

**CWI**

**IN BEDRIJF**

Digitaal kompas

16 mei 2019

# The immutability of Blockchain

Marc Stevens  
Cryptology Group  
CWI

scientific computing

algorithm

complex data

cybersecurity

digital finance

data systems

quantum software

blockchain

neuroscience

societal relevance

AI

machine learning

predictions

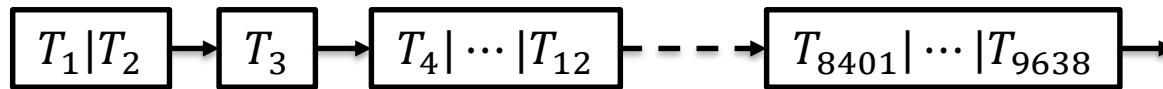
# Blockchains & Applications

# Blockchain Protocol

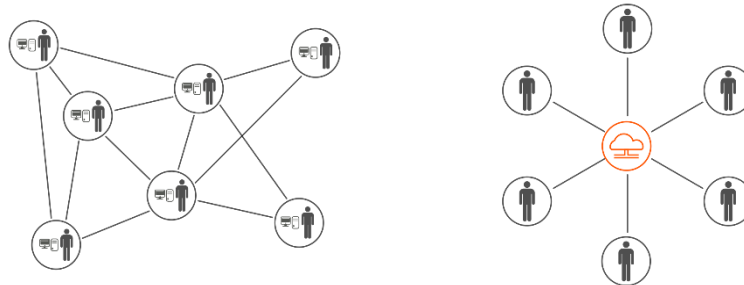
- Blockchain definition

*“A blockchain is a distributed digital ledger that contains a continually updated chain of all transactions.”*

- Chain of Blocks of Transactions



- Protocol: Distributed versus Centralized:



- all parties in a network maintain a copy
- decide together on next block of transactions

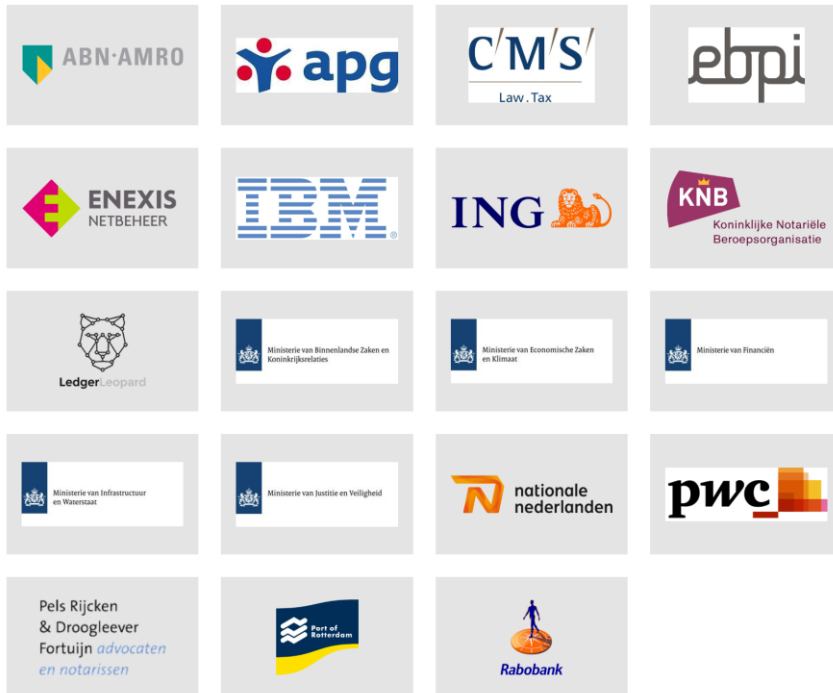
# Blockchain Applications

- Distributed Ledger
  - Digital- / Crypto-currencies
- Distributed Database
- Distributed Filesystem
- Any distributed information system where a (virtual) State is continuously modified by (blocks of) Transactions
  - Virtual Machines on a Blockchain
  - Smart Contracts
  - Programmable Economy

# Dutch Blockchain Coalition

Jointly developed partnership by  
industry, government and knowledge institutions

## Kernpartners



## Support Partners



## Kennispartner



## DBC Action Agenda

- The focus of the coalition lies in properly arranging the fundamental principles of Blockchain:
  1. ensuring the technology works well
  2. developing the conditions for blockchain, such as explaining and applying the legislation
  3. realizing a human capital agenda, in other words developing education and talent.

