

Blockchain Technology and Applications Summary

D. Papaioannou, Prof. Ioannis Pitas
Aristotle University of Thessaloniki
pitas@csd.auth.gr
www.aiia.csd.auth.gr
Version 3.1

Blockchain Technology and Applications



- **Introduction to Cryptography**
- Introduction to Blockchain
- Introduction to Blockchain Consensus Algorithms
- Blockchain Technology
- Blockchain Applications
 - Blockchain and Cryptocurrencies
 - Blockchain and Identity
 - Blockchain and Biometrics

Blockchain Technology and Applications



- Introduction to Cryptography
- **Introduction to Blockchain**
- Introduction to Blockchain Consensus Algorithms
- Blockchain Technology
- Blockchain Applications
 - Blockchain and Cryptocurrencies
 - Blockchain and Identity
 - Blockchain and Biometrics

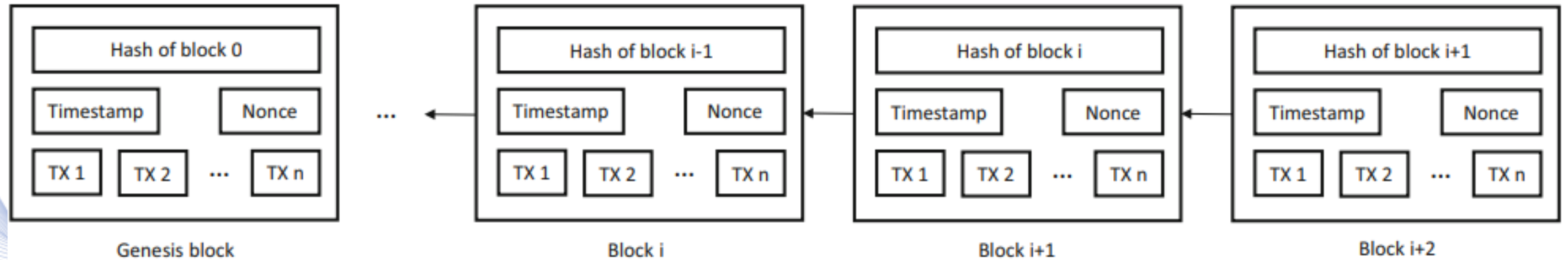
Introduction to Blockchain



Blockchain essentially consists of a ***sequence of blocks*** each one of them holding a complete list of transactions records.

Can be defined as a database system which holds data sets secured and bounded to each other in a ***chain***, using crypto-graphic principles, in form of packages (blocks) where each one of the blocks consist of various transactions (TX-n).

Introduction to Blockchain



The blocks structure.

Introduction to Blockchain

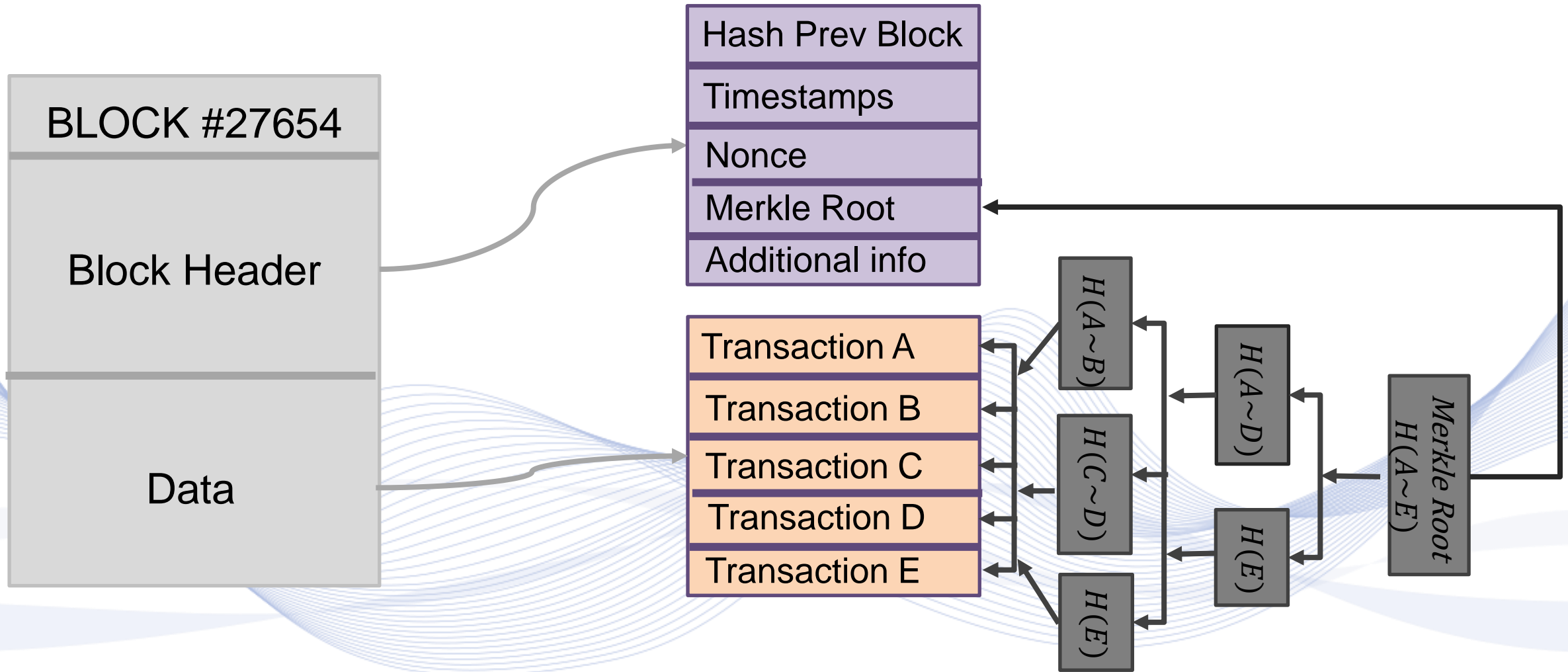


Each block contains the header where ***timestamp, hash for the past block, hash for the block itself*** and a ***nonce*** are stored inside. The above structure can ensure the integrity of the chain from the first to the last block.

First block is known as “***Genesis block***” and does not contain hash value for the previous block.

Nonce is a 32 – *bit* random integer number used in order to validate the hash value produced for the specific block.

Introduction to Blockchain



Introduction to Blockchain



Blockchain technology is a ***peer-to-peer***, distributed network ledger which is secured by cryptography methods, immutable, append-only and updated only via consensus or agreement between nodes.

- ***Peer-to-peer***: No central authority governs this network, but instead all participants (peers) must communicate directly with each other. In case of transaction cash, this feature allows exchanges to be achieved directly between peers without third-party interaction.

Introduction to Blockchain



- ***Distributed Ledger:*** Ledger is spread all over the network and between all the nodes (peers), and each node keeps a copy of the entire ledger.
- ***Cryptographically-secure:*** Cryptography assures the security, making in that way the ledger safe in terms of misuse and tampering. Data origin authentication and integrity is necessary for that step.

