Lero THE IRISH SOFTWARE RESEARCH CENTRE

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Blockchain for Government

Hitesh Tewari

htewari@cs.tcd.ie

Research Areas

Internet Voting

Cryptocurrencies

Authentication

Identity Mgt

Efficient Consensus Mechanisms

KYC

Healthcare & IoT

Online Lotteries

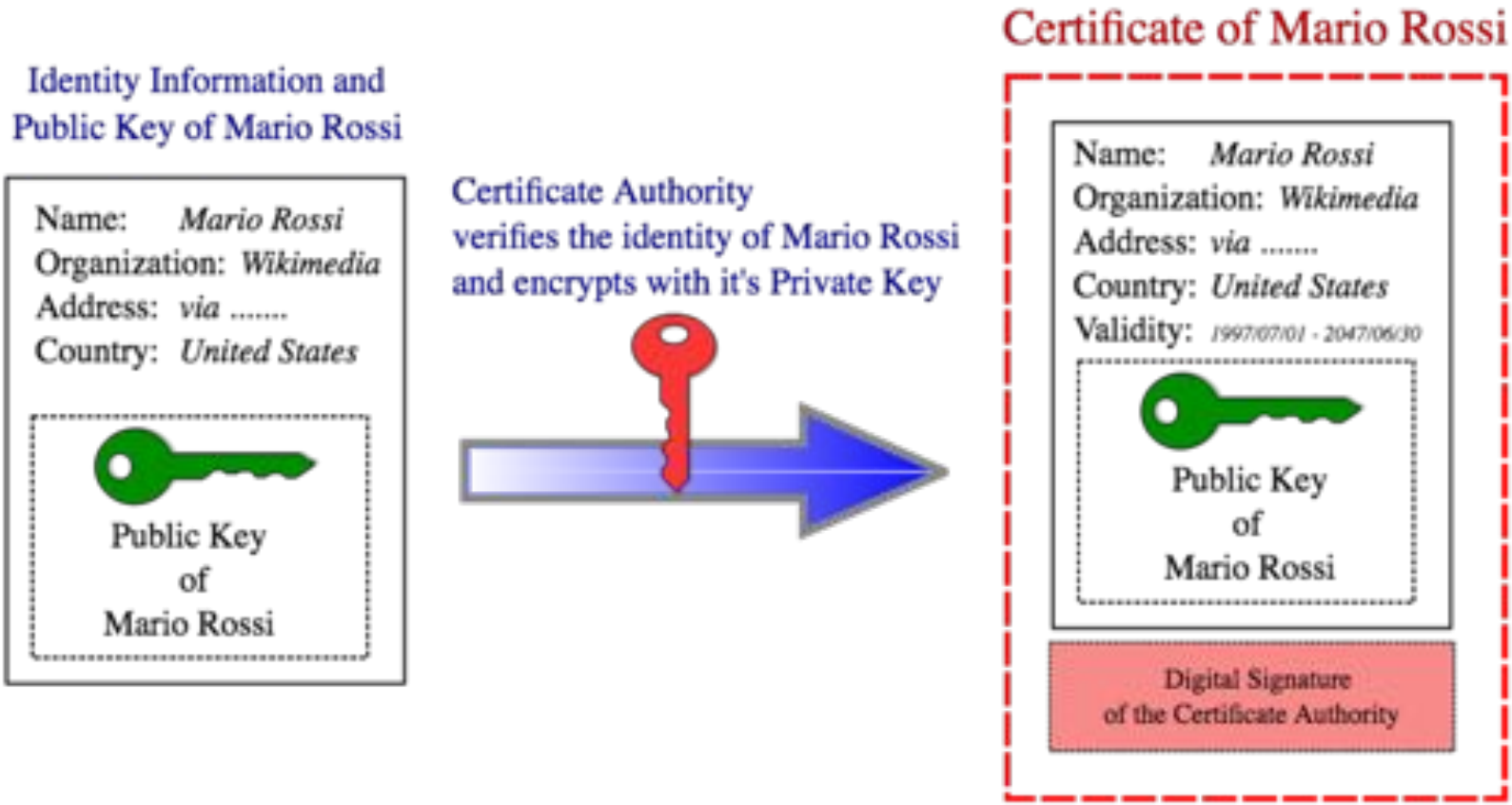
Secure Email

Issue a public key certificate to every citizen at "zero cost"

