Track 01 - Blockchain for IoT

Antonio Tenorio Fornés and Rubén Fuentes Fernández
GRASIA-UCM - Intelligent Infrastructure Design, Master IoT

3

Decentralization

GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández

Before Blockchain

- Advantages
- Disadvantages

GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández

After Blockchain

- Blockchain
- Bitcoin
- Anyone else?

GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández

6

History

From Bitcoin to Blockchain

GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández

What is Bitcoin?

- First distributed digital currency
- Proposal by Satoshi Nakamoto
  - 10/31/2008 - Article published on the metzdowd.com cryptography mailing list
  - 2009 - Launches Bitcoin software, which creates the network, and the first units of the currency.
  - Mid 2010 - End of his collaboration with the project.
    - Transfers control of the source code repository and the network alert key.

Who is Satoshi Nakamoto?

Satoshi Nakamoto goes public and denies he's bitcoin founder

Channel 4 News ✓ 91K views • 3 years ago

A reclusive Japanese American man named by Newsweek as the founder of bitcoin, denies any involvement with the digital

Mr Bitcoin: "I don't want money, I don't want fame!" BBC News

BBC News ✓ 186K views • 1 year ago

Australian entrepreneur Craig Wright has publicly identified himself as Bitcoin creator **Satoshi Nakamoto**. His admission ends years

Satoshi Nakamoto is an Alien from the next Dimension

SteemSpeak • 877 views • 7 months ago

A euphoric rant about cryptocurrency - Bitcoin and Steem on Steemspeak.

Who is Satoshi Nakamoto?

- Nakamaoto Bitcoins remain unchanged since January 2009
- As of May 2017, Nakamoto had approximately 1 million Bitcoins.
  - Approximate value of $15 billion USD in December 2017.
  - At the December 2017 peak Forbes estimated $19 "billion" USD, 44th richest person in the world.

Why Bitcoin?

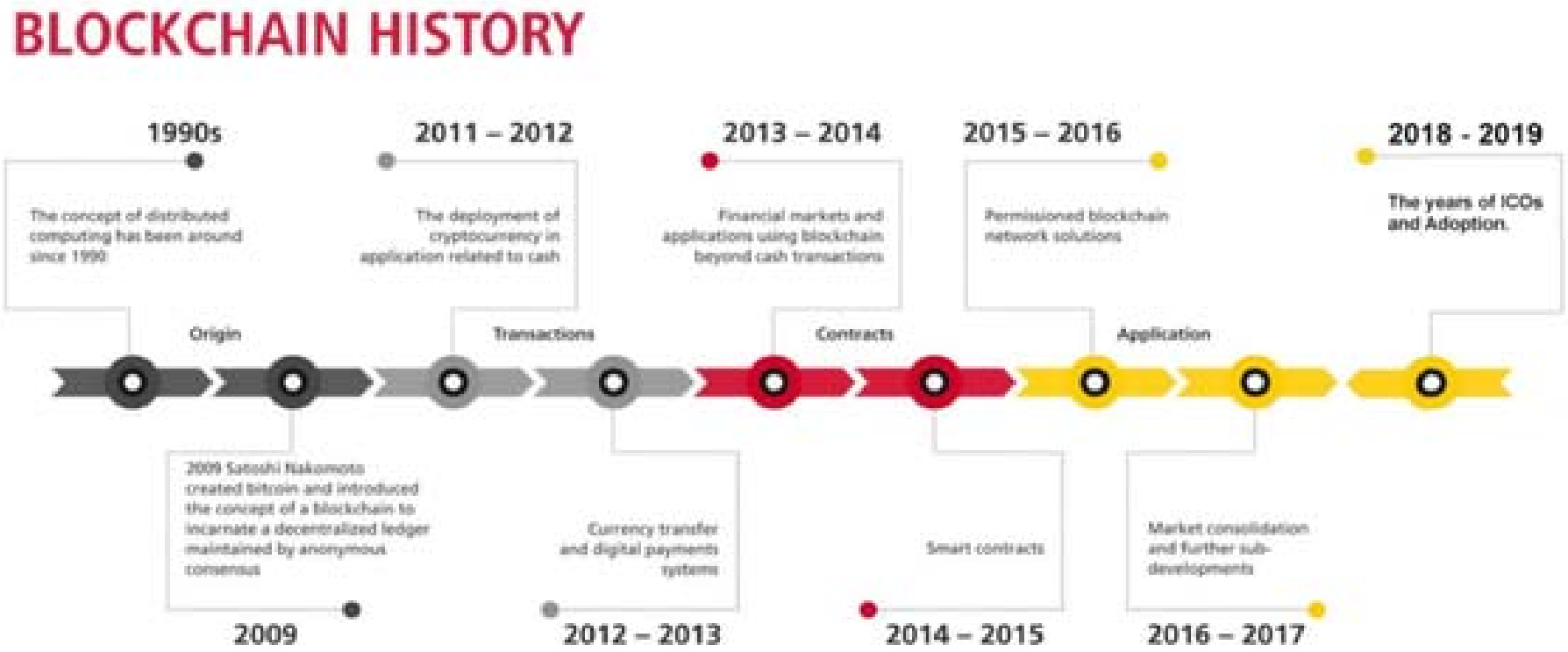
- No trust in third parties
- Reduce costs
- Privacy
- Avoiding corruption
- …

