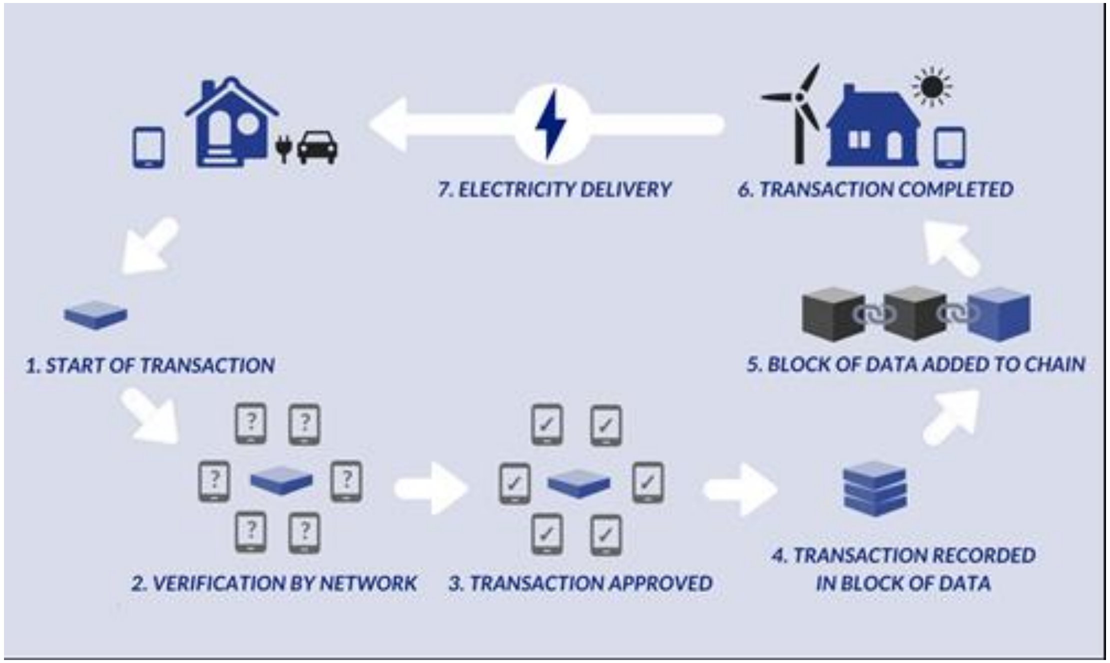
Allows for coordination, reduces opportunity for single points of failure

Use case: Energy and Sustainability

- Oil and gas companies suffer from siloed infrastructures and several issues concerning transparency, efficiency, and optimization.
- Blockchain has the potential to significantly increase business process efficiencies and reduce costs associated operations and distribution.
- Combined with IoT devices, a blockchain-enabled power grid automates billing and settlement, clears payments in real-time, and reduces utility costs.