Digital Identity

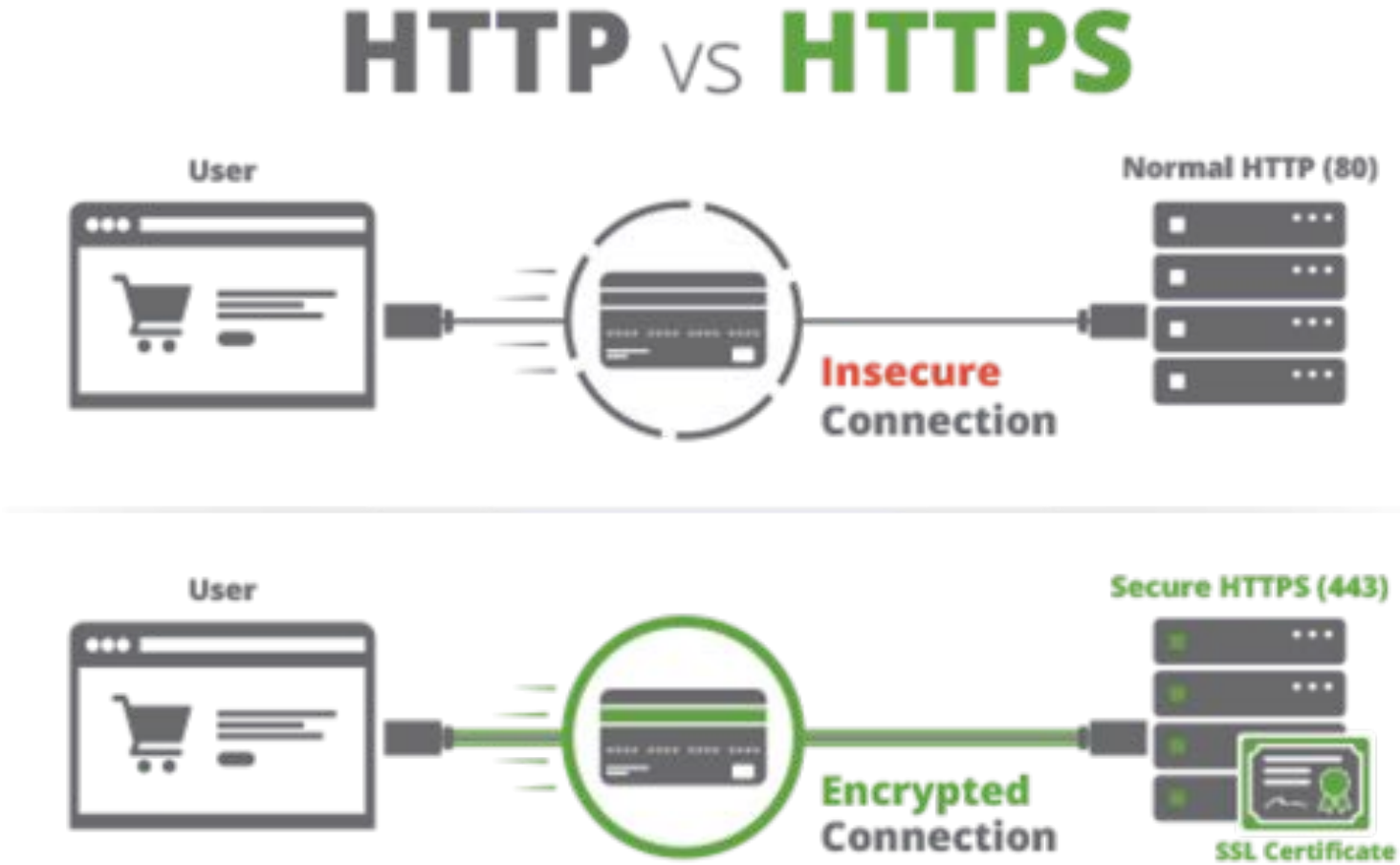
Public Key (SSL) Certificate

What is a SSL Certificate?