Introduction to Blockchain



- ***Append-Only:*** Data enter in the chain only via time-ordered sequential order. Once data enter the chain is almost impossible to change them (immutability).
- ***Updated via consensus:*** The last critical aspect, no central authority upgrades the ledger but instead, the upgrades that are being made in the blockchain are invoked through various guidelines determined by the chain protocol and are entered only when a consensus has been made between the nodes (participants) in the chain.

Blockchain Technology and Applications



- Introduction to Cryptography
- Introduction to Blockchain
- **Introduction to Blockchain Consensus Algorithms**
- Blockchain Technology
- Blockchain Applications
 - Blockchain and Cryptocurrencies
 - Blockchain and Identity
 - Blockchain and Biometrics

Blockchain Consensus



- In synchronous communication models a clock consistency frequency is being used, allowing for a limited time the presence of errors.
- The consensus protocols relying on:
 - Synchronous communication models.
 - Weak synchronous communication models, where a timeout method is used for the transition of messages.

Blockchain Consensus



- Blockchain is using weak synchronization communication models, where a message even if delayed, it would eventually reach the recipient within a certain time limit.
- A solution to Byzantine Generals' Problem through a consensus protocol where each individual node of the chain could reach an agreement about the state of the chain.

Blockchain Consensus



- Those consensus algorithms must guarantee:
 - **Consistency:** If a message (transaction) is verified for a loyal node then it will be verified for the remaining loyal nodes too. So, if honest nodes is the majority then the double-spending attacks will never be a success in a blockchain system.
 - **Liveness:** All valid messages (transactions) between loyal nodes must and eventually will be confirmed, ensuring in that way the system's sustainability.

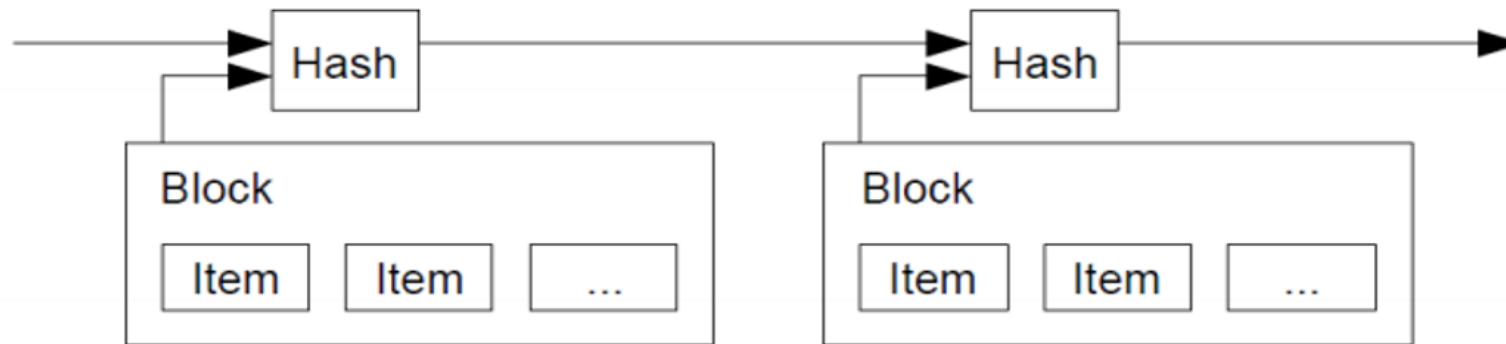
Proof of Work



- ***Proof of Work (PoW)***: Is an algorithm (protocol) formed around a cryptographic zero-knowledge proof where it involves two independent ***nodes, the prover*** (requestors) and ***the verifier*** (provider).
- The prover also called ***miner*** executes a time consuming hard computational task (cryptographic task or mathematical problem) trying to reach a specific goal and present it to verifier or in group of them in order to validate the task.

Proof of Work

- PoW consensus protocol is also used for adding new blocks in the chain.
- As we know blocks in the chain are append-only in a sequence of timestamped blocks using hash values for verifying their existence.



Timestamps.

Proof of Work

- Miners via the requested computational task are actually trying to produce a new hash for the candidate block, which is supposed to be less than a dynamically varying target value (consensus rule).
- Mining the hash performed using three known values:
 - Hash for the previous block.
 - Hashes of the transactions inside the block.
 - And the blocks creating time.
- Goal is to create the “nonce” value which fits better in the pattern.

Proof of Work

- When a miner generate such value then it needs to be verified from at least 51% of the nodes in order to be accepted (***winning value***).
- The verification is considered as a low computational procedure which can last almost a few seconds, if the process indicates that the block is valid then the node is add it in his version of the chain.
- Once a winning value is detected then the miner is being rewarded with the amount of Bitcoins, that correspond to the effort he provided to the chain as well as the sum of all fees.

Blockchain Technology and Applications



- Introduction to Cryptography
- Introduction to Blockchain
- Introduction to Blockchain Consensus Algorithms
- **Blockchain Technology**
- Blockchain Applications
 - Blockchain and Cryptocurrencies
 - Blockchain and Identity
 - Blockchain and Biometrics

Smart Contracts



- **Smart Contracts** is self-execute programs with specific rules who runs in the blockchain and used in the chain for ensuring **security**.
- Solidity is a Turing-complete programming language used in Ethereum blockchain for writing smart contracts.
- Turing-Completeness is a property over a language which allows to write any logic inside it.

Decentralized Applications



- Decentralized Applications it contains an interface for people to interact with the blockchain. It consist of backend and frontend design which is basically a smart contract.
- We can think smart contracts as a form of API which is helping to build applications which interact with a blockchain and hence they are decentralized.
- A DApp example is the steemit, a kind of twitter, which is totally decentralized since it is not loading from a central server but from a blockchain.

Decentralized Autonomous Organizations (DAOs)



- DAOs is essentially a blockchain organization model which is designed in order to address a challenge that face every organization and industry: the principal-agent dilemma.
- ***Principal-agent Dilemma:*** When we have a system structure where an individual or entity (agent) have the rights to act or make decisions on behalf of another entity (the principal) there exists an inherit risk in the different goals, priorities of the respective parties.

The DAO Attack



- In 2016, Vitalin Buterlin and a group of others created the first DAO organization in the Ethereum blockchain, the concept was the creation of Investor-directed venture capital fund which would help the development of DApps.
- It was crowd-funded by tokens achieving the world's most successful crowd founding campaign (\$150 million) and that because people just believed in the whole idea of decentralization.

The DAO Attack

- But there was an error in the way that smart contracts were coded for this organization leading in a huge attack and hack in June 2016 for around 50 million dollars.
- The attackers didn't do something illegal they just found that flaw in the code and they use it to leech money out of the DAO account into their own account using an attack contract.
- Everyone could see this glitch but none could do something for that since DAO is autonomous and therefore its governed by its own code.