# Blockchain for Good

De Dutch Blockchain Coalition presenteert zes use cases voor betrouwbare en maatschappelijke geaccepteerde blockchaintoepassingen waar op publiek-private basis aan wordt gebouwd. De toepassingen zijn van belang voor de samenleving en de economie van Nederland. Daarmee zijn het aantoonbaar waardevolle toepassingen van deze technologie.



Jouw gegevens      Jouw identiteit      Jouw beheer

### Self-Sovereign Identity (SSI)

Digitale identiteit is van cruciaal belang. De SSI is het puzzelstukje dat diverse vraagstukken rondom blockchain kan verbinden. Bijvoorbeeld de bevestiging dat jij jij bent en/of dat jij 18+ bent.



Wereldwijd te implementeren op basis van wederkerigheid.

### Logistiek

Transparante, betrouwbare en eerlijke ketens. Minder administratieve lasten en efficiënter transport.



Reeds op kleine schaal in meerdere landen getest. Nu op Europees niveau verder.

### Onderwijscertificaten en diploma's

Officiële documenten zoals diploma's, certificaten en registers betrouwbaar delen en verifiëren.




### Pensioen

Een simpele vraag zoals: "Hoeveel pensioen heb ik waar opgebouwd?" kan door blockchaintechnologie makkelijker beantwoord worden dan met de huidige systemen.



### Compliance by design

Meer transparantie en automatisering van subsidie-processen zodat het voor iedereen makkelijker, eerlijker en efficiënter wordt. Blockchain biedt die mogelijkheid. In de taal van technologie: 'Compliance by design'.



2018: Werkende demo.

### Hypotheken

Bij een hypotheekaanvraag kan de tijdrovende (papieren) administratie vervangen worden door een digitaal en dus sneller proces.



Bij vaak wisselen van baan kunnen de administratiekosten omlaag wat ten goede komt aan jouw pensioenopbouw.

# Ideal Cryptographic Properties of Blockchain

- *Consensus: One Truth*
  - all parties agrees on the same blockchain
  - thus all parties agree on processed transactions
- *Immutable: Final Truth*
  - Can only append a new Block of Transactions
  - Previous Blocks cannot be altered:  
Transactions are final
- *Verifiable Correct: Accountable*
  - Anyone can check entire Blockchain
- *Sound: Democratic*
  - A Transaction, when valid,  
will eventually be accepted
- *Secure*
  - If all above properties hold

Conflicting Transactions:  
Double Spending

Re-Spending

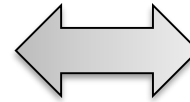
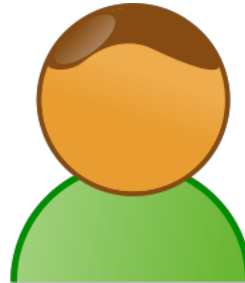
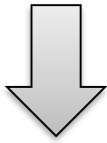
Illegitimate transactions

Denial-Of-Service



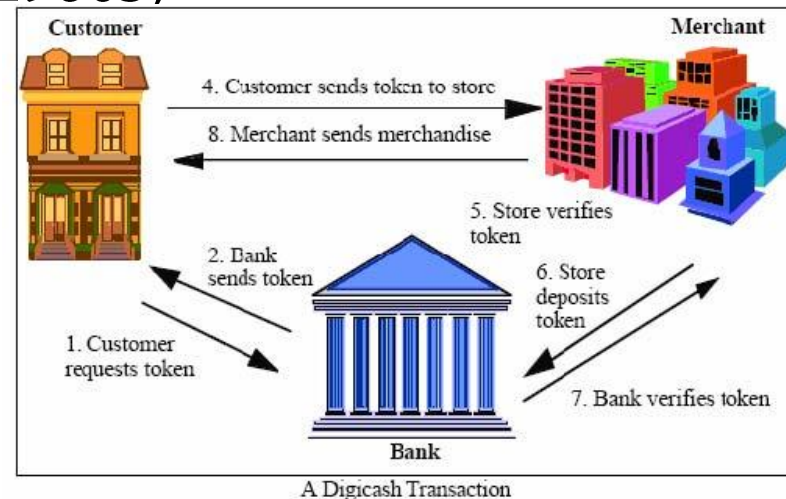
The First Blockchain:

The Bitcoin Solution



# Digital Currencies

- “Digital currency is a digital medium of exchange exhibiting properties similar to physical currencies.”
- Secure digital currency pioneered by David Chaum (head Cryptology Group, CWI, 1980s)
- DigiCash
  - Anonymous
  - Centralized
  - Fixed-value token signed by Bank





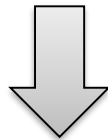
**decentral digital 'currency'**

decentral immutable  
chain of transactions

# Cryptographic Tools

- hash
- ‘digital fingerprint’

```
144g8xpNFUsKxHovczACoxDSOhotiA
QhL16j2kwD1eTmaUMiuWgqNSHncrsu2
69Z4nz147XLq8r7xnQSiCx19cNEd1j6
hJn3gnmqJ15AJMyf5Qx489hL81oziMN
.....
RgHjLHA4cjJt6cFB8JJ9cH5768PfSbx
cf3kb8XX3D386q1Gx1HpCBp7RjGbnS3
BZ3KWZgtGwv5Vc4351FoMpj2NT12FPE
```

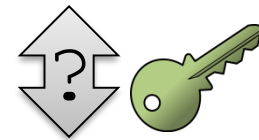
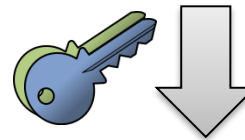


```
a441b15fe9a3cf56
661190a0b93b9dec
7d04127288cc8725
0967cf3b52894d11
```

hash pseudo-random  
inverting hash is practically  
impossible

## digital signature

```
144g8xpNFUsKxHovczACoxDSOhotiA
QhL16j2kwD1eTmaUMiuWgqNSHncrsu2
69Z4nz147XLq8r7xnQSiCx19cNEd1j6
hJn3gnmqJ15AJMyf5Qx489hL81oziMN
.....
RgHjLHA4cjJt6cFB8JJ9cH5768PfSbx
cf3kb8XX3D386q1Gx1HpCBp7RjGbnS3
BZ3KWZgtGwv5Vc4351FoMpj2NT12FPE
```

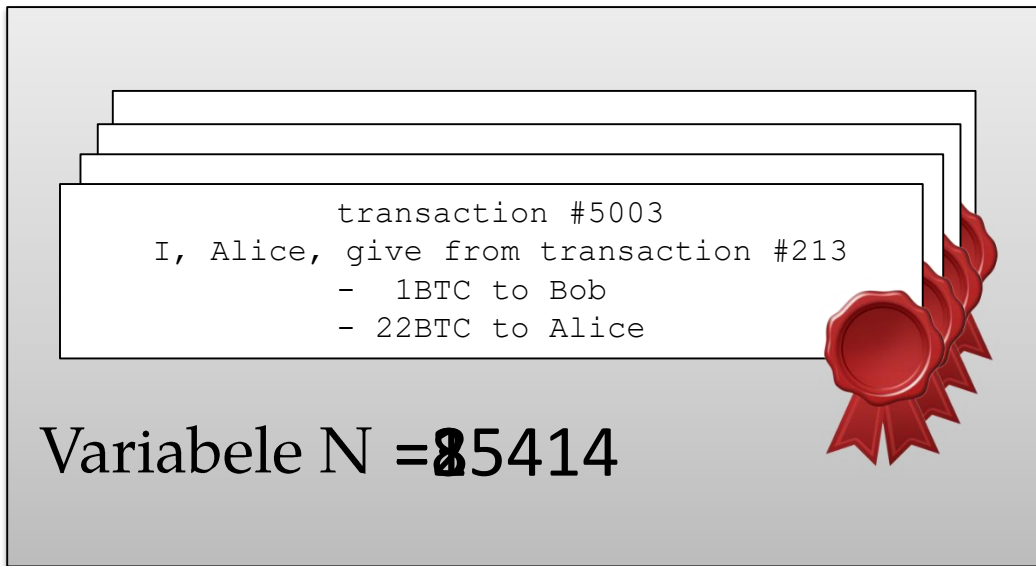


```
YTQ0MWIxNWZlOWEz
MTI3Mjg4Y2M4NzI1
MDk2N2NmM2I1Mjg5
NGQxMQ==
```

