Blockchain Basics
and Examples: eMoney and eVoting

Roger Wattenhofer

ETH Zurich – Distributed Computing Group

Blockchain = Ledger

Figure 9-3 Manual Journal Voucher.

Page 1 of 1

MANUAL JOURNAL VOUCHER

PREPARED BY	DATE
WLR	2/2/X5
APPROVED	DATE

Batch 1101	Batch Line 9	Total Amount 11,200.20
Description ACCRUED INTEREST INCOME		Effective Date 1/31/X5 · Type A
Reference J43-JAN INTEREST		Accounting Company 10- CORPORATE

Seq.	Account Number	Description	Debit Amount	Credit Amount
01	1280-000	INTEREST RECEIVABLE	11,200.20	
02	8050-010	FIRST NATIONAL - CD		1,330.10
03	8050-020	MUNICIPAL BONDS		6,220.80
04	8050-010	OTHER INVESTMENTS		3,649.30
05				
06				
07				
08				
09				
10				
11				
12				
		Footing	11,200.20	11,200.20

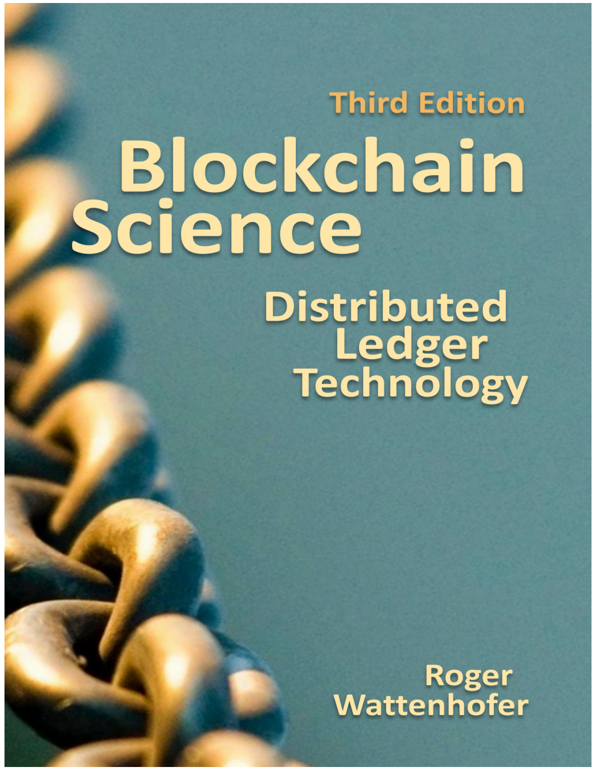
FinTech developers and managers understand that the *blockchain* has the potential to disrupt the financial world. The blockchain allows the participants of a distributed system to agree on a common view of the system, to track changes in the system, in a reliable way. In the distributed systems community, agreement techniques have been known long before cryptocurrencies such as Bitcoin (where the term blockchain is borrowed) emerged. Various concepts and protocols exist, each with its own advantages and disadvantages. This book introduces the basic techniques when building fault-tolerant distributed systems, in a *scientific* way. We will present different protocols and algorithms that allow for fault-tolerant operation, and we will discuss practical systems that implement these techniques.