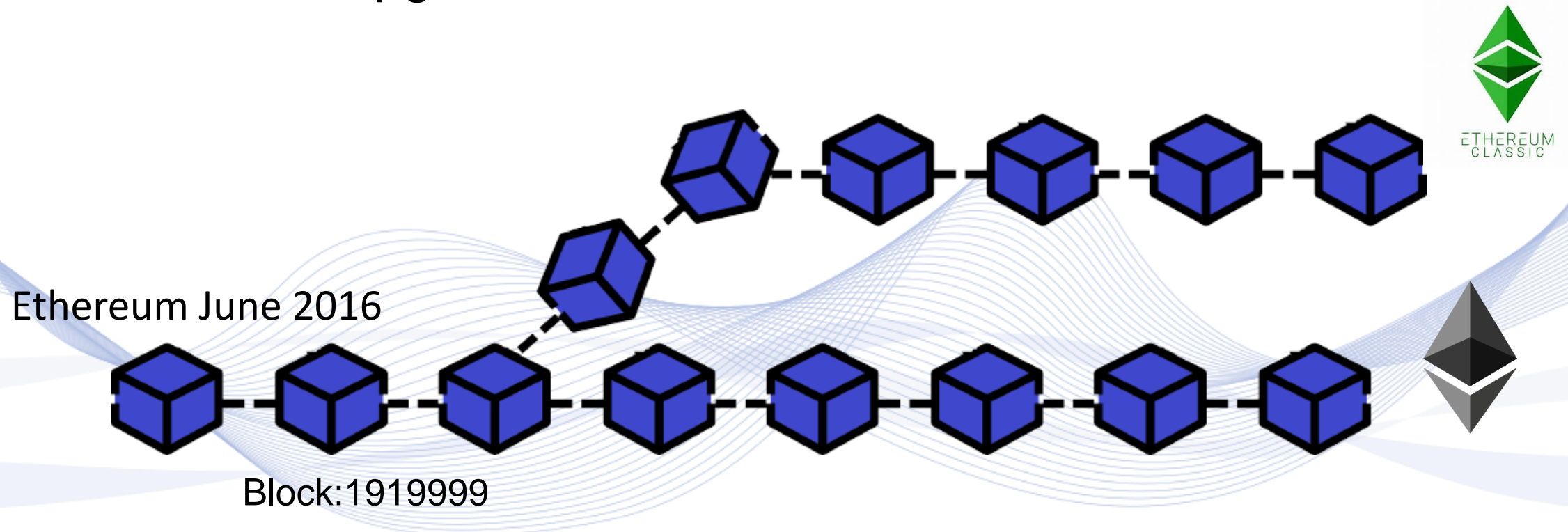
The DAO Attack



- The flaw allowed the attackers to perform that valid transaction, as a valid part of the contract and so on since blockchain is immutable they could not do anything about this.
- But according to the way DAO is coded there was a failure save mechanism which didn't allowed the funds taken out entirely, they had to wait 30 days until the funds move to their account.
- And then a dilemma arised for the community: Is code the law?

Soft and Hard Forks

- Hard forks is radical update to the network's protocol which make previous invalid blocks and transactions valid. During a hard fork all nodes must upgrade to the latest version of the blockchain.

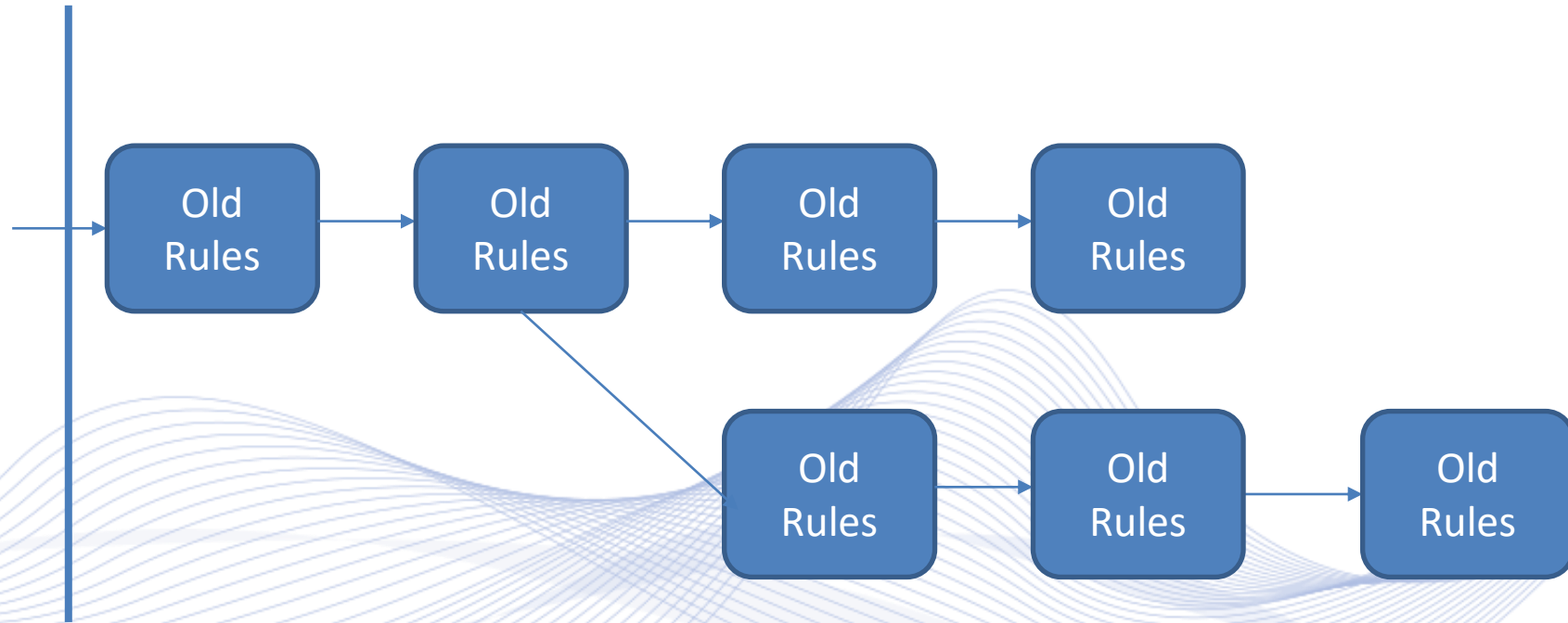


Soft and Hard Forks

Hard Fork

Blocks mined from no upgraded miners.

Blocks mined from upgraded miners.