Bitcoin and Blockchain

- Bitcoin is considered the birth of Blockchain technology.
- Later other Blockchains became popular
  - Ethereum (https://www.ethereum.org/)
  - Various Hyperledger projects (https://www.hyperledger.org/)
  - Other *Blockchain-like* solutions.

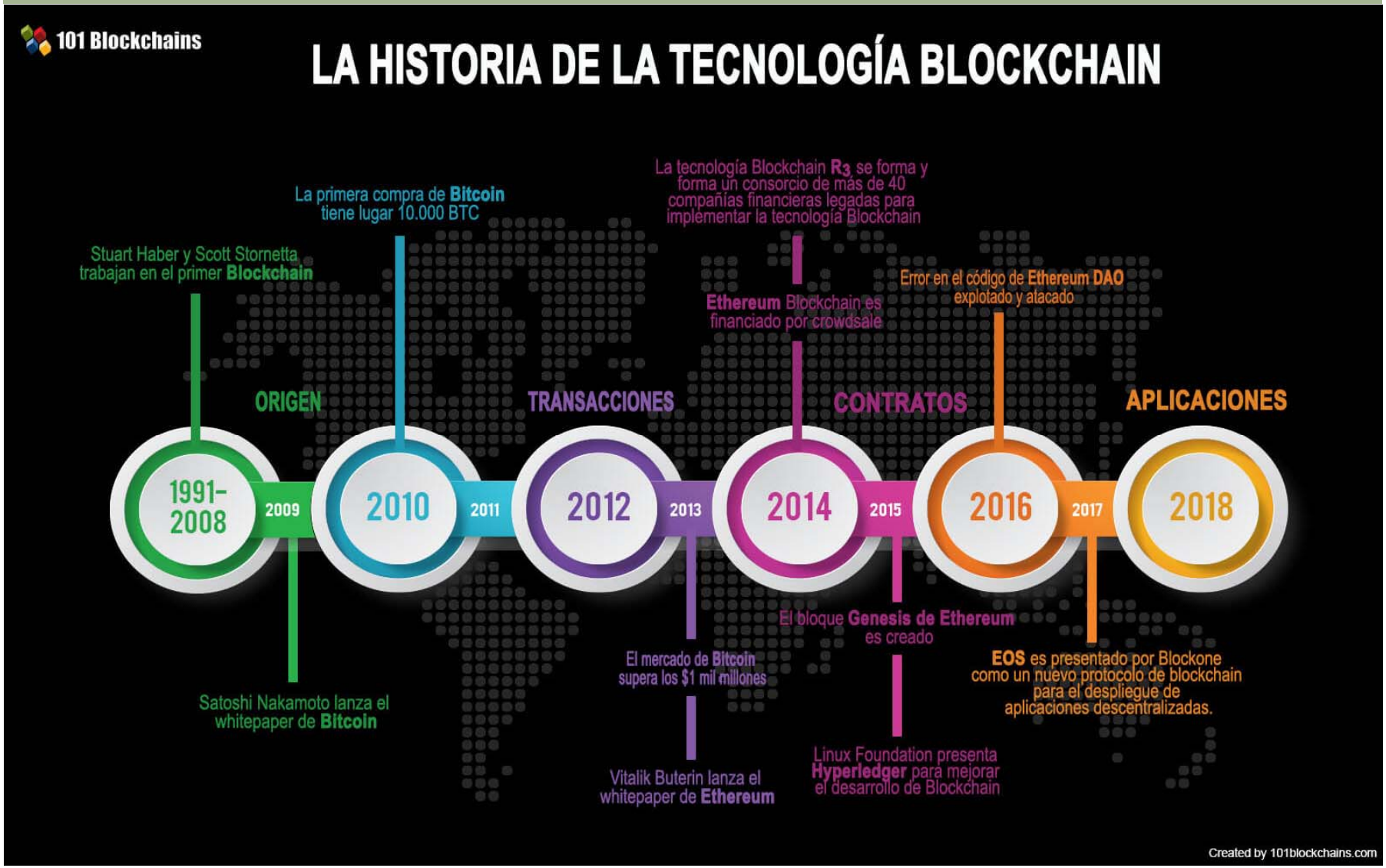
GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández

Bitcoin and Blockchain - History



GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández

Bitcoin and Blockchain - History



14

Blockchain

GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández

Why Blockchain?

- Problem of double spending in decentralized systems
  - How to prevent A from paying B and C using the same currencies
- Consensus on the status of records
- Immutable
- Verifiable
- …

How?

- Blockchain is a system:
  - That stores *transactions*
  - On immutable *public accounting records* (or *ledgers*)
    - *Ledgers*
  - Through decentralized *peer-to-peer* work
    - *Peer to Peer, P2P*
  - Whose security is based *on encryption processes*
  - And *consensus mechanisms*
    - Ex. *Proof of Work* (PoW)
  - Can optionally support *smart contracts*

GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández

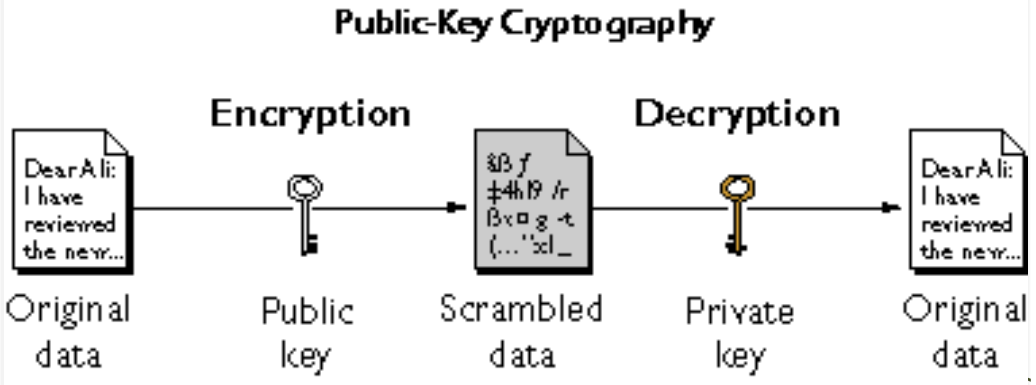
Blockchain

- The use of the blockchain structure together with the proof of work allows to make a decentralized and secure registry.
  - Creation of the first cryptocurrency, Bitcoin.
- The *Blockchain Demo* website allows you to explore blockchain concepts in an interactive way.