Energy Trading

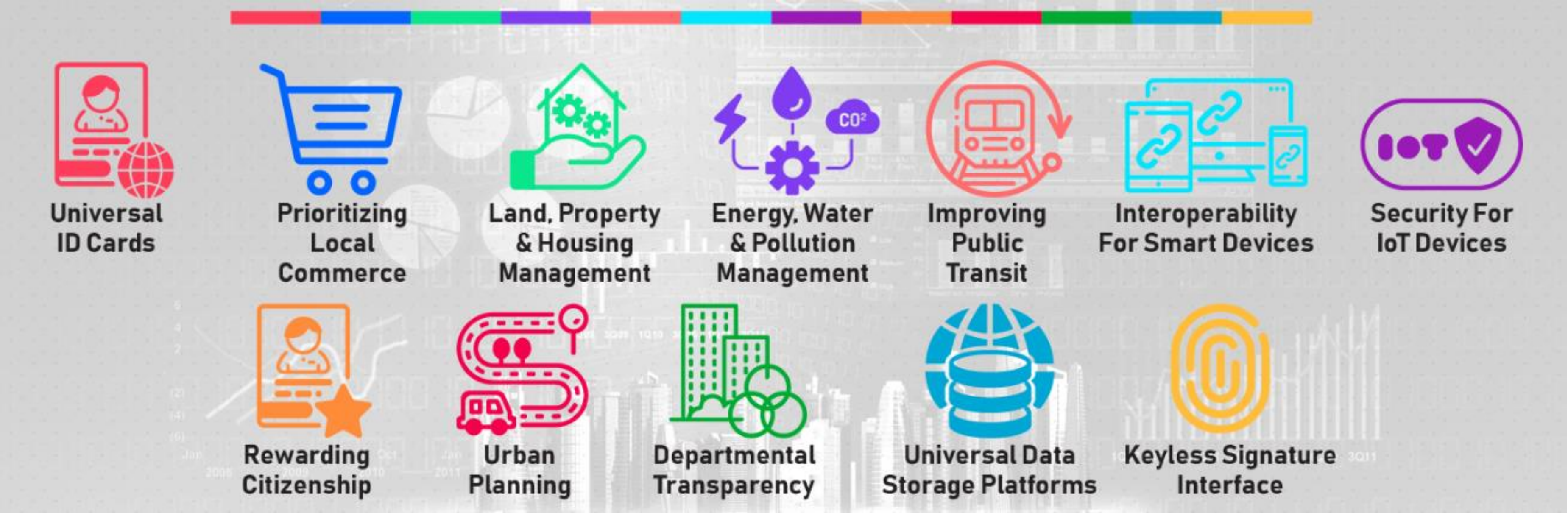




Use case: Government and the Public Sector

- Traditionally, national and local governments rely heavily on out-dated processes, legacy software, and inefficient organization structures.
- Yet, the public sector requires high-level security.
- (Encrypted) Ledger and smart contracts allow governments to build trust, improve accountability and responsiveness, increase efficiency, reduce costs, and create high-performing government functions with more secure, agile, and cost-effective structures.