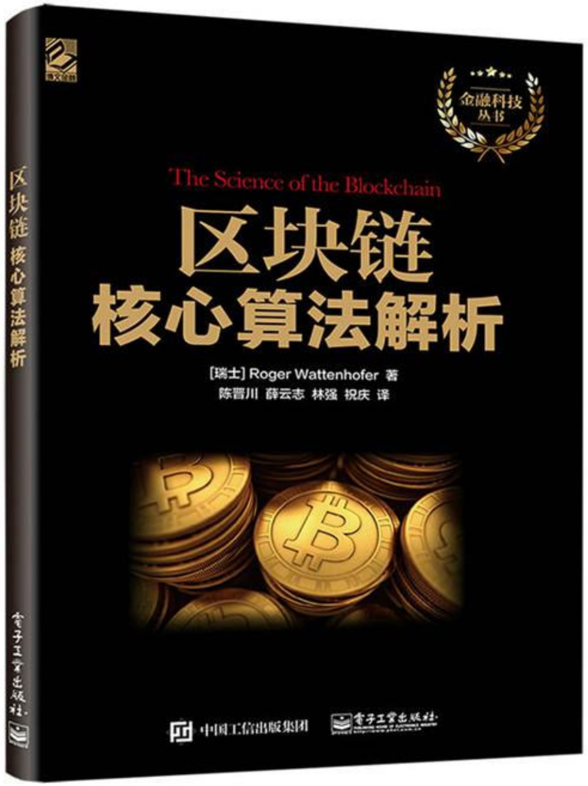
About the author

Roger Wattenhofer is a professor at ETH Zurich. Before joining ETH Zurich, he was at Brown University and Microsoft Research. His research interests include fault-tolerant distributed systems, efficient network algorithms, and cryptocurrencies such as Bitcoin. He has published more than 250 scientific articles.

Inverted Forest Publishing
First Edition, 2016
ISBN-13 978-1522751830
ISBN-10 1522751831

ISBN 9781522751830


Third Edition
Blockchain
Science
Distributed
Ledger
Technology
Roger
Wattenhofer

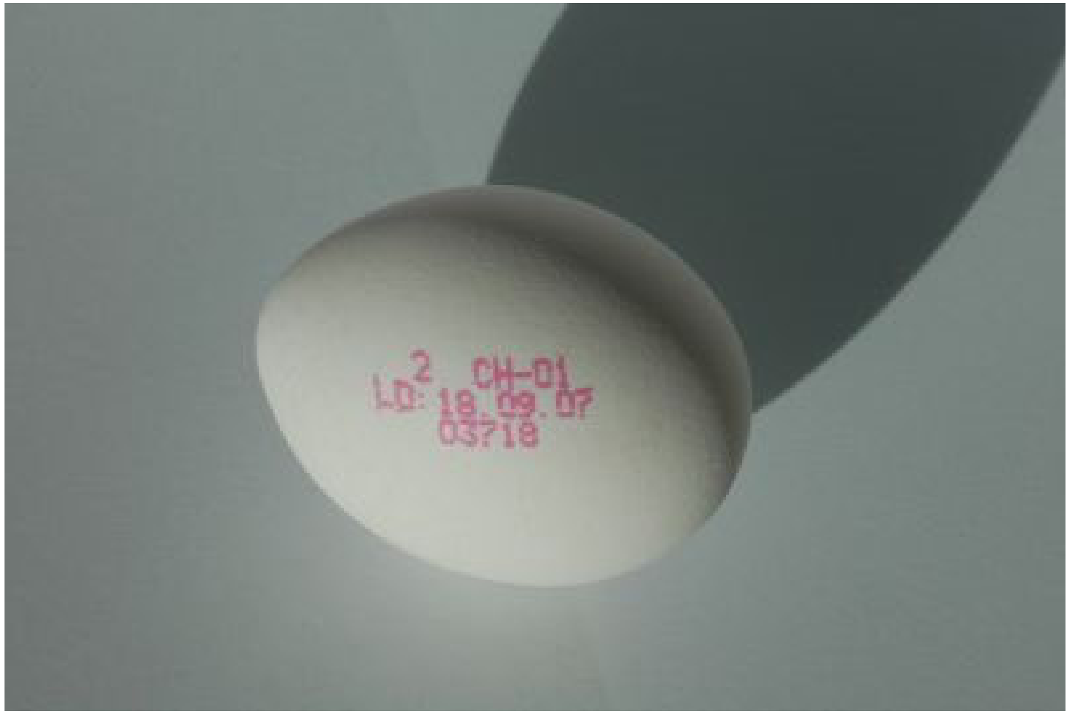

金融科技
丛书
The Science of the Blockchain
区块链
核心算法解析
[瑞士] Roger Wattenhofer 著
陈晋川 薛云志 林强 祝庆 译
区块链 核心算法解析
中国工信出版集团
电子工业出版社