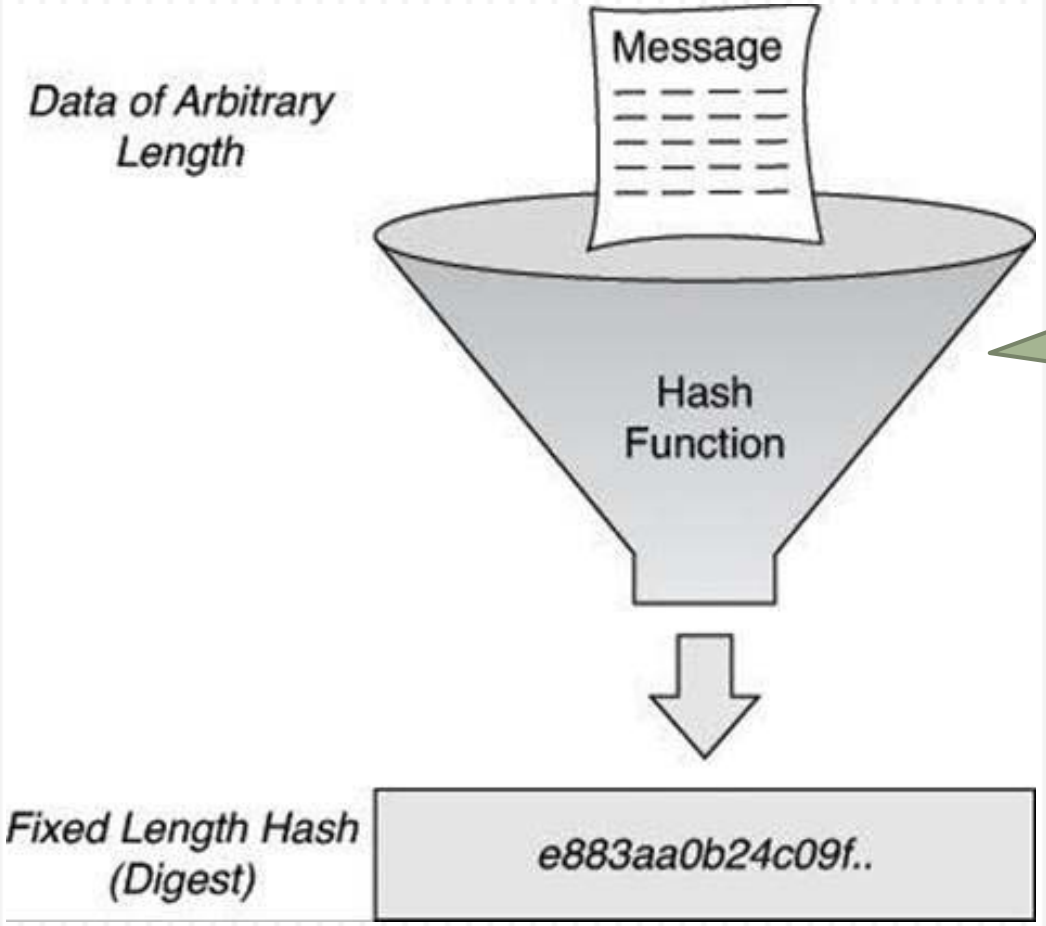
  - See hash, block, blockchain, blockchain, distributed chains, transactions...

Identity

- Each identity on the Blockchain is associated with an **asymmetric key,** consisting of:
  - **Public key** (public address)
    - Address to **receive** or **send** a transaction
  - **Private Key** (secret key)
    - **Authorize** (sign) transactions



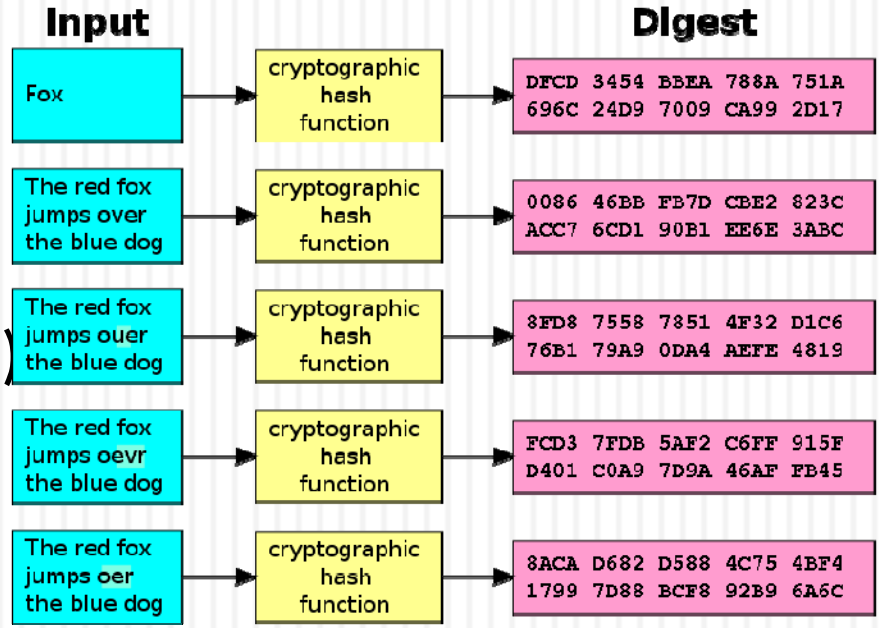
Cryptographic hashes



What are they?
What are the requirements?