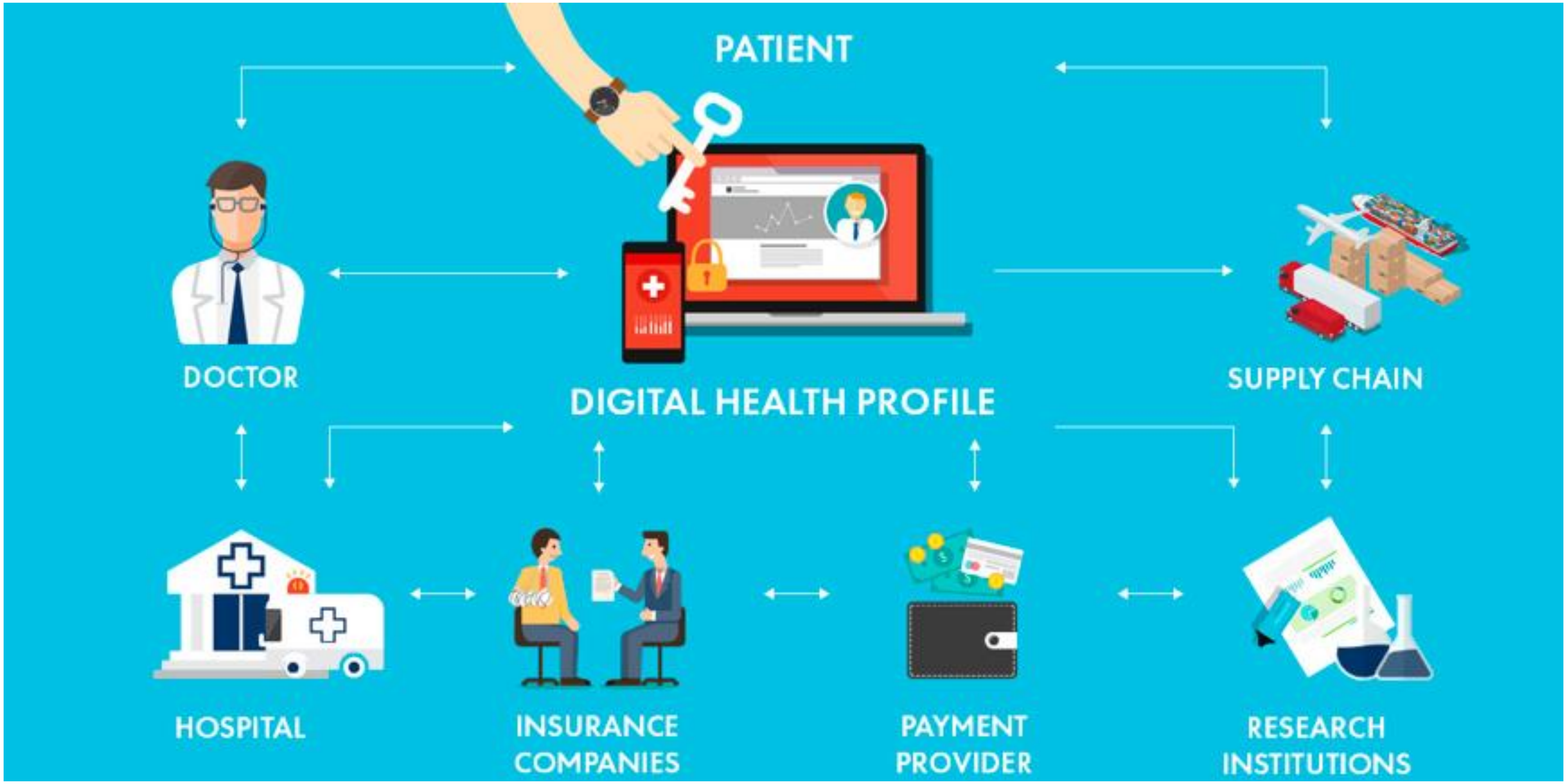
Blockchain for Smart Cities

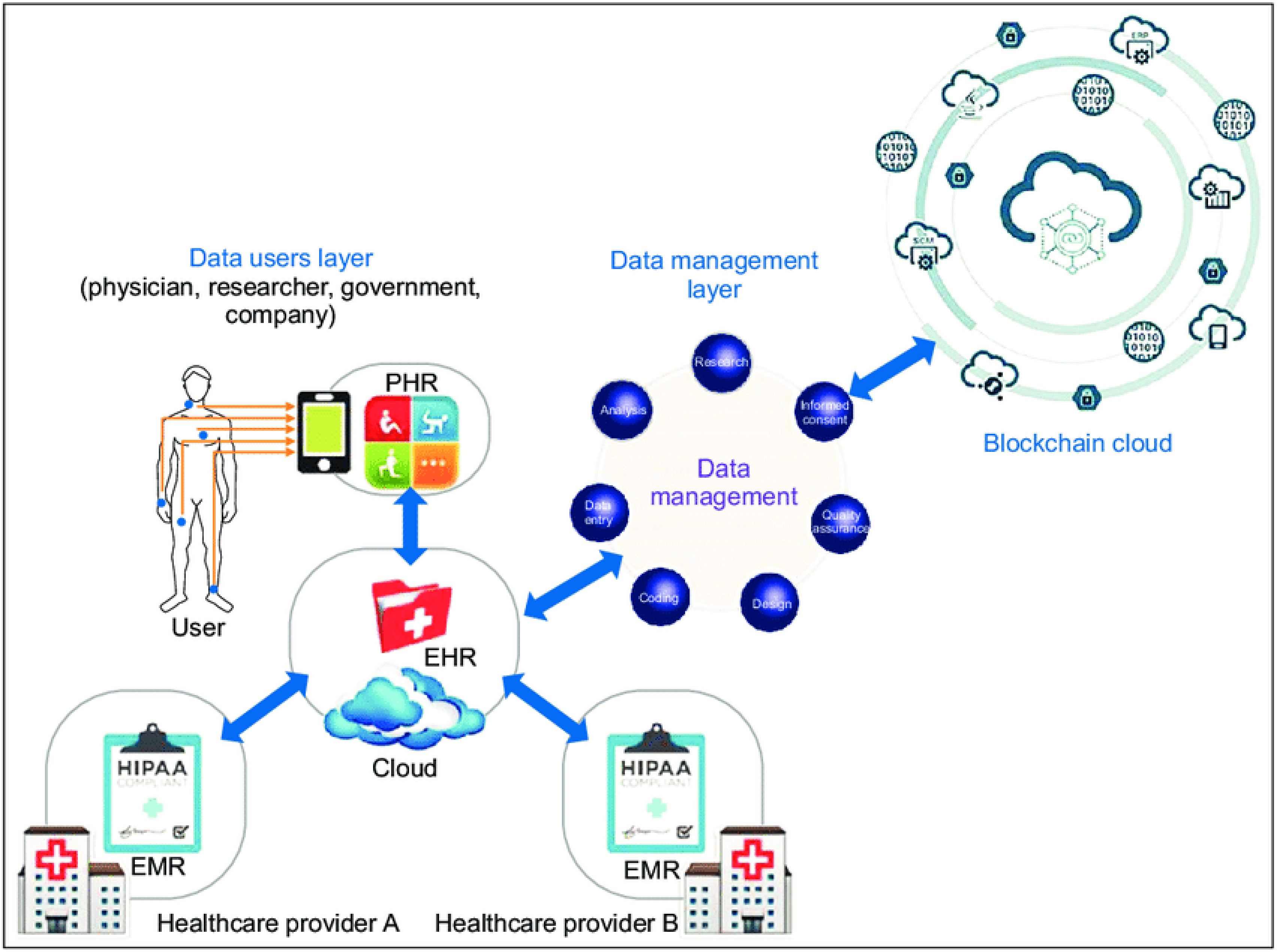

Universal ID Cards
Prioritizing Local Commerce
Land, Property & Housing Management
Energy, Water & Pollution Management
Improving Public Transit
Interoperability For Smart Devices
Security For IoT Devices
Rewarding Citizenship
Urban Planning
Departmental Transparency
Universal Data Storage Platforms
Keyless Signature Interface

Use case: Healthcare and the Life Sciences

- Misinformation, data silos, and the lack of communication between patients, providers, hospitals, and doctors plague the healthcare world.
- Blockchain-based data sovereignty and permissioned exchange scenarios will lead to faster, more efficient, and more secure medical data management and drug and medical device tracking.
- This could significantly improve patient care, facilitate the advancement to medical discoveries, ensure the authenticity of drugs circulating global markets, and more.

Blockchain in health care




Data users layer
(physician, researcher, government, company)
PHR
User
EHR
Cloud
Data management layer
Research
Analysis
Informed consent
Data management
Data entry
Quality assurance
Coding
Design
Blockchain cloud
ERP
SCM
HIPAA
COMPLIANT
EMR
HIPAA
COMPLIANT
EMR
Healthcare provider A
Healthcare provider B

Use case: International Trade and Commodities

- Trade financing and commodities exchange systems rely heavily on paper records that are prone to fraud, human error, and delays.
- With blockchain, every element of the trade finance process can be digitized, and only authorized parties can access data, validate documentation, and execute transactions.

Use case: Law

- Global legal services are forecasted to grow to $1,011 billion by 2021.
- While the industry grows, manual, laborious tasks take up the bulk of the work. Time wasted in document creation and management activities costs firms $9,071 per lawyer a year, equivalent to a 9.8% loss in the firm’s total productivity.
- Blockchain and AI can reduce the labor-intensive manual processes while providing accessibility, transparency, cost savings, speed, efficiency, and data integrity to the legal industry.