Creating forgeries is  
practically impossible

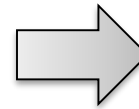
# Transactions are verified in Blocks with *Proof-of-Work*

## Block with new Transactions



transaction #5003  
I, Alice, give from transaction #213  
- 1BTC to Bob  
- 22BTC to Alice

Variabele N = **85414**



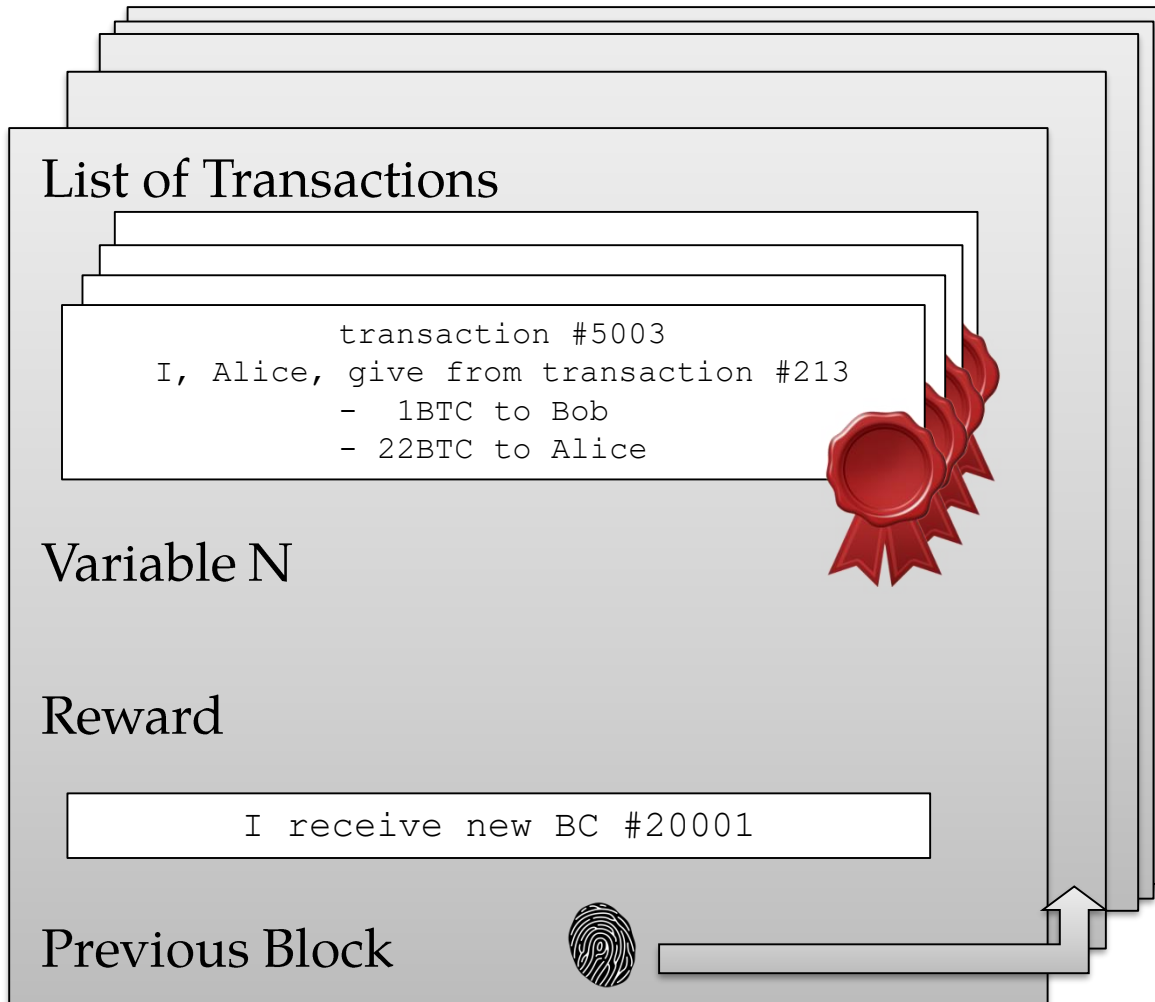
<? 0000010000000000  
0000000000000000  
0000000000000000  
0000000000000000  
0000008562bedb8b  
60ce05c1decfe3ad  
16b72230967de01f  
640b7e4729b49fce