Hash functions

- A **hash function** is a mathematical algorithm that maps a set of data of arbitrary size to a string of characters (or bits) of fixed size, and is a one-to-one function.
- Some algorithms:
  - MD5, SHA1 (invalid)
  - SHA2 (**SHA-256**, SHA-512)
  - SHA3, BLAKE2

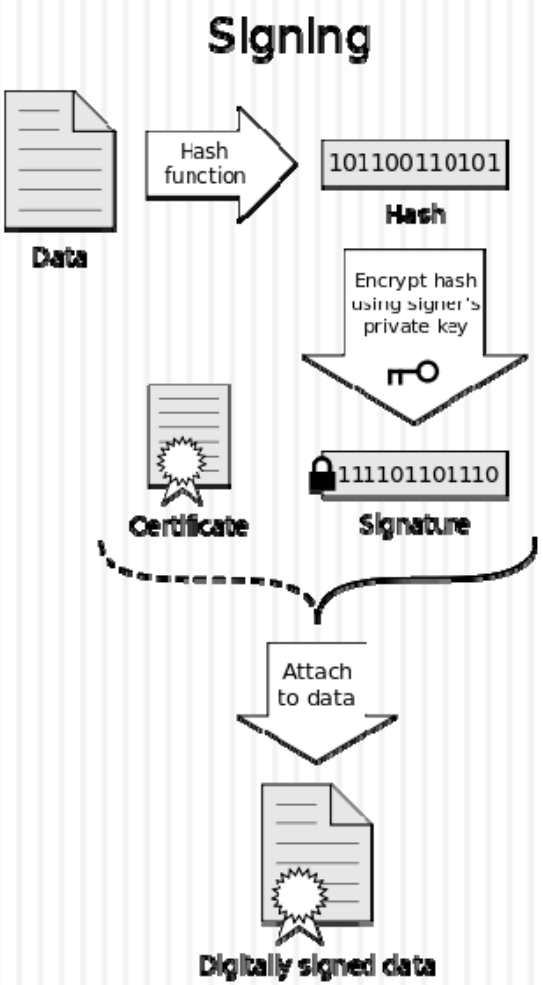


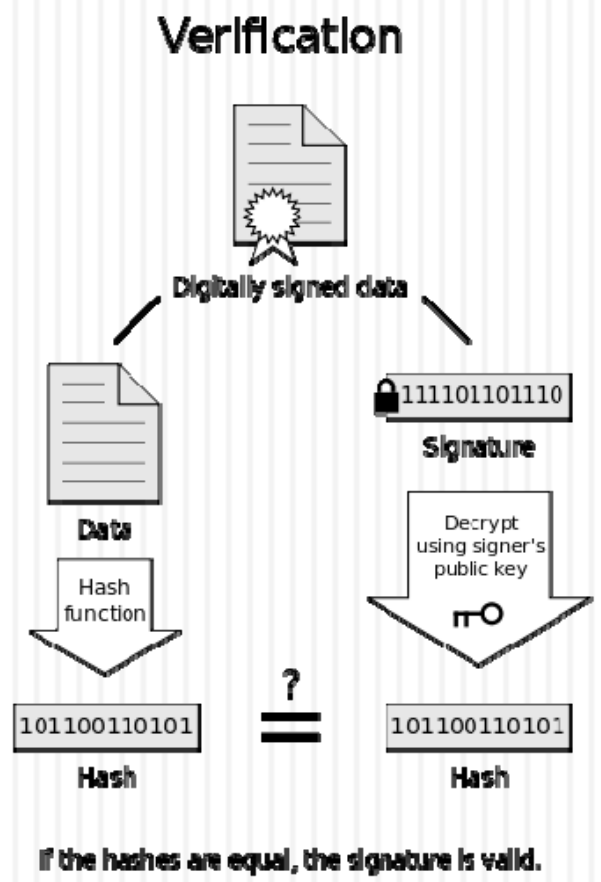
GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández

Cryptographic hashes

- Given some data, a **hash function** generates a **"fingerprint"** with the following characteristics:
  - **Determinism:** The same data always generates the same hash.
  - **Low cost:** Calculating the hash of any data is computationally simple.
  - **Pre-image resistance:** It is computationally intractable to know the data from its hash.
  - **Collision resistance:** It is computationally intractable to find two pieces of data that generate the same hash.