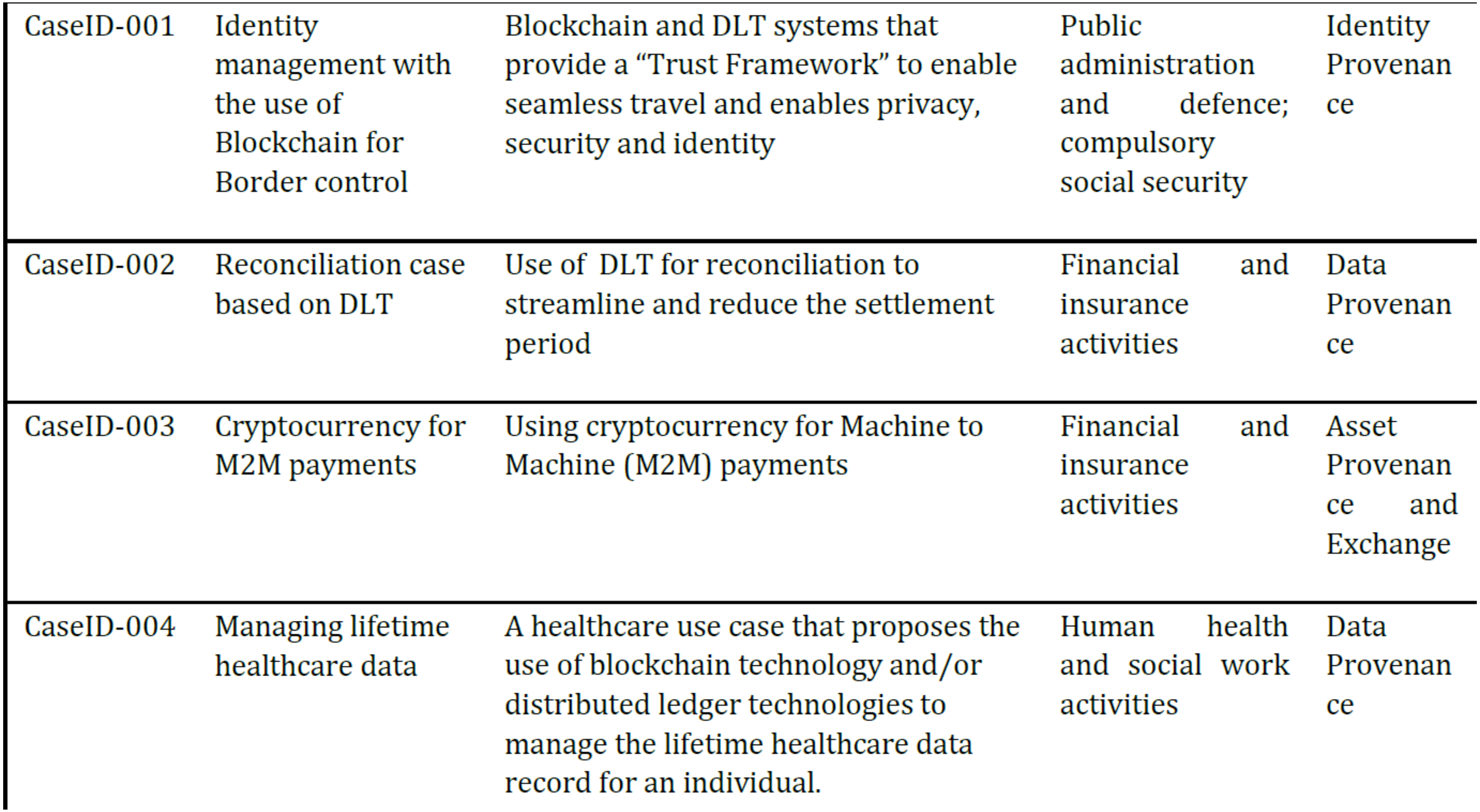
Use case: Media and Entertainment

- Digital piracy, fraudulent copies, infringed studio intellectual property, and duplication of digital items cost the entertainment industry costs the US film and TV industry an estimated $71 billion annually.
- With Blockchain, one can create a distributed ledger to track the life cycle of any content, which has the potential to drastically reduce piracy of intellectual property, protect digital content, and facilitate the distribution of authentic digital collectibles