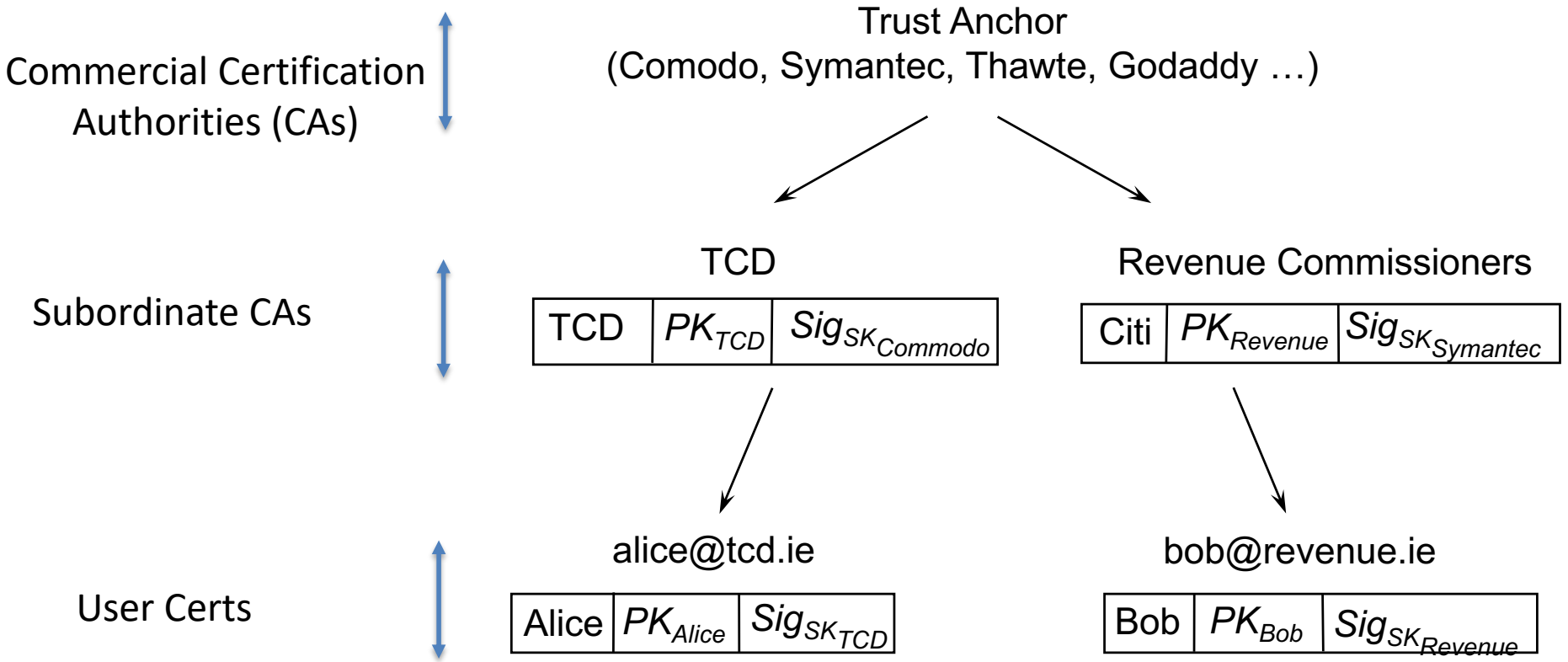
Binds a public key to an identity

Who Buys SSL Certs?



SSL certs cost €200-2000 per annum!!

Public Key Infrastructure (PKI)



Make use of blockchain technology for storage and dissemination of certs

Certificate Issuance

Alice
(alice@tcd.ie)