Cryptographic signature verification





Encryption

- Standard encryption practices
  - Some Blockchain allow the use of *Bring Your Own Encryption* (BYOE).
  - As good as the next SW and/or HW innovation
    - E.g. quantum computing
- All blocks are encrypted

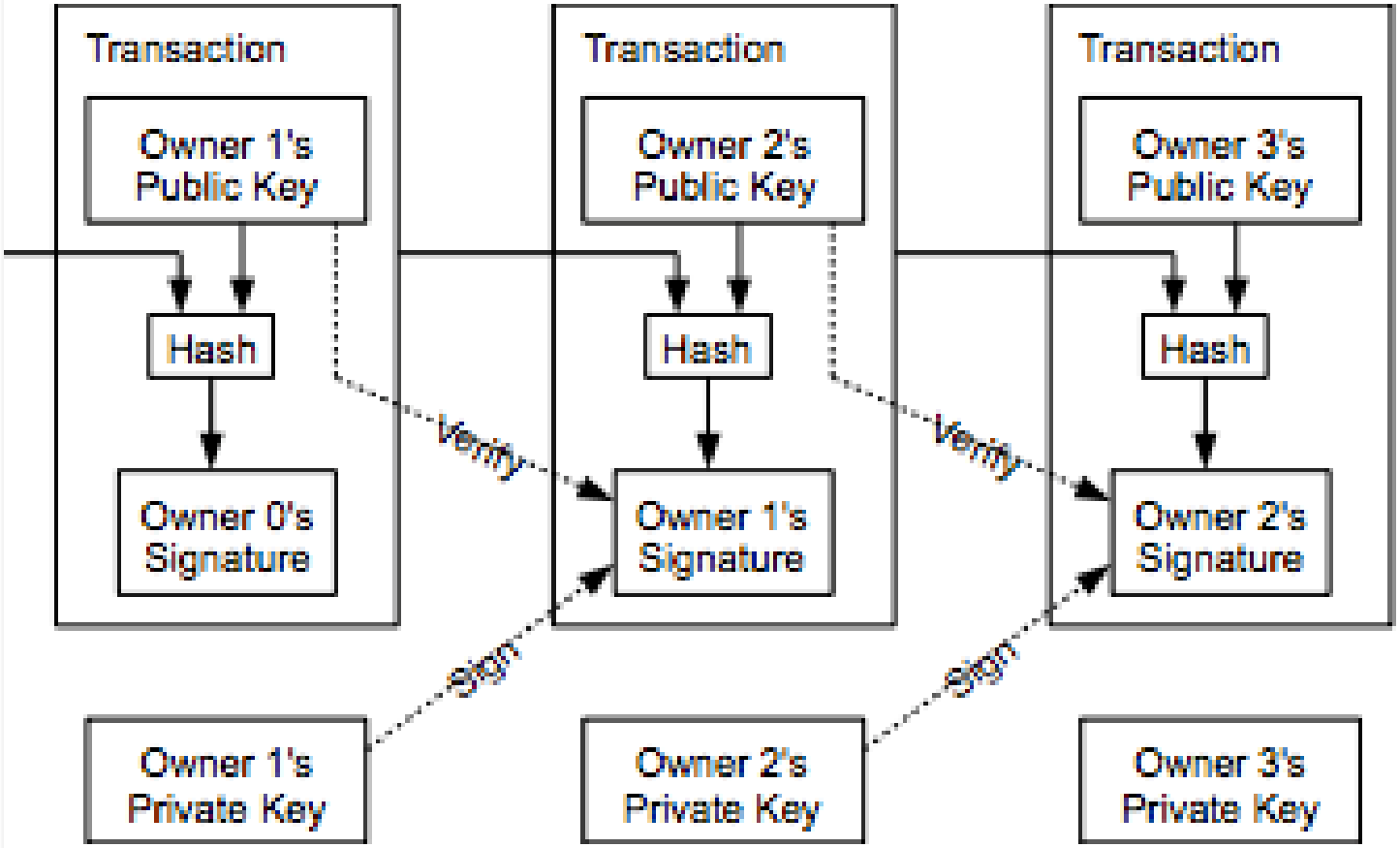
GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández

Transactions

- Historical archive of decisions and actions taken.
  - Proof of history and provenance

Use cases		
Land Registry	Replacement of deed research requirements.	Land registration in Sweden
Personal identification	Replacement of birth/death certificates, driver's licenses, social security cards.	Estonia
Transport	Shipping information, tracking, certificates of origin, international forms.	Maersk / IBM
Banking	Document storage, increased back office efficiency.	UBS, Sberbank of Russia
Food distribution	By providing location, lot, harvest date..., supermarkets can identify problematic foods.	Walmart
Audit	Blockchain's decentralized and immutable nature will fundamentally change audits	

Transactions



GRASIA-UCM - Antonio Tenorio Fornés and Rubén Fuentes Fernández