Variable difficulty:

Goal is on average about 6 solutions per hour

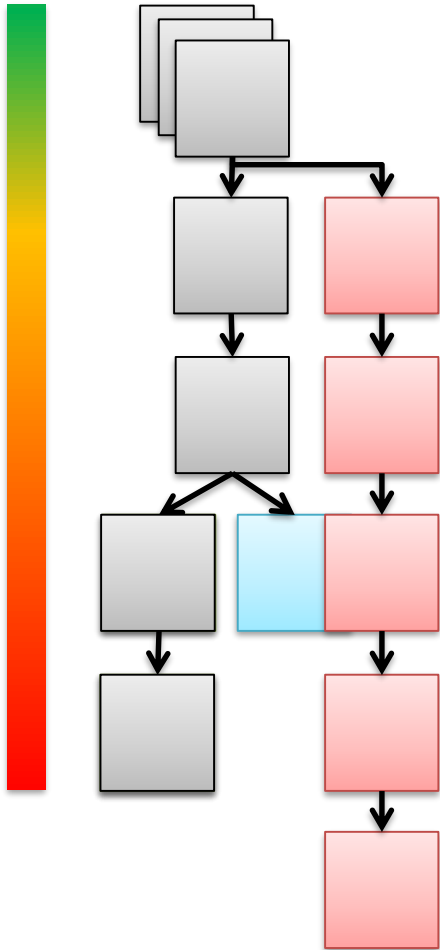
# *Blockchain:* Chain of Transaction Blocks



Long chain of Blocks

Transactions and their  
order clear to everyone

# Blockchain: Chain of Transaction Blocks



Every party maintains private copy

Longest Chain rules

Equally long Chains live till clear winner

Personal incentive to work on longest Chain

Adapting chain is race against the rest

to Bob => to Alice

Insecure against Majority of comp. power

Without Majority: Security of a Block grows exponential in # subsequent Blocks

Incentive crucial to guard against Majority, thus crucial to Security



# Ideal Properties

## Properties of the Bitcoin Blockchain Protocol

- *Consensus: One Truth*
  - all parties agrees on the same blockchain
  - thus all parties agree on processed transactions

Consensus up to last few blocks
- *Immutable: Final Truth*
  - Can only append a new Block of Transactions
  - Previous Blocks cannot be altered:  
Transactions are final

Only if no adversarial group has Majority computational power
- *Verifiable Correct: Accountable*
  - Anyone can check entire Blockchain

Transparent & Pseudonymous
- *Sound: Democratic*
  - A Transaction, when valid, will eventually be accepted

Sufficiently many Honest Miners  
Limit on Transactions per Block
- *Secure*
  - If all above properties hold

Other blockchains:  
weak & strong immutability

# Immutability without Proof-of-Work

- *Strong immutability:*  
if protection against malicious changes is **computationally hard**
- *Weak immutability:*  
Otherwise: protection against malicious changes is obtained through **incentives** or **monitoring**
- Without proof-of-work there is no computational problem creating additional problems to solve:
  - low cost simulations
  - cheap to have multiple forks