Use case: Real Estate

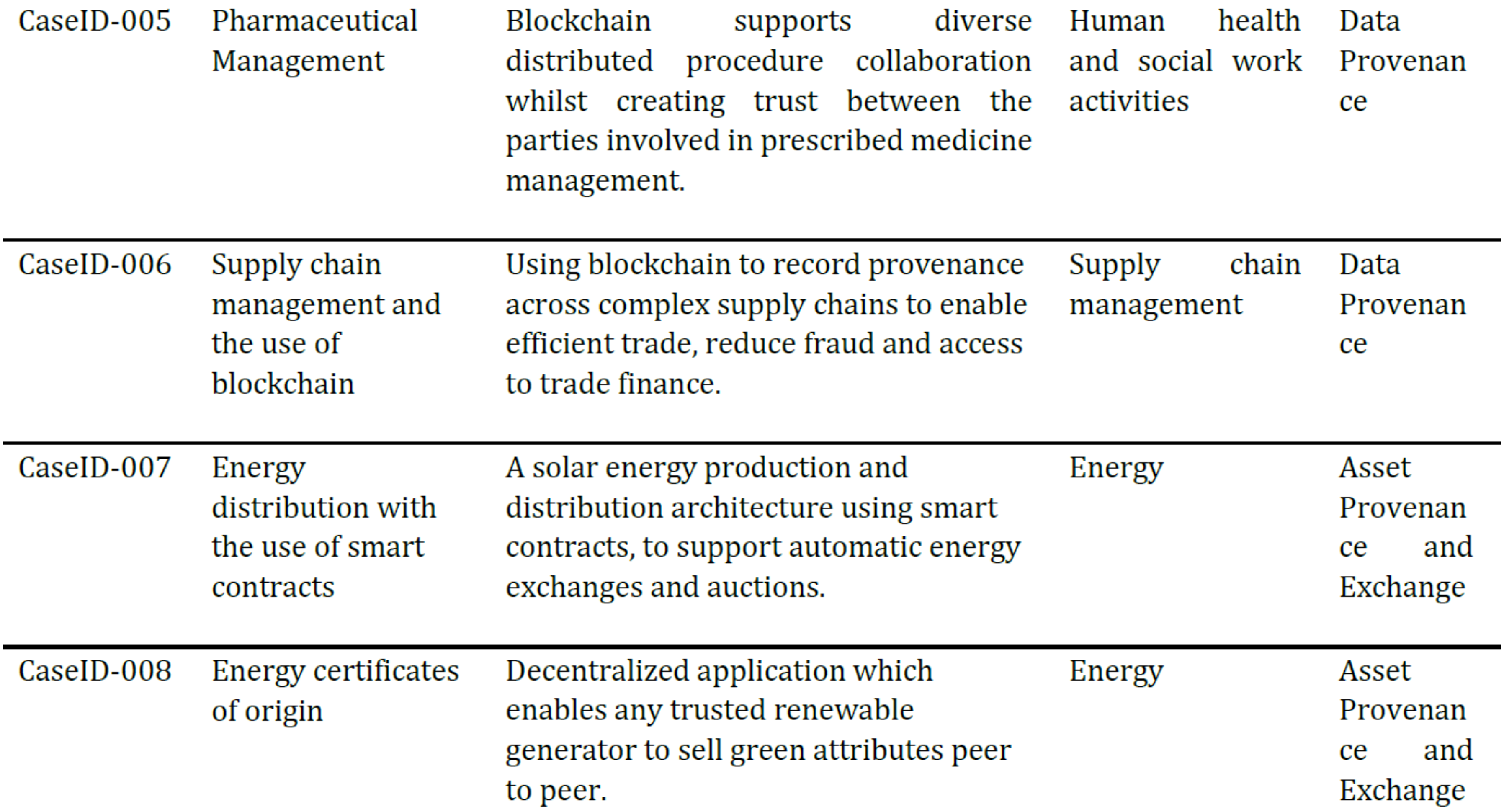
- Real estate investments are often inaccessible to many. Currently, it offers investors limited liquidity while requiring the involvement of multiple intermediaries, resulting in higher transaction costs.
- Blcokchain and smart contracts enhance real estate operations by eliminating intermediaries and optimizing processes.
- Furthermore, blockchain technology allows industries to digitize assets and financial instruments. This enables the fractionalization of ownership, increased liquidity, and democratized access to real estate investment opportunities.

ISO TC 307 use cases



CaseID-001	Identity management with the use of Blockchain for Border control	Blockchain and DLT systems that provide a “Trust Framework” to enable seamless travel and enables privacy, security and identity	Public administration and defence; compulsory social security	Identity Provenance
CaseID-002	Reconciliation case based on DLT	Use of DLT for reconciliation to streamline and reduce the settlement period	Financial and insurance activities	Data Provenance
CaseID-003	Cryptocurrency for M2M payments	Using cryptocurrency for Machine to Machine (M2M) payments	Financial and insurance activities	Asset Provenance and Exchange
CaseID-004	Managing lifetime healthcare data	A healthcare use case that proposes the use of blockchain technology and/or distributed ledger technologies to manage the lifetime healthcare data record for an individual.	Human health and social work activities	Data Provenance