2. Request cert from organizational CA

5. Certificate

TCD CA Server

1. Generate public key pair (PK_A, SK_A)

3. Create and broadcast new cert to P2P network

4. CAs verify and lock certs into blockchain

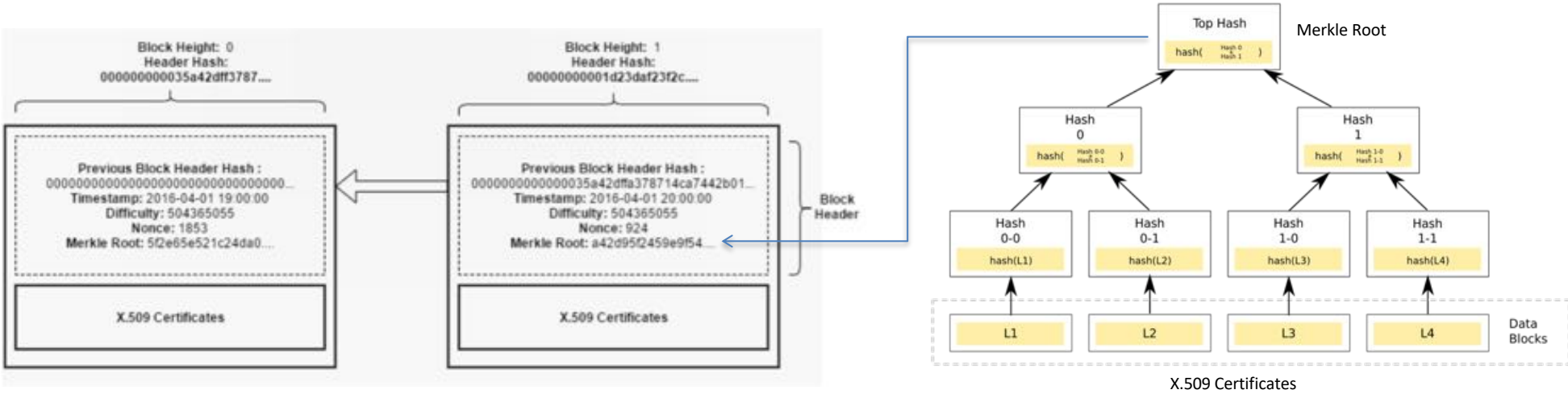
Internet

Revenue CA Server

BoI CA Server

CAs are equivalent of "miners" - collectively verify certs

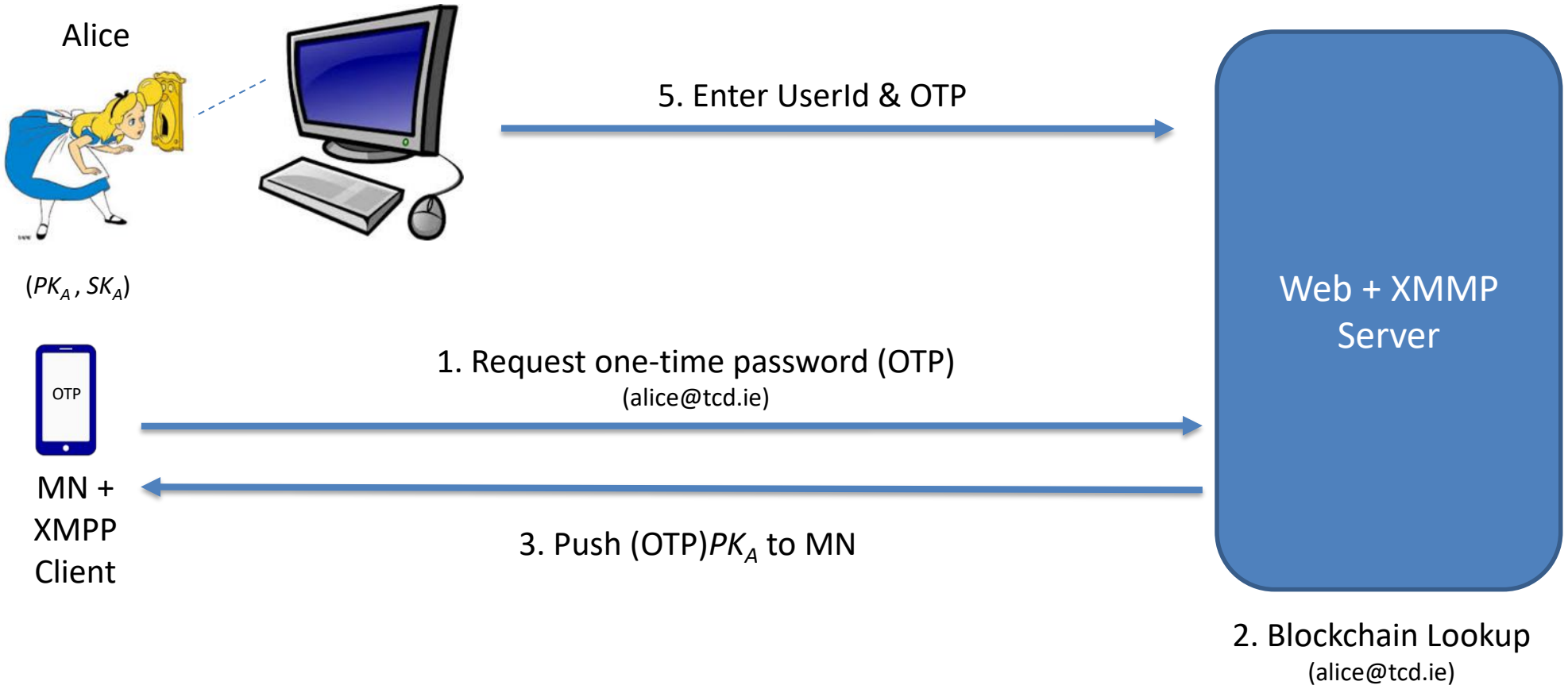
Blockchain Structure



- Certs replace monetary transactions on the blockchain
  - Indexed via an email address
- On average we require 1K of storage per cert
  - 1 million certs require 1GB
- Individuals can have more than one cert
  - e.g. employer cert, government cert …

No more weak passwords!!

Two Factor Authentication



Minimal changes to login process – password replaced with OTP

XMPP – Instant Messaging Protocol e.g. WhatsApp

Lero THE IRISH SOFTWARE RESEARCH CENTRE

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Verified Social Media Accounts

Lero THE IRISH SOFTWARE RESEARCH CENTRE

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Stop Abuse on Social Media

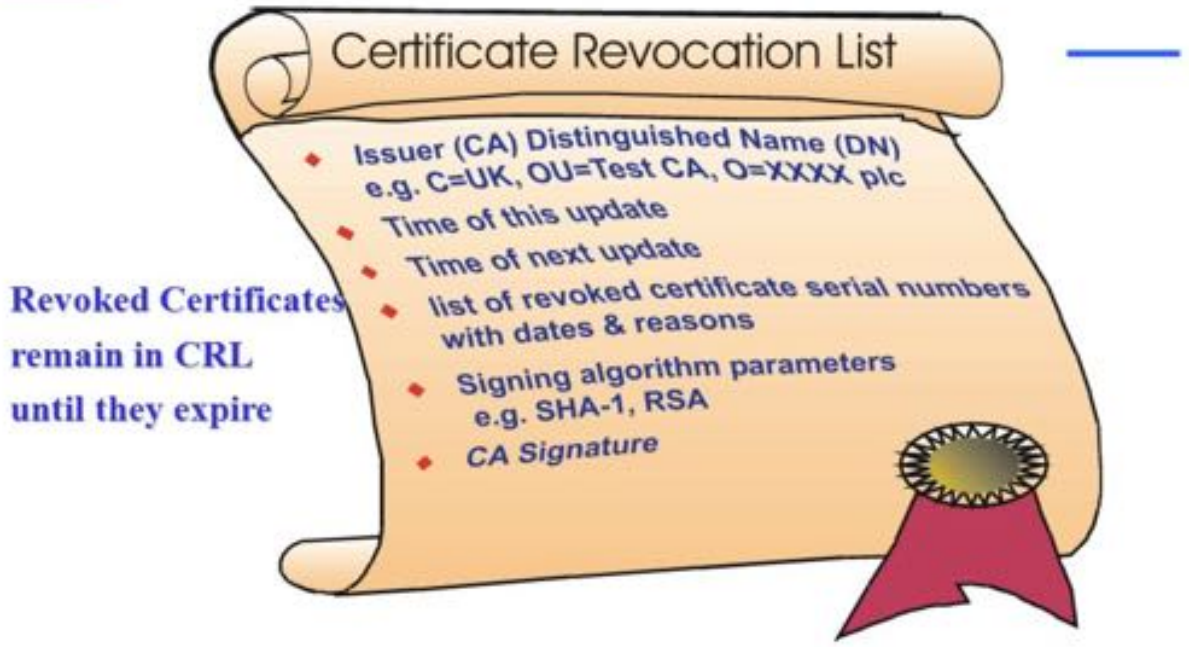
- Users authenticated using their public key cert
  - Account can be traced back to a ***real*** person

- Required to use the same identity across *all* sites
  - Prevents users from setting up fake accounts etc.