# Immutability classification

## Strong Immutability

- Proof-of-Work
- Proof-of-Work in small networks

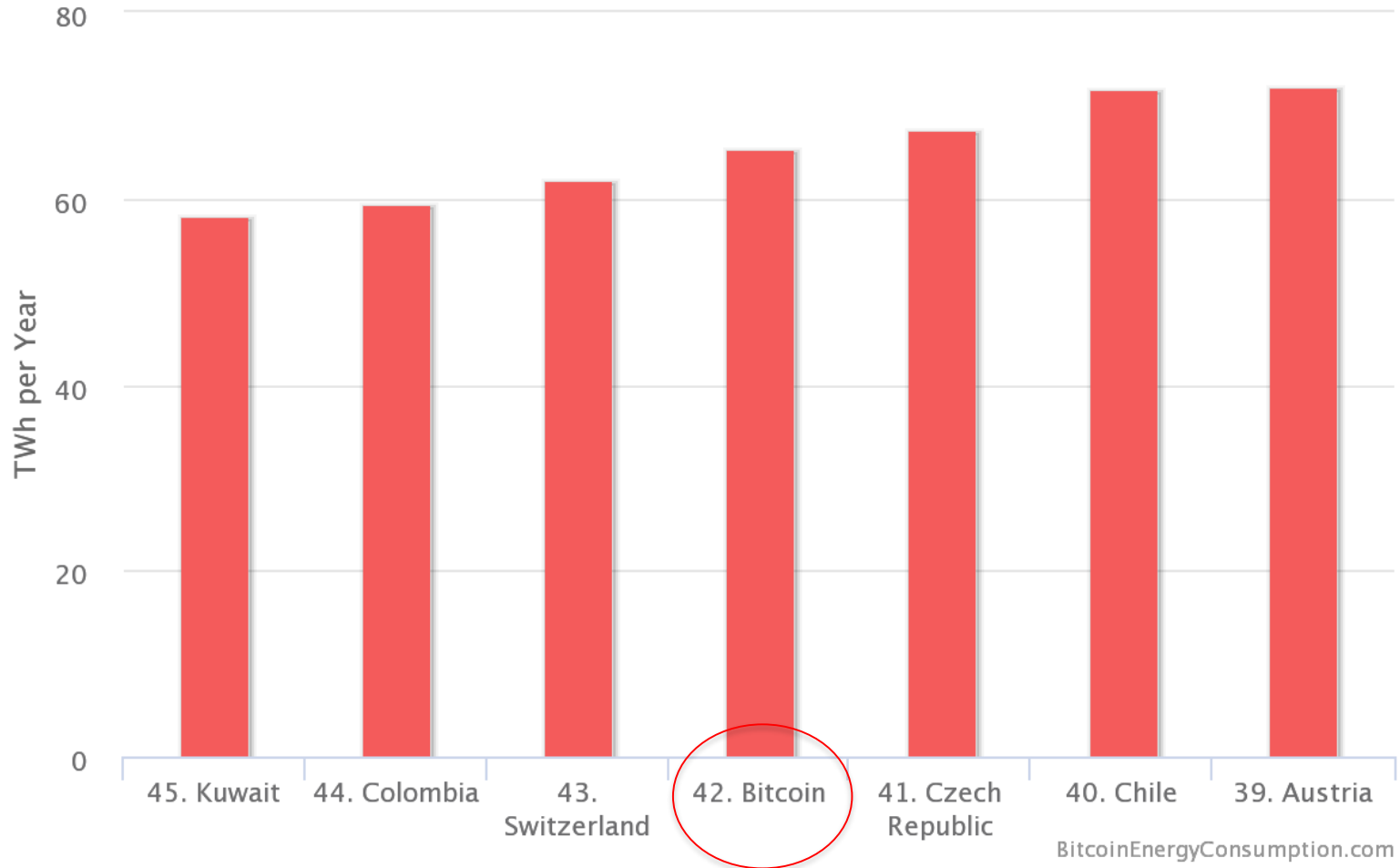
## Weak Immutability

- Proof-of-Stake
- Proof-of-Space
- ...

- BFT-based
- ...

# Proof-of-Work is not sustainable

Energy Consumption by Country Chart



# Another solution:

## A new cryptographic tool: VDF

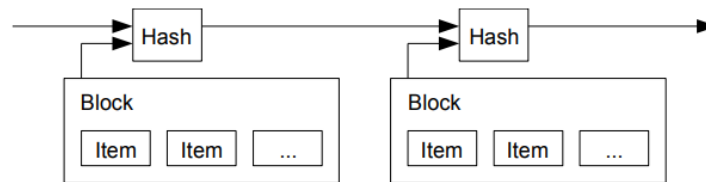
- **Verifiable delay functions (VDF)**
  - *Function*: unique output for every input
  - *Delay*: can be evaluated in time  $T$  on 1 CPU, but not faster than time  $T$  on  $N$  CPUs.
  - *Verifiable*: correctness can be verified very fast
  - Constructions by Wesolowski (CWI), working towards special hardware together with Ethereum foundation
- Unlike PoW a VDF cannot be used to build consensus
- Our work: VDFs can be used to add strong immutability

# Timestamping with VDFs

- An immutable blockchain is a timestamping mechanism

## 3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



- Our result goes the other direction:
  - Build timestamping mechanism from VDFs
  - Timestamping adds strong immutability to blockchains