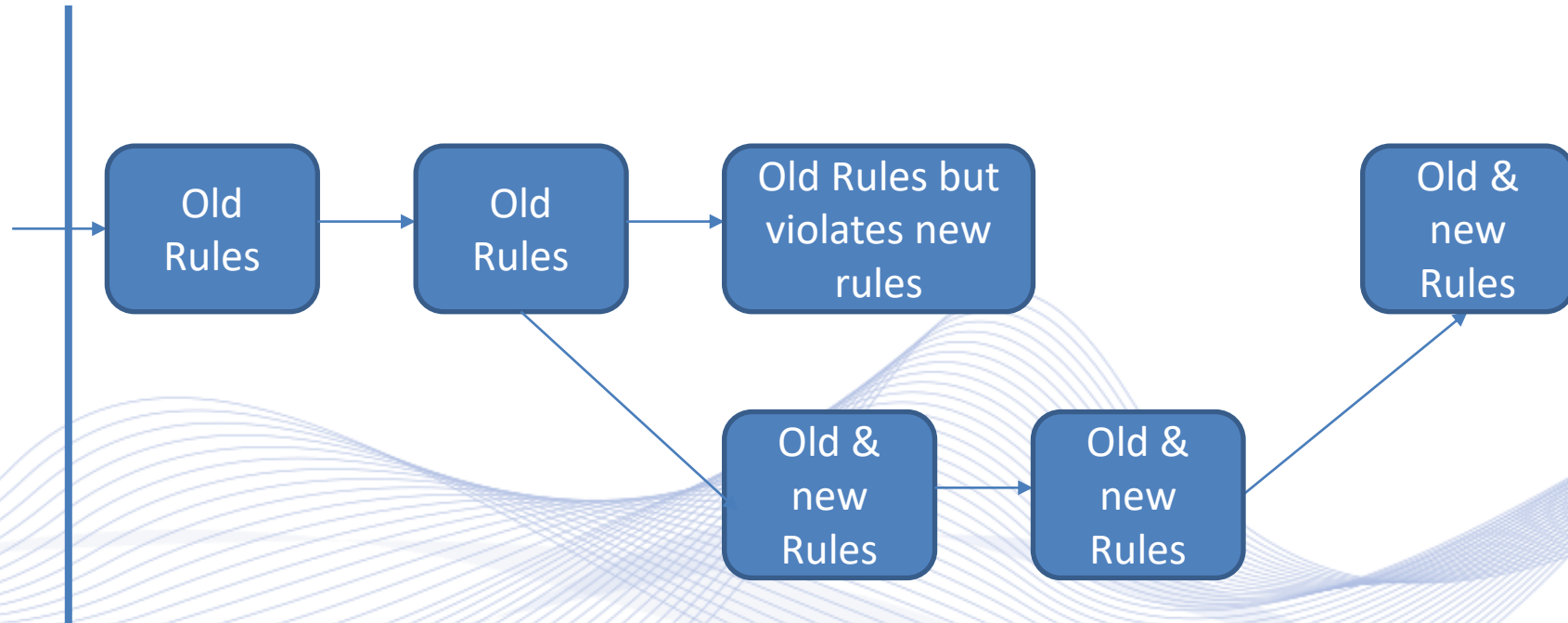


Soft and Hard Forks

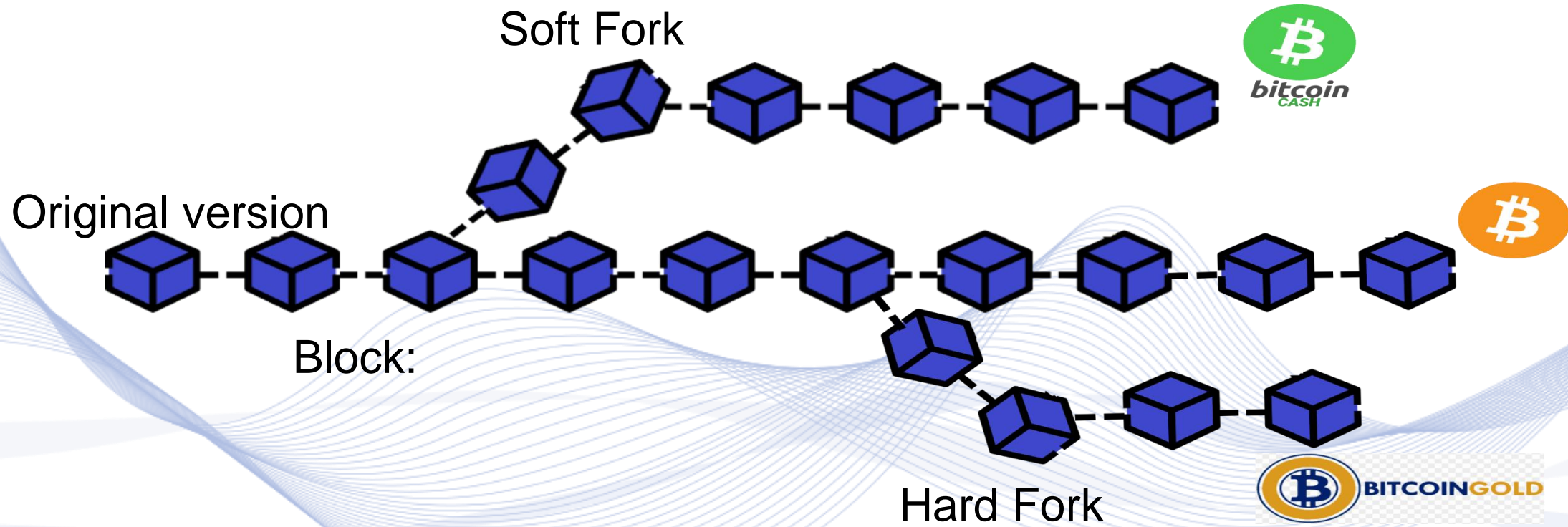
Soft Fork

Blocks mined from no upgraded miners.

Blocks mined from upgraded miners.



Soft and Hard Forks



Blockchain Technology and Applications



- Introduction to Cryptography
- Introduction to Blockchain
- Introduction to Blockchain Consensus Algorithms
- Blockchain Technology
- **Blockchain Applications**
 - Blockchain and Cryptocurrencies
 - Blockchain and Identity
 - Blockchain and Biometrics

Technology and Applications



- ***Blockchain technology can be used for:***
 - Cryptocurrency
 - Distributed identity management
 - Biometrics
 - Supply Chain
 - Internet of Things (IoT)
 - e-Government
 - Healthcare: Where healthcare providers can use the blockchain to record medical data for their customers.
 - Passports.

Technology and Applications



- **Blockchain technology can be used for:**
 - **Railway company:** Tickets are purchased online using debit or credit cards, where the card company usually collects a fee for the execution of the transaction. Blockchain Technology, can be used so the railway processor saves the extra tax by moving the ticket process in the blockchain.
 - The tickets here represent a block inserted in the chain. So, here the chain is a set of transaction records referring to the route or the train network

Technology and Applications



- ***Blockchain technology can be used for:***
 - ***E-books:*** Blockchain enable writers to earn much more profits rather than using amazon or other publishers' companies.
 - ***Music:*** Blockchain allows the rights of recorded music profits to go directly to artists without involving companies such as Apple and Spotify.