- Abusive posts will result in a user's cert being revoked
  - Prevent further access to *all sites instantly*

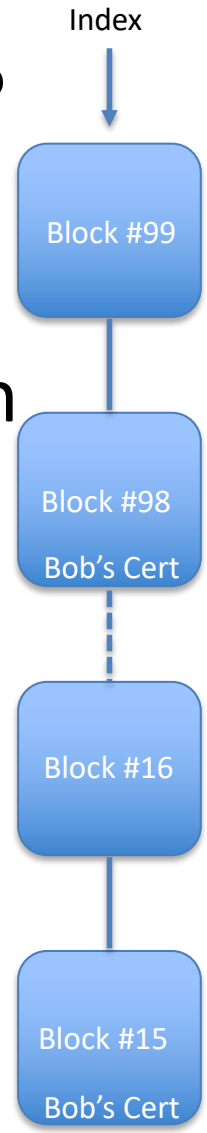
No Need for CRLs!!

Certificate Revocation List



Lost or Revoked Certs

- What happens if a user's keys are compromised?
  - Ask organization to issue new cert
- Can be more than one cert for a user in the chain
  - Indexed using newest block in the chain
- If an employee leaves an organization/dismissed
  - Issue a cert on their behalf
    - Instantly preventing access to company servers!!



Reduce Spam Mail

Alice
(PK_A, SK_A)

1. Compose email

4.Digitally **Signed** and **Encrypted** email

Email Server

2. Lookup Bob's cert
(bob@revenue.)

3. Bob's cert

X509Cloud Service
or Local Blockchain

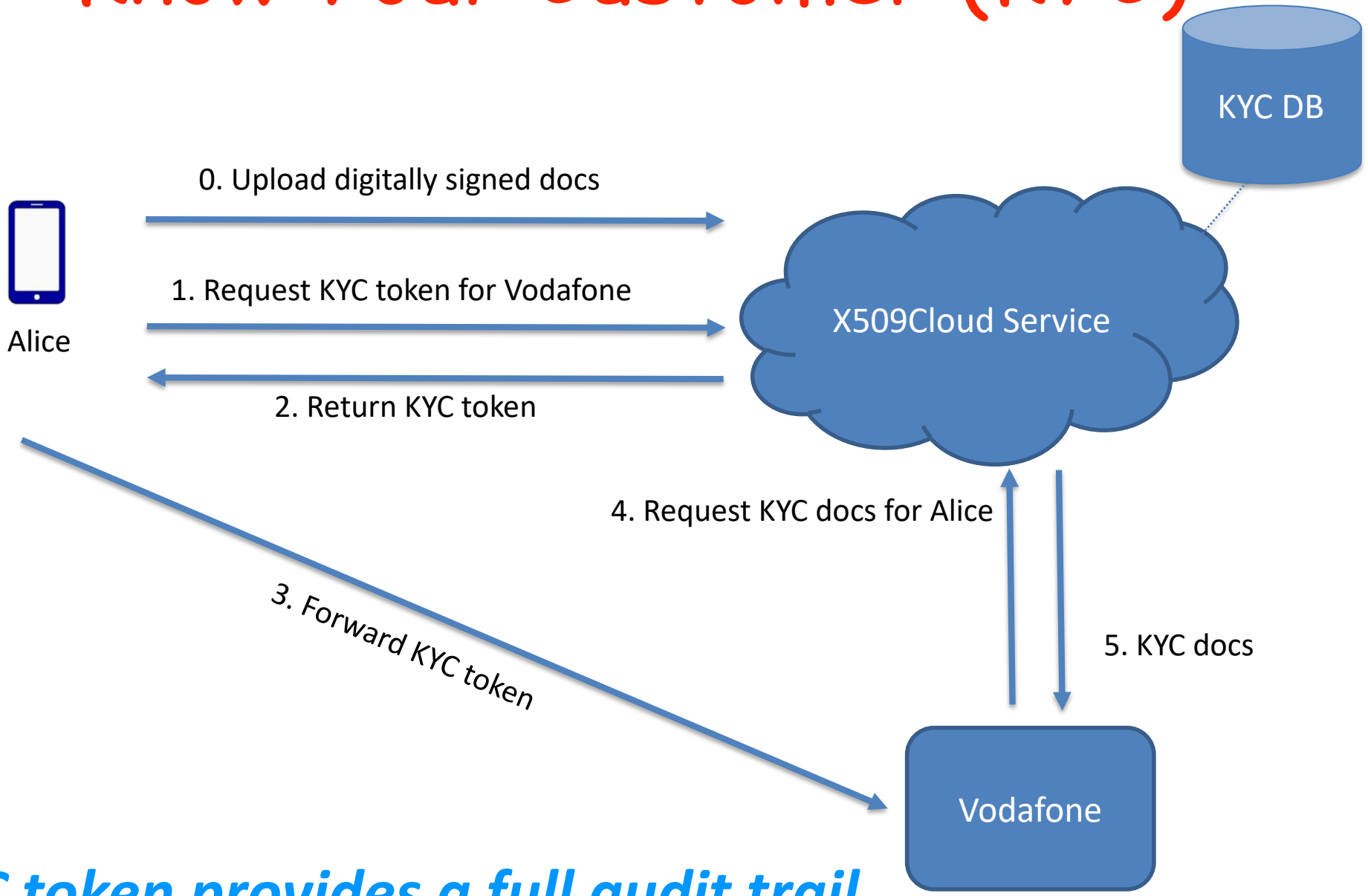
5. Lookup Alice's cert
(alice@tcd.ie)

6. Alice's cert

Bob
(PK_B, SK_B)

X509Cloud Service could be maintained by a govt. agency

Know Your Customer (KYC)