# Timestamping with VDFs

- Our timestamping construction [Landerreche, Schaffner, Stevens, 2018]
  - Single prover protocol & multi-prover protocols
  - Based on VDFs
  - Non-interactive:  
timestamping proofs are publicly verifiable and transferable
  - **Secure-by-design:**  
proved secure in the *universal composability framework*



# Strong immutability achieved

## Strong Immutability

- Proof-of-Work
- Proof-of-Work in small networks

- Proof-of-Stake + VDF
- Proof-of-Space + VDF

- BFT-based + VDF

## Weak Immutability

- Proof-of-Stake
- Proof-of-Space
- ...

- BFT-based
- ...

CWI

IN BEDRIJF

Digitaal kompas

16 mei 2019

Digital Compass:

“Secure by design”  
/ “provable-secure”

scientific computing

predictions

algorithm

complex data

cybersecurity

digital finance

data systems

quantum software

blockchain

neuroscience

AI

societal relevance

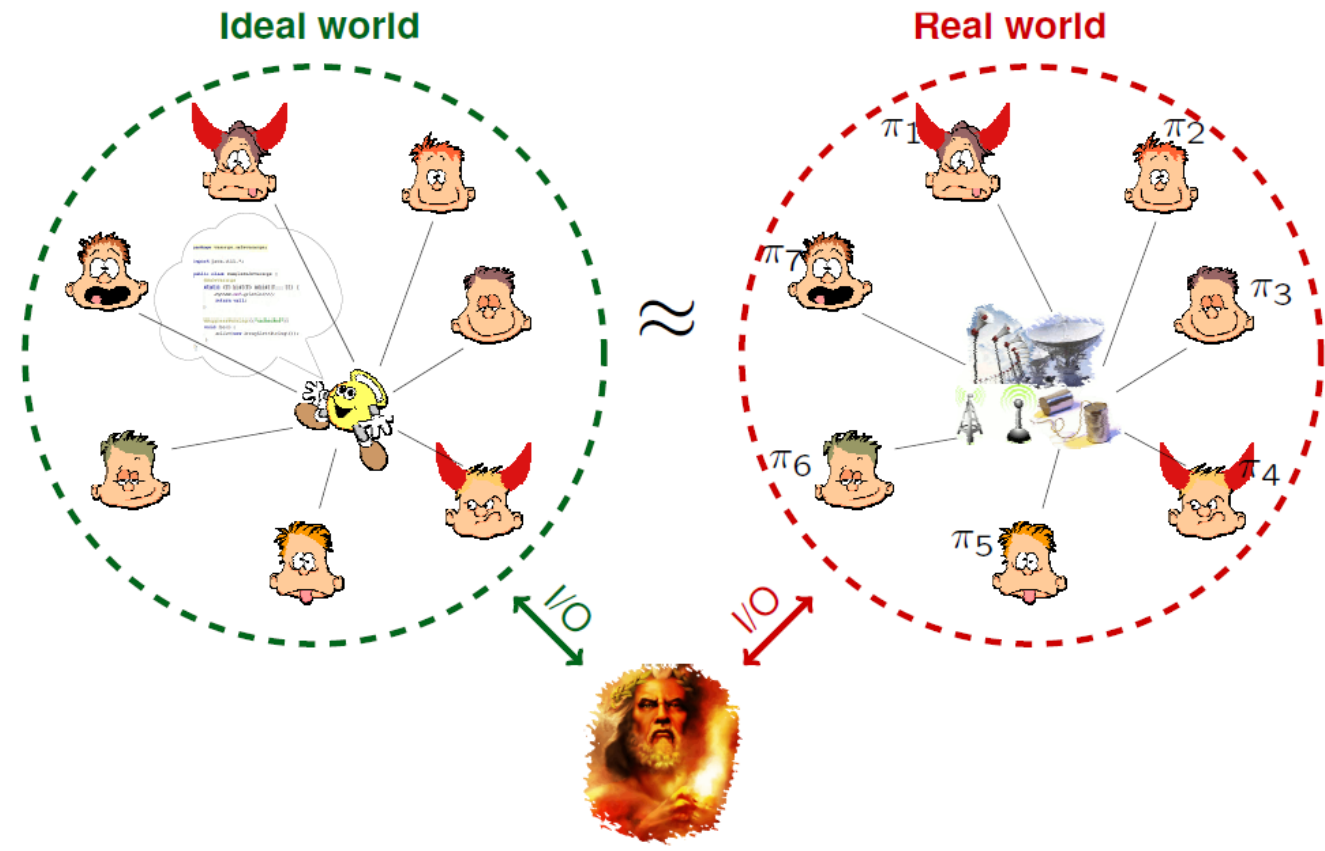
machine learning

# Provable security

- Many constructions in Blockchain are **ad-hoc** constructions
  - Providing *arguments* against common attacks, not proofs
- Some constructions are proven-secure (sometimes after-the-fact: Bitcoin)
  - Cryptographic proof that construction achieves ideal properties
  - Or cryptographic proof that construction behaves like an ideal functionality
  - Strong guarantees against entire classes of possible adversaries

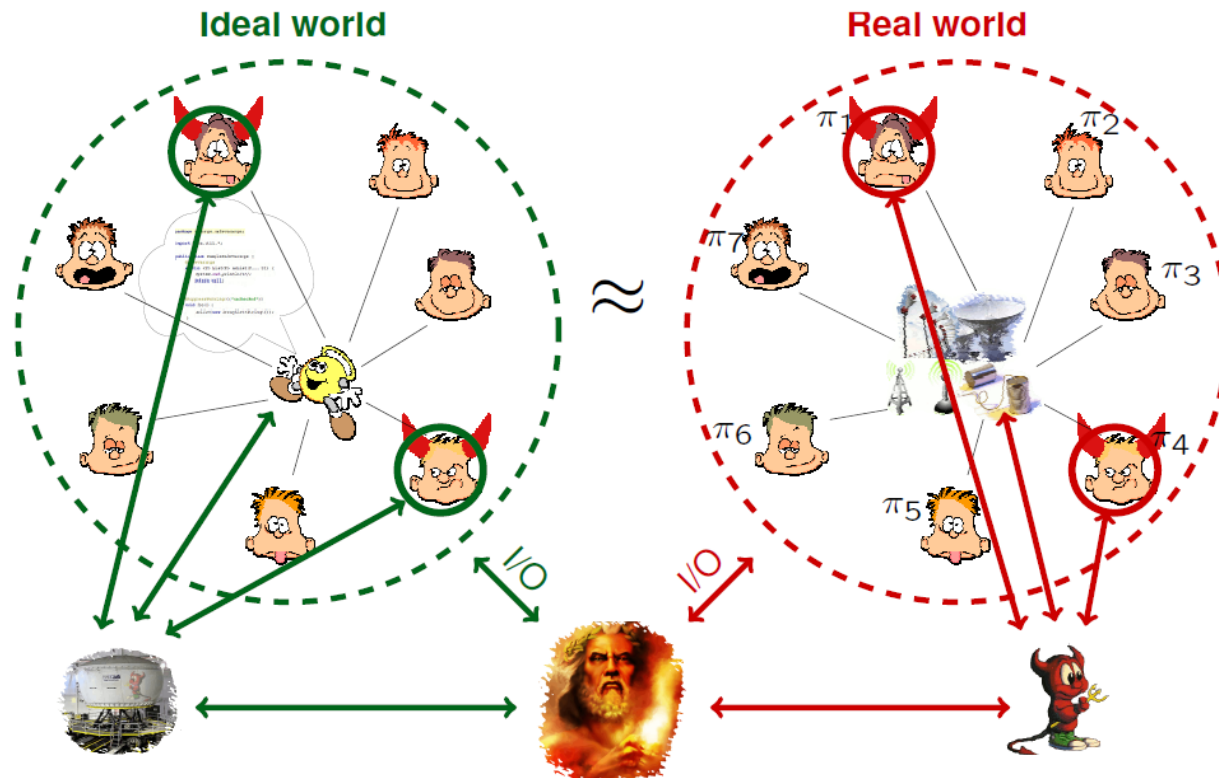
# Ideal / Real

- Ideal/real paradigm:  
outsiders should not be able to distinguish between worlds



# Adversaries

- Moreover, for any adversary in the real world there should be an 'equivalent' ideal adversary



- Indistinguishability implies that any real adversary can only achieve things what the ideal functionality allows

Thank you for your attention!