Blockchain Technology and Applications



- Introduction to Cryptography
- Introduction to Blockchain
- Introduction to Blockchain Consensus Algorithms
- Blockchain Technology
- Blockchain Applications
 - **Blockchain and Cryptocurrencies**
 - Blockchain and Identity
 - Blockchain and Biometrics

Cryptocurrency







- Usage of Blockchain in financial:
 - **Investment Management:** Blockchain transparency provides easily verification transaction services, it enhance the security of the overall data since they stored in immutable records.
 - **Cross-Border Transactions:** Due the globalization effect, businesses or any financial entity can perform faster and more efficiency cross-border transactions, by eliminating the need of middleman (etc. bank).
 - **Trade Finance:** Blockchain can digitize the finance trading in order to achieve transparent governance, reduce the number and complexity of middleman's, fast processing, eliminate any possible risks and frauds.

Cryptocurrency



- Blockchain as a decentralized mechanism can have huge impact in economy by creating **electronic currencies** which attempts to be more **trustworthy** and **secure** than the physical money due to:
 - There is no central authority controlling the money flow.
 - Customers are no longer needed to put their “faith” in centralized systems (e.g. bank) but instead they must trust the technology.
 - Transparent.

Cryptocurrency Institution

Technology	Blockchain			
Protocol - Coins	Bitcoin 	Ethereum 	Ripple 	Neo 
Tokens	No Tokens	<ul style="list-style-type: none">• TRX• SNT• AE• PPT	No Tokens	<ul style="list-style-type: none">• ACAT• DBC• TNC• IAM

Cryptocurrency



- ***Cryptocurrency***: Is defined as an electronic or digital currency that is ***secured*** via a ***cryptographically mechanism***. Many cryptocurrencies are using decentralized networks like the blockchain technology.

Blockchain Technology and Applications



- Introduction to Cryptography
- Introduction to Blockchain
- Introduction to Blockchain Consensus Algorithms
- Blockchain Technology
- Blockchain Applications
 - Blockchain and Cryptocurrencies
 - **Blockchain and Identity**
 - Blockchain and Biometrics

Distributed Identity Management



- Identities are an integral part of a functionally stable society or economy system.
- They are usually information about people, things or places. The data of this information are usually collected by centralized entities (e.g. government) and stored on central databases (e.g. government central servers).
- Companies that holds this data are usually vulnerable to infringements or frauds.

Distributed Identity Management



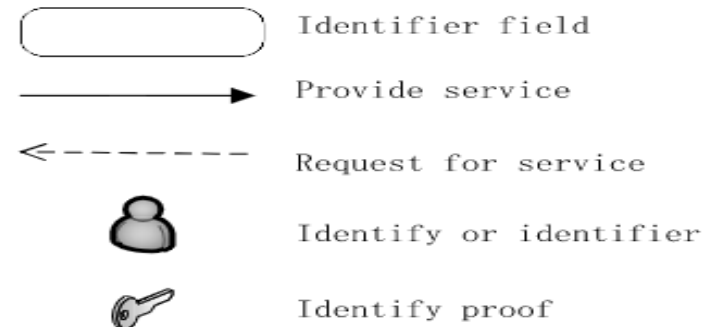
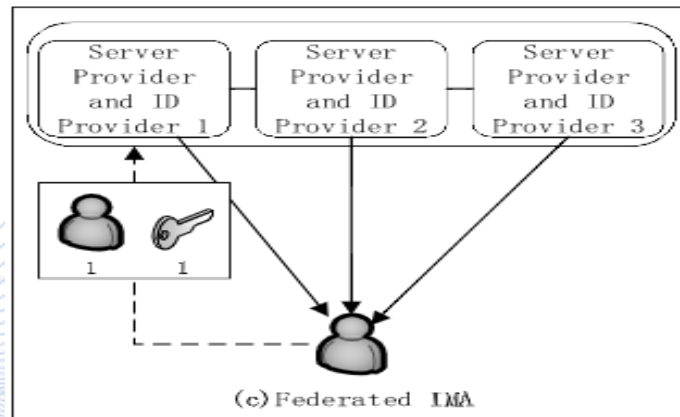
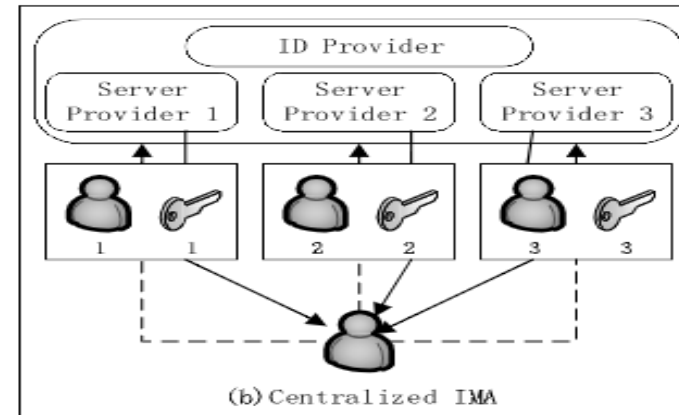
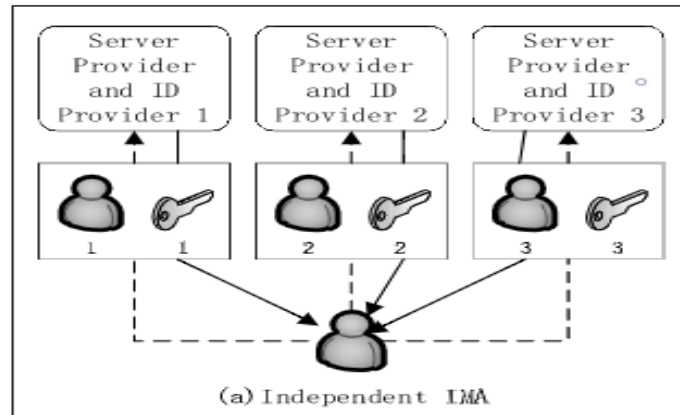
- A ***digital identity*** constituting the use of personal data on the internet as well as a set of hidden data created by the actions of the individual on the internet.
- Data that contribute to the creation of a digital identity are usernames and passwords, medical history, drive license, purchasing history and more.