ISO TC 307 use cases



CaseID-005	Pharmaceutical Management	Blockchain supports diverse distributed procedure collaboration whilst creating trust between the parties involved in prescribed medicine management.	Human health and social work activities	Data Provenance
CaseID-006	Supply chain management and the use of blockchain	Using blockchain to record provenance across complex supply chains to enable efficient trade, reduce fraud and access to trade finance.	Supply chain management	Data Provenance
CaseID-007	Energy distribution with the use of smart contracts	A solar energy production and distribution architecture using smart contracts, to support automatic energy exchanges and auctions.	Energy	Asset Provenance and Exchange
CaseID-008	Energy certificates of origin	Decentralized application which enables any trusted renewable generator to sell green attributes peer to peer.	Energy	Asset Provenance and Exchange

ISO TC 307 use cases

CaseID-009	Self-management of prosumer renewable energy mirco-grids	Utilizing blockchain technology for the invoicing and its smart contracts to govern the use of energy amongst these solar communities.	Energy	Asset Provenance and Exchange
CaseID-010	Smart inheritance proceeding	This use case describes a public service implementing statutory and wilful inheritance on blockchain, using smart contracts.	Public administration and defence; compulsory social security	Data Provenance Asset Provenance and Exchange
CaseID-011	Title registry system using blockchain land ledger	Blockchain real estate pilot programs being developed for land ownership administration	Real estate activities	Data Provenance
CaseID-012	Land Development Pipeline	Recoding land title ownership using blockchain	Real estate activities	Data Provenance