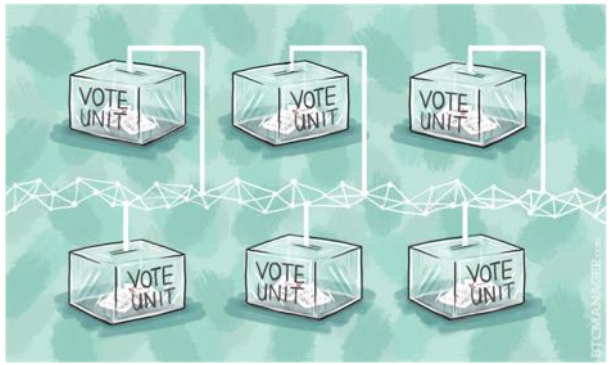


KYC token provides a full audit trail

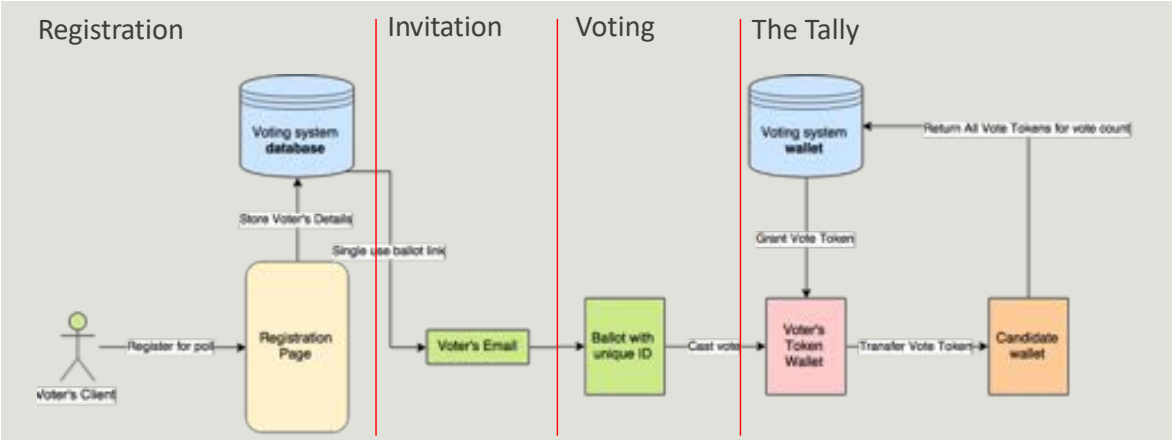
e-voting

Internet Voting

- e-voting protocols to date have been too complicated to deploy!!
- Easier and more *transparent* alternatives required
  - Blockchains allow for observers to ***verify in real-time*** the casting and counting of votes
- Allow citizens to vote using their mobile devices
  - More young people will exercise their franchise



Internet Voting Using Zcash



- Zcash can be thought of as an *anonymous* version of Bitcoin
  - Makes use of zero coins (ZEC) as currency
- Provides a full *audit trial* of spent tokens
  - Total **input** values = Total **output** values in a transaction
- Make use of low-value ZECs as voting tokens!!
  - Potential voters sent a ZEC at the start of an election
    - Candidate crypto wallet that receives most ZECs wins election

Lero THE IRISH SOFTWARE RESEARCH CENTRE

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

National Healthcare Blockchain

Managing Lifetime Healthcare Data on the Blockchain

- Enable *all* medical records pertaining to a citizen to be stored on the blockchain

- IoT enabled devices will *automatically* load patient test results onto the blockchain
  - e.g. Blood tests, X-rays, CT scans

Data Storage and Retrieval

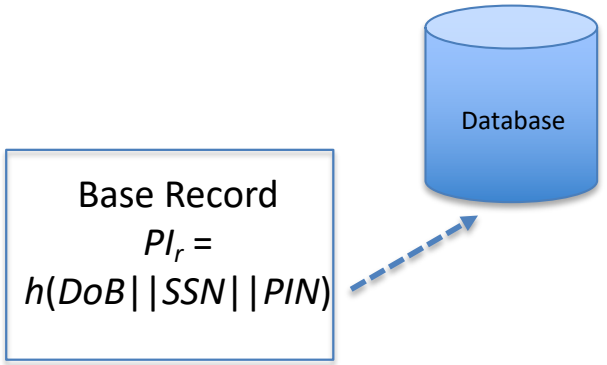
Two competing requirements

- *Pseudonymisation* of patient data stored on databases and indexed via the blockchain
  - Enable mining by external organizations

- Allow *authorised users* to view all records for particular individual on the blockchain
  - Given knowledge of certain security params