Distributed Identity Management



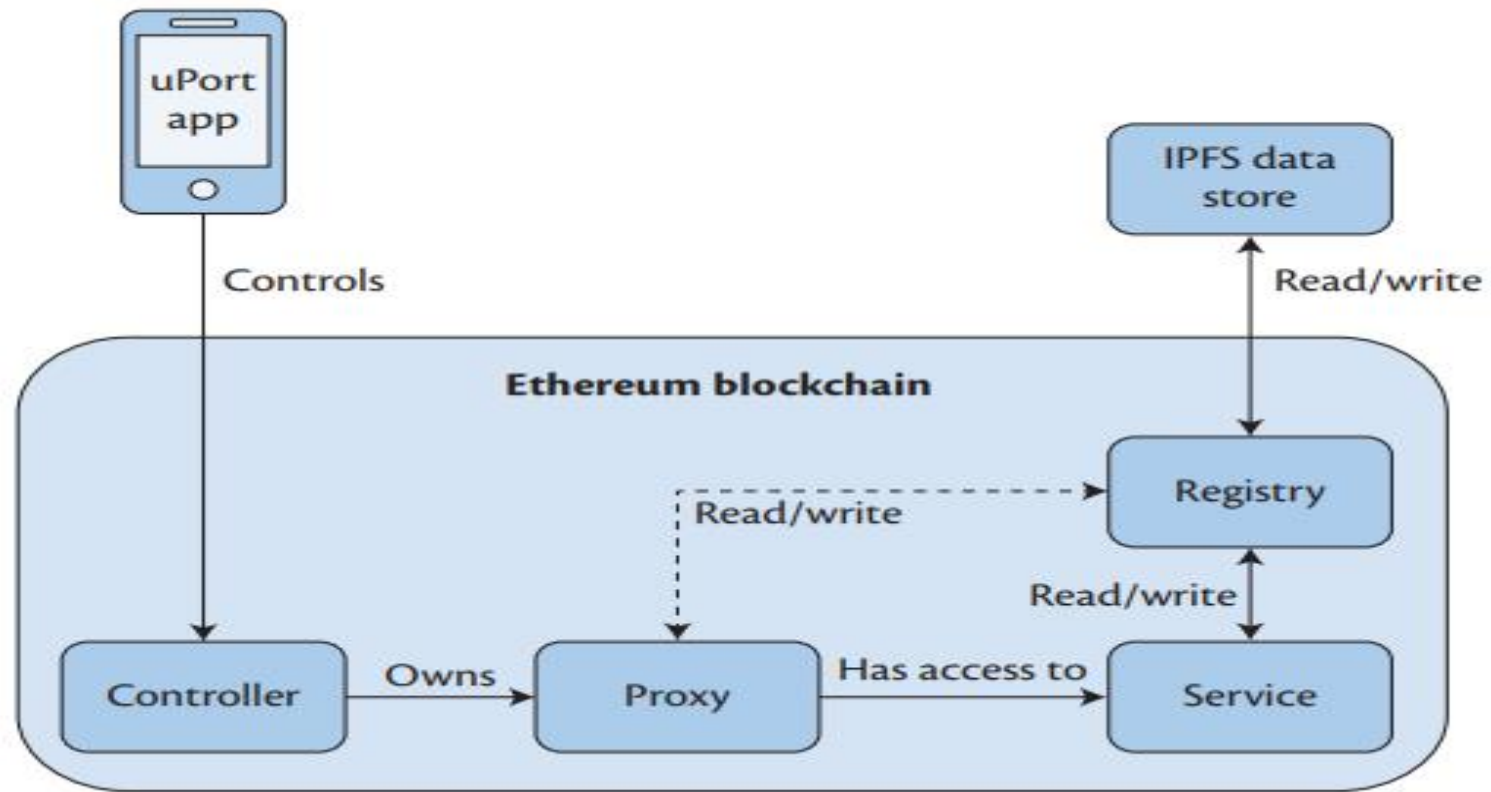
- A ***decentralized identifier (DID)*** can be considered as a pseudo-anonymous identifier refer to a person or company.
- Private key used to secure each DID.
- Only the holder of the PK can prove that he control or own this identity.
- Each individual can have multiple DIDs.

Distributed Identity Management



Identity Management Architectures.

- **uPort** is considered as a decentralized open-source identity management framework with main goal to provide a decentralized identity to all. uPort is designed based on the Ethereum DLT system and involves smart contracts.
- Each uPort identity use two smart contracts templates:
 - **Controller:** To generate new identity, we first create a pair of asymmetric keys within the user's uPort mobile application, and then the transaction is sent to Ethereum where a new controller creation is achieved by storing a public key reference.
 - **Proxy:** Proxy just holds a reference to the created controller.



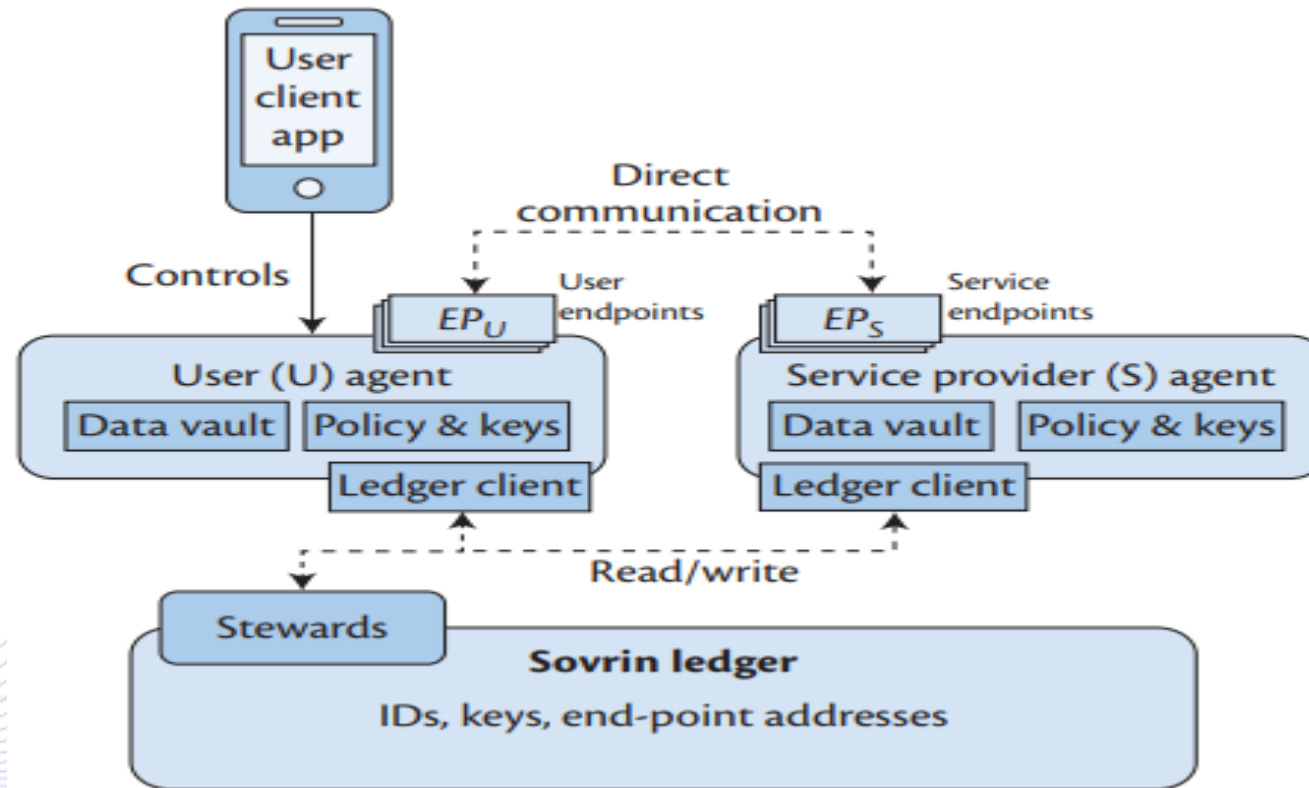
uPort Architecture.