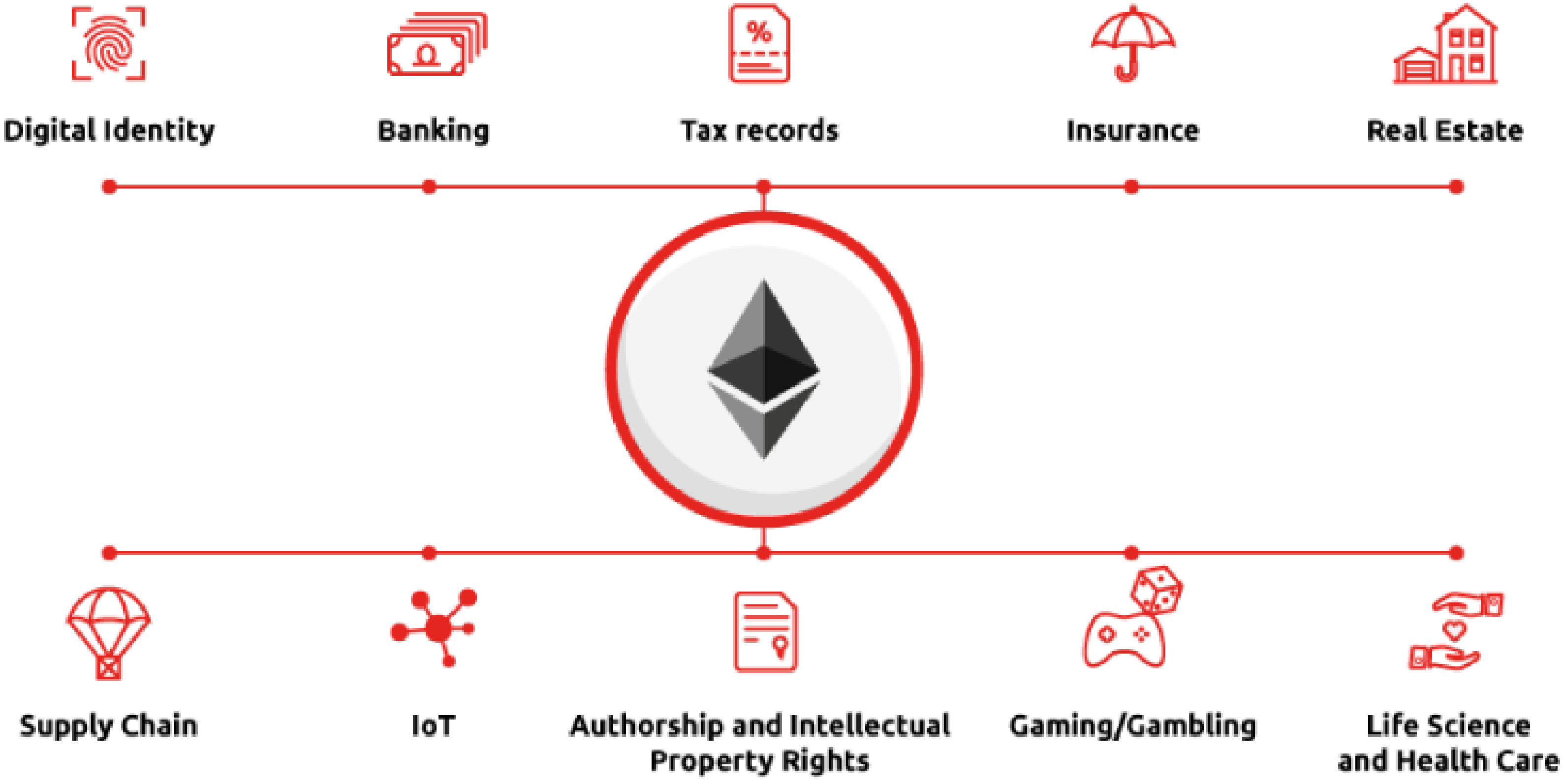
ISO TC 307 use cases

CaseID-013	Smart contracts for data accountability and provenance tracking	Smart contracts can be used to track data provenance and encode usage control policies regulating the access and usage (e.g., redistribution) of subject's data by controller and processors	Other service activities	Data Provenance
CaseID-014	Commercial fish stock management	A blockchain solution for the effective management of commercial fish stocks in wild fisheries	Agriculture, forestry and fishing	Data Provenance
CaseID-015	Sharing economy	Using blockchain and DLT to operate a sharing economy without a centralized platform.	Other service activities	Asset Provenance and Exchange
CaseID-016	Arbitration Use Case Based on DLT	Store legally binding, authentic, and immutable data on blockchain to solve traditional problems and reduce processing time and costs	Other service activities	Data Provenance

ISO TC 307 use cases

CaseID-017	Recruitment	With Digital Identity based on Blockchain/DLT infrastructure can provide multi-source identity system (for human being) utilized, recruitment process shall be optimized by increasing the transparency both for the hirers and the candidates.	Other service activities	Identity Provenance

Blockchain Smart contracts: Use cases



Digital Identity

Banking

Tax records

Insurance

Real Estate

Supply Chain

IoT

Authorship and Intellectual Property Rights

Gaming/Gambling

Life Science and Health Care

Securing Blockchain

- In a blockchain system, data is stored as part of transactions.
- Transaction data include both the metadata used for verification and administration in the blockchain (e.g. signature, transaction fee) as well as the content data processed by the transaction (e.g. payment orders, certificates).
- Normally, these transaction data are available in unencrypted form and can therefore be viewed by all nodes with appropriate rights

Securing Blockchains

- Several blockchain systems allow use of smart contracts, which aims to make possible the tamper-proof execution of contracts between parties unknown to or mistrusting each other.
- Security problems range from bugs in the code—which cannot be corrected for technological reasons—and manipulable random numbers to a lack of authenticity for data which is entered from the real world and processed in the contract

Securing Blockchains

- Security and trust in a blockchain system are largely based on cryptographic primitives such as signatures or hash functions
- Blockchain on its own does not solve IT security problems
- Choosing a suitable blockchain model is important
- When designing blockchains, security aspects must be taken into account early on
- Sensitive data requiring long-term protection must be specially protected in a blockchain
- Standardised security levels for blockchains must be defined and enforced

Security Advisory

- Confidentiality is difficult to achieve in blockchains.
- Sensitive data should not be stored or processed directly or without protection on a blockchain.
- Cryptographic mechanisms should be state-of-the-art, and a good key management is required.
- Mechanisms for anonymization and pseudonymization on blockchains are often not reliable in practice
- The properties of the network directly influence the security of the entire blockchain system.
- The immutability of the code of smart contracts and their automatic execution require utmost care in programming