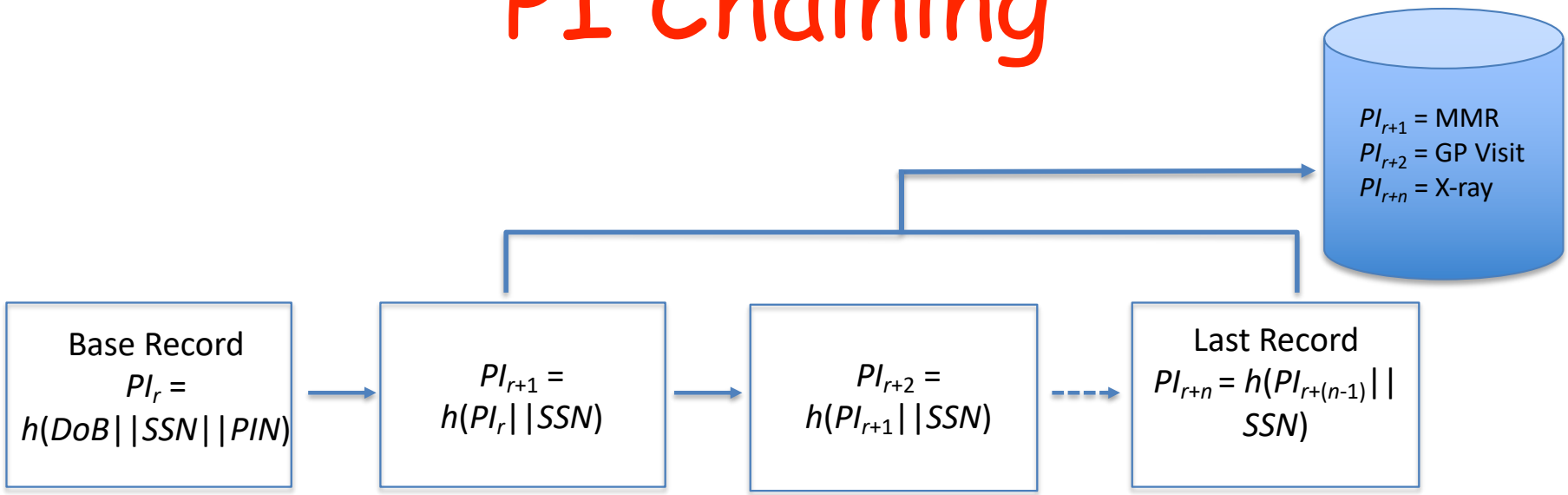
Pseudo-Anonymous Identifier (PI)

- Initial *base record* (PI_r) entry created on the blockchain for each child at time of birth cert issuance
- Generated by passing the following parameters through a hash algorithm
  - Date of Birth (DoB)
  - Social Security Number (SSN)
  - Secret Seed (PIN)
    - e.g. last four digits of the birth cert serial number



- Individuals can retrieve their base record from a web portal
  - Can be stored as a QR code on a mobile device

PI Chaining



- Each subsequent record on the blockchain for an individual will be linked to their base record (PI_r)
- Records belonging to a patient spread over many blocks in the blockchain
  - Logically chained together

Lero THE IRISH SOFTWARE RESEARCH CENTRE

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Cryptocurrencies & Distributed Consensus