Sovrin



- **Sovrin** is an identity open-source network for storing identity records and is based on permissioned DLT.
- Even is Sovrin is public, only trustworthy organizations (**stewards**) can run the nodes of the blockchain, which they take part in the consensus protocol. Ledger is permissioned.
- **Sovrin Foundation** assures the proper government of the stewards as well as their commitment to the legal agreement known as **Sovrin Trust Framework**.

Sovrin



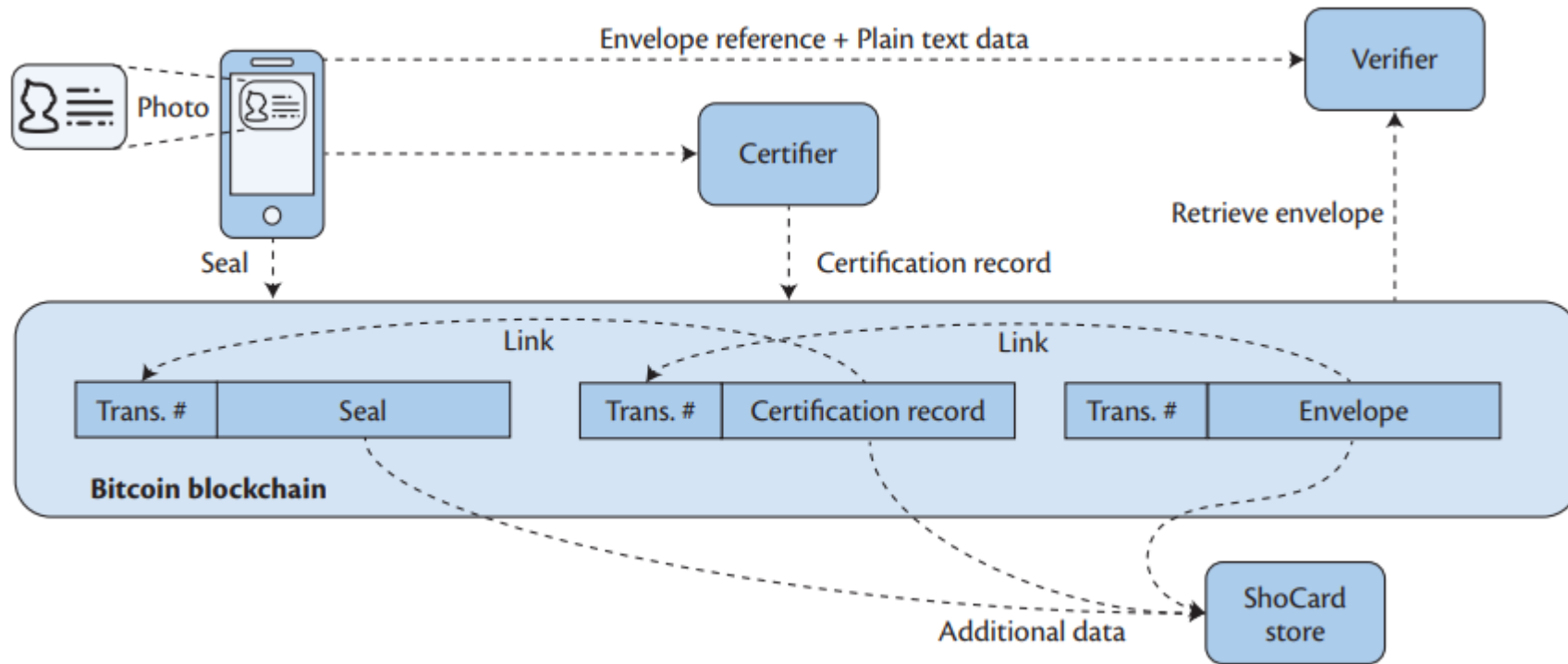
Sovrin Architecture.

ShoCard



- ShoCard is a digital ID card that operates on a mobile phone and combines ***user identifier, additional identity features*** and ***existing trusting credentials*** (e, g, driver's license, passport) using hash functions and storing them in the bitcoin chain.
- ShoCard utilizes the Bitcoin as timestamp service in order to save the user's id information in the Bitcoin blockchain with cryptographic hashes.

ShoCard



ShoCard Architecture.

Blockchain Technology and Applications



- Introduction to Cryptography
- Introduction to Blockchain
- Introduction to Blockchain Consensus Algorithms
- Blockchain Technology
- Blockchain Applications
 - Blockchain and Cryptocurrencies
 - Blockchain and Identity
 - **Blockchain and Biometrics**