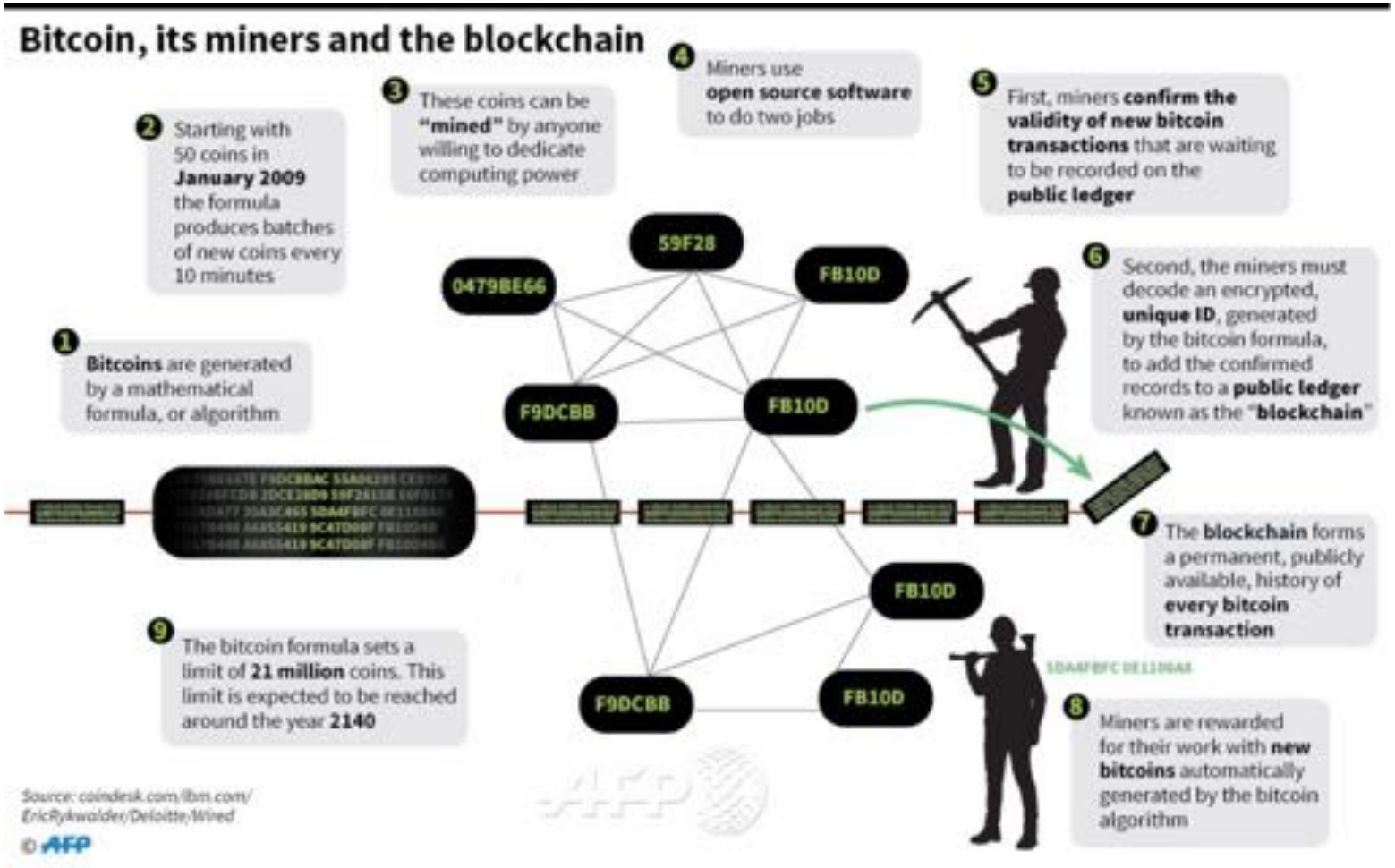
Fiat Backed Cryptocurrencies

- Cryptocurrencies are being used as an “asset” class
  - Not as a means of exchange for goods and services

- Require cryptos to be backed by fiat currency
  - Prevent hoarding of coins etc.

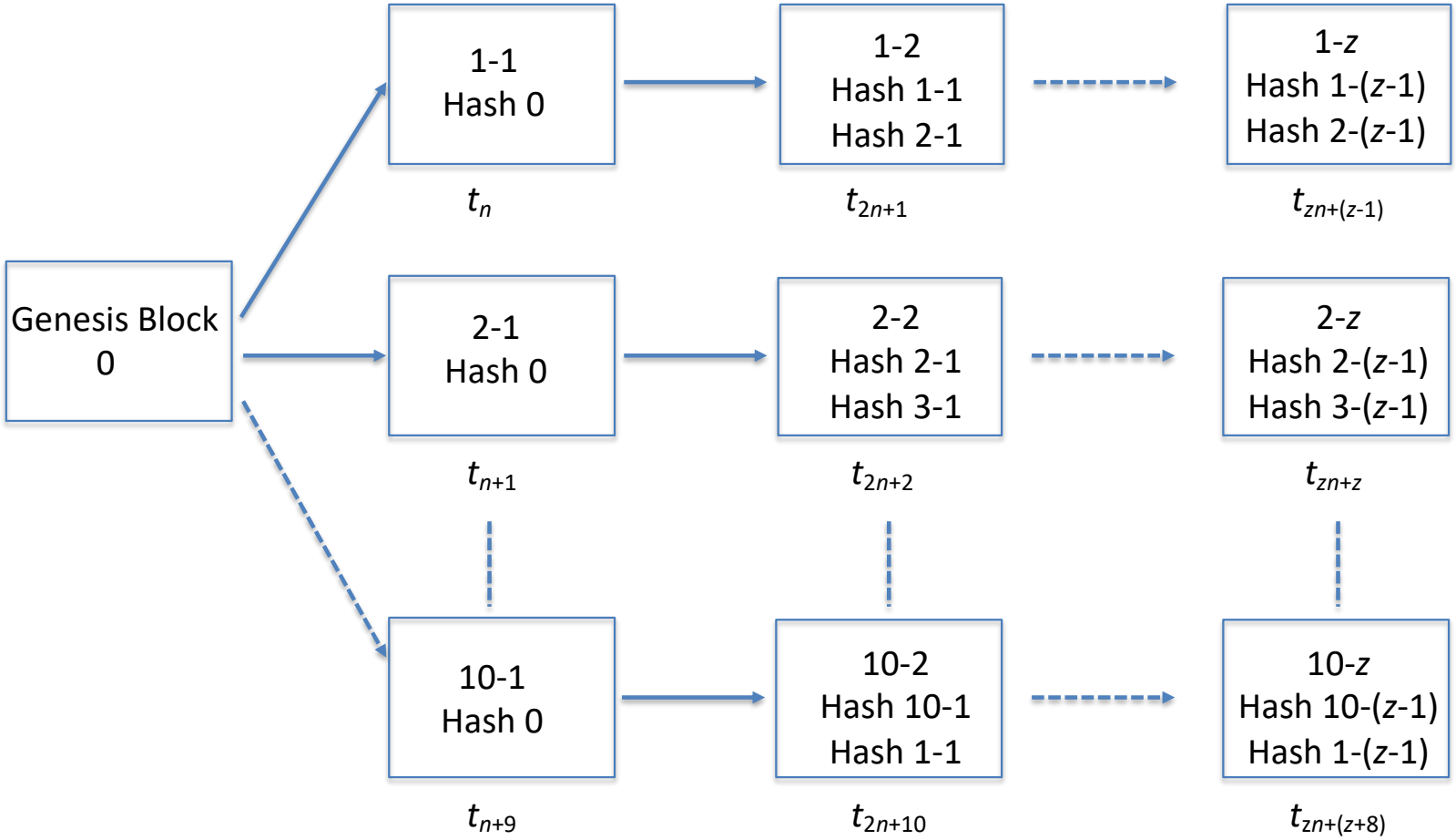
- Also need better *distributed consensus* mechanisms
  - Faster transaction processing and real-time point-of-sale

Mining



On average the Bitcoin network processes 7 transactions per second - as opposed to 2,000 on the Visa network!

Efficient Mining



Sub-chains mined in a sequential but overlapping manner - allows for parallel mining of blocks

Thank You

Internet Voting

Cryptocurrencies

Authentication

Identity Mgt

Efficient Consensus Mechanisms

KYC

Healthcare & IoT

Online Lotteries

Secure Email