Blockchain and Biometrics



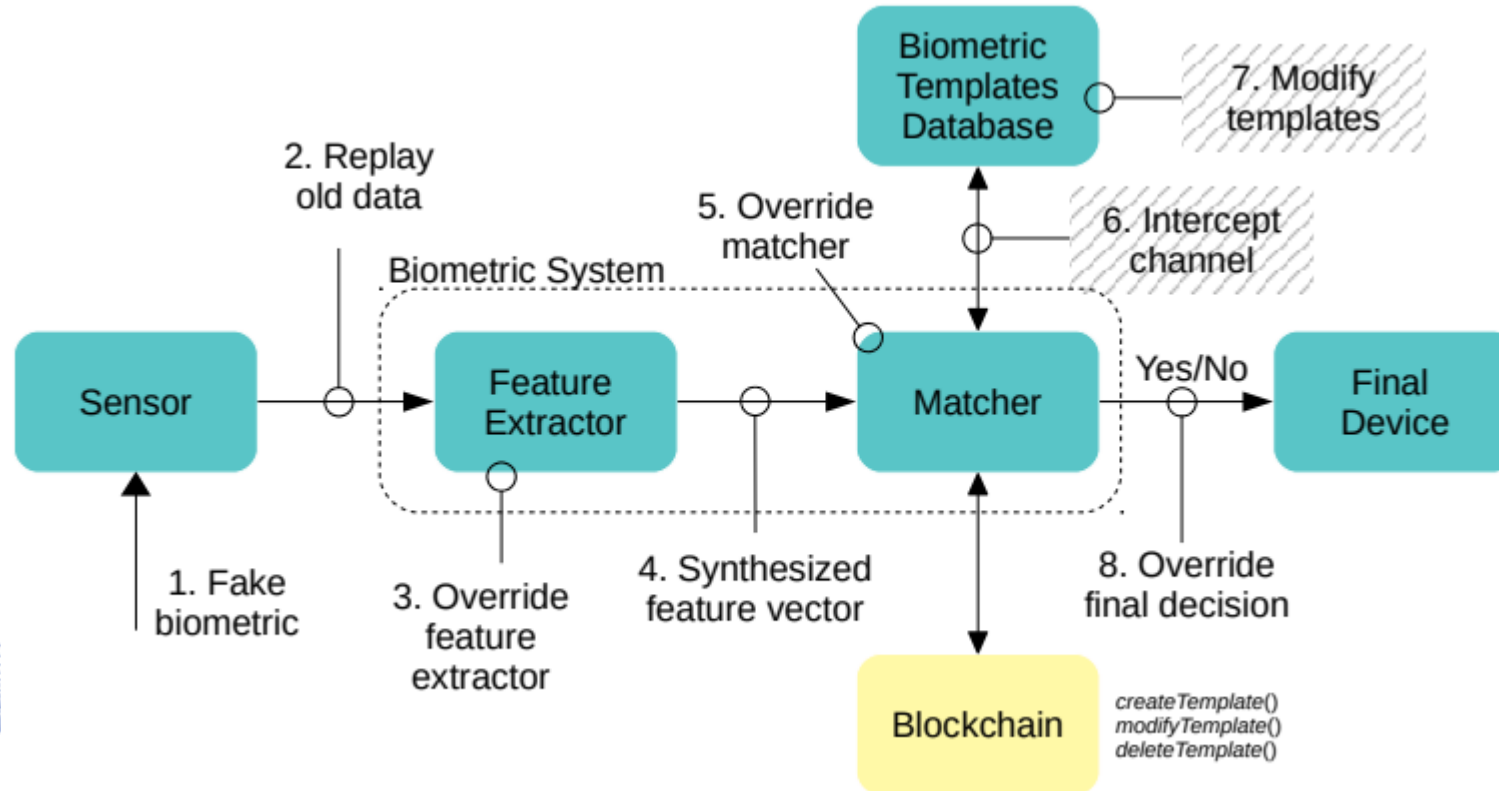
- Biometrics refers to the automated recognition of entities by using physiological (face recognition, fingerprint) or behavioral (voice sound, signature) characteristics.
- Advantages over the traditional identity methods:
 - There is no need to remember passwords or usernames.
 - Less vulnerability in hacking.
 - Provide a stronger bound between subject and action.

Blockchain and Biometrics



- Blockchain due to its nature provides features like immutability, accountability, availability, access so bound them around biometric modules we can provide more security and privacy in Biometric systems.
- Public Blockchains seem to be less suitable for such systems since all of the participants can have access on the ledger, so due to the ***sensitivity of the biometric data*** we need to form structures with more ***privacy-preserving way***.

Blockchain and Biometrics



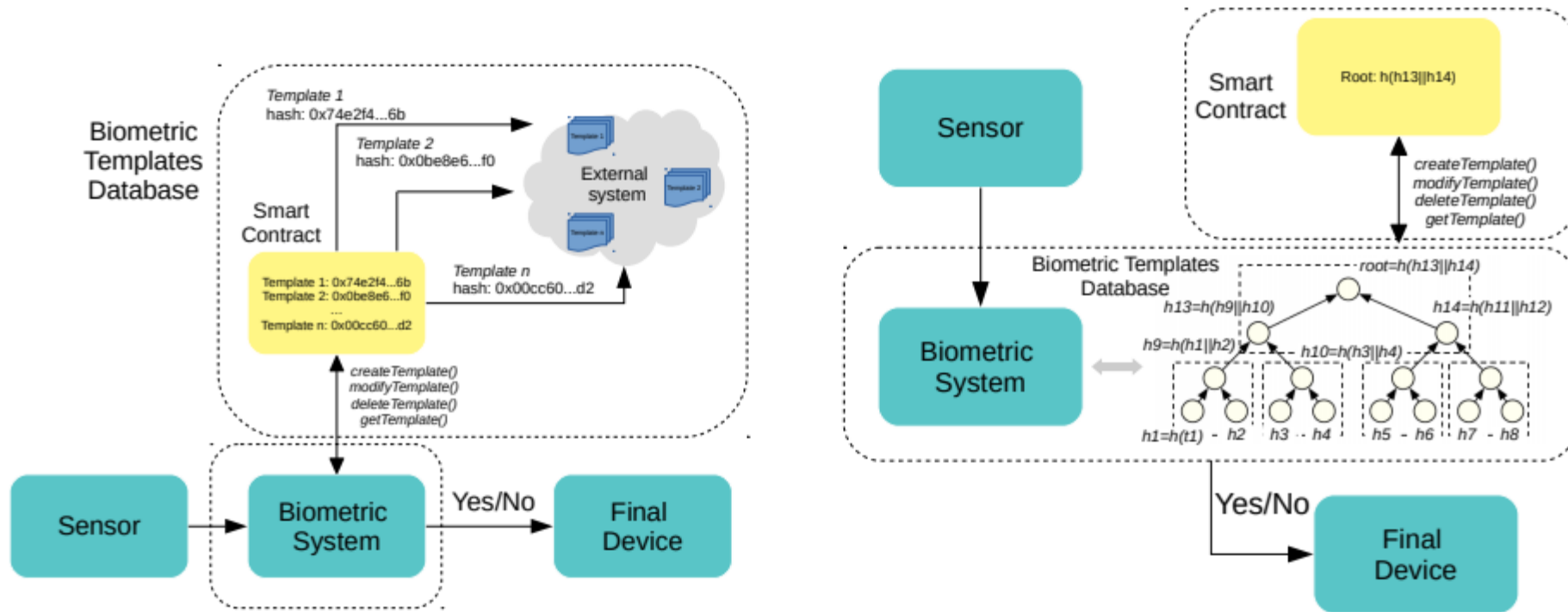
Biometric Modules.

Biometric Template Protection



- There are basically three ways to storage biometric data in blockchain:
 - **Full on chain storage:** Data, all of them are stored as they are in the chain. BT can be stored directly using smart contracts. Easiest way but the most costly and inefficient.
 - **Data Hashing:** Other approach is storing the data out of the chain and blockchain here can be used as a guarantee in terms of data integrity due to the feature of immutability (more efficient way). Complete templates can be stored in classical external systems and only the hashes of them can be stored in the chain using the smart contracts.
 - **Linked Data Structure:** We can boost Data hashing even more by using linked data structures like Merkle Trees.

Biometric Template Protection



Biometric system with Merkle Tree and Data Hashing.

Blockchain ATMs



- **Blockchain ATMs** are created to allow the scanning of biometrics features that will be linked to bank account holders.
- In this way the identity check will be achieved without the use of the banking databases but instead we will use the blockchain.
- Fraud cards can be detected while at the same time citizens' personal data will be protected.

Q & A

Thank you very much for your attention!

**More material in
<http://icarus.csd.auth.gr/cvml-web-lecture-series/>**

**Contact: Prof. I. Pitas
pitass@csd.auth.gr**