Blockchain Basics

Transaction

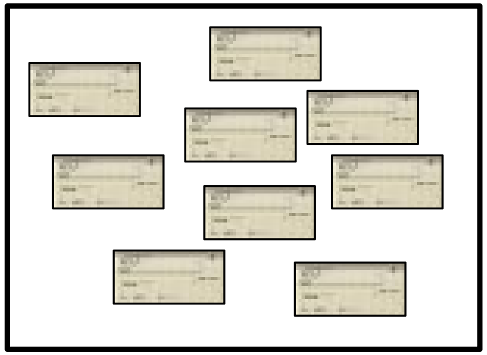
Transaction

Transaction

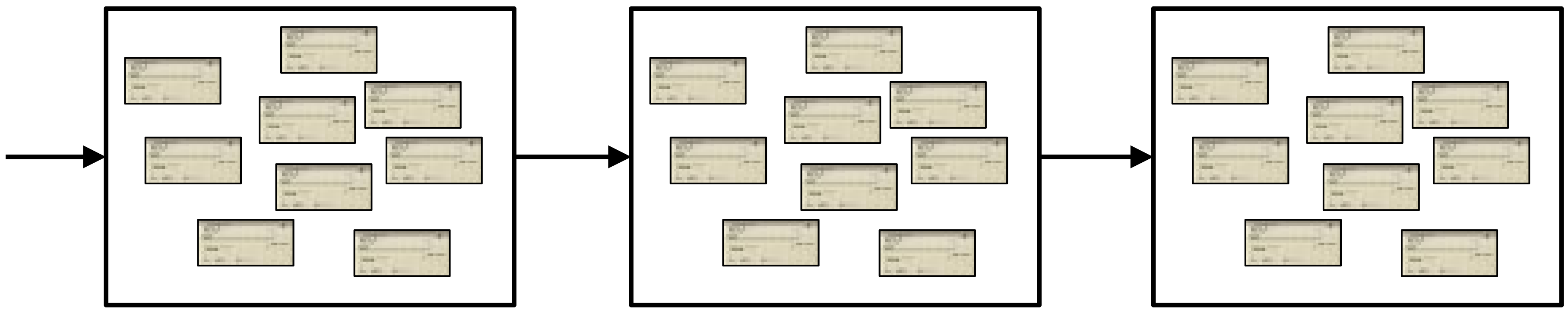


Transaction

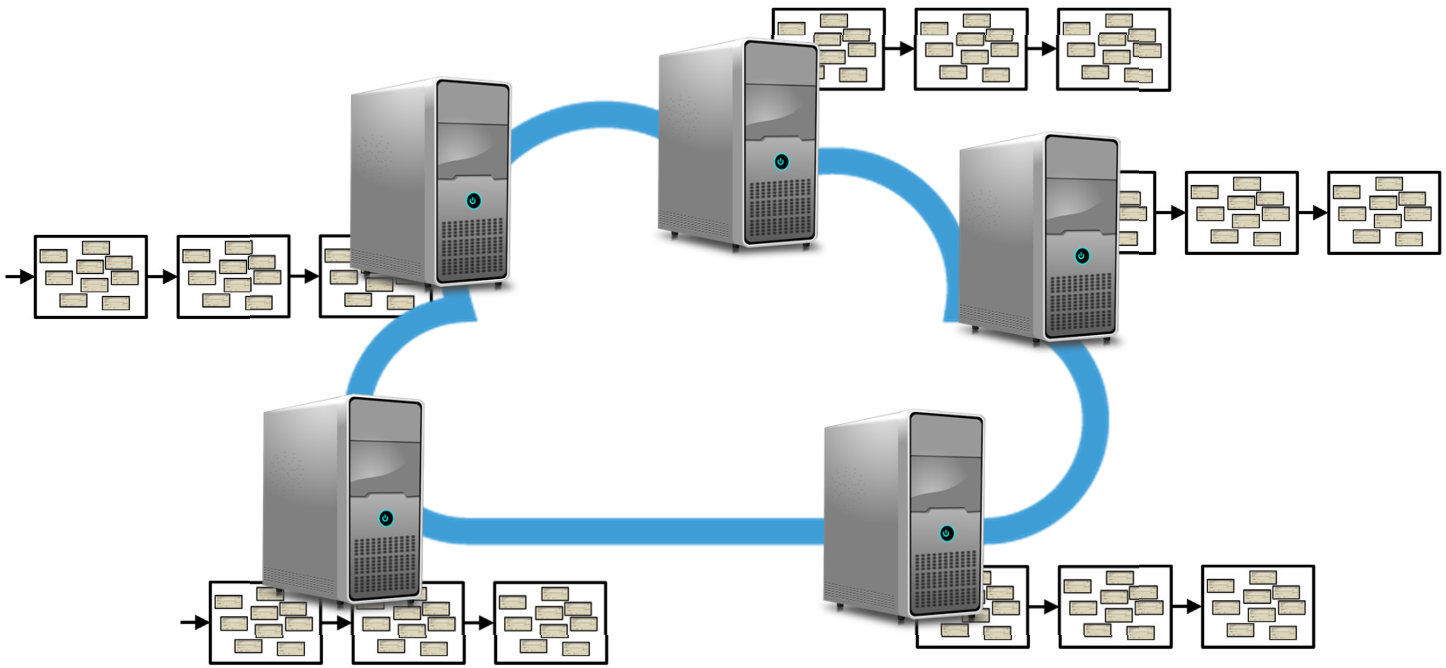
Block



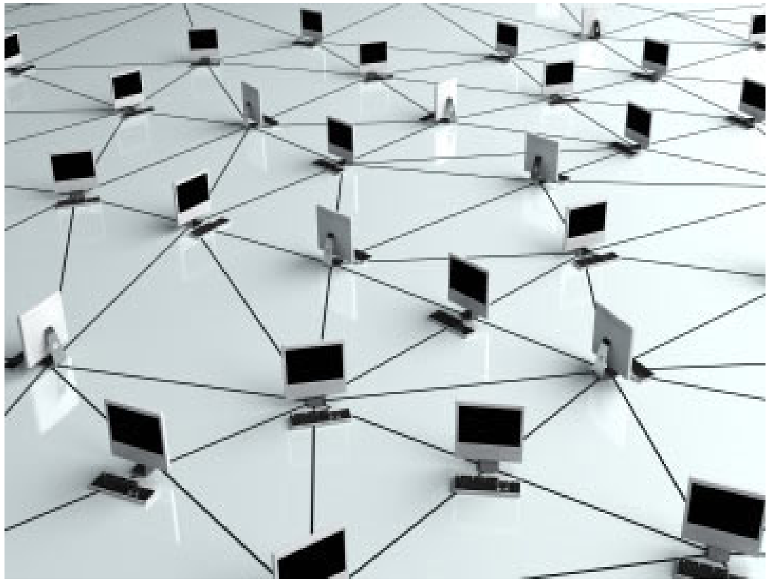
Blockchain



A Blockchain is Replicated



Blockchain Ingredients



&

Distributed Systems

Cryptography

Turing Awards

2008 Barbara Liskov
2010 Leslie Valiant*
2013 Leslie Lamport

Rivest, Shamir & A. 2002
Micali & Goldwasser 2012
Hellman & Diffie 2015

Asymmetric Cryptography

“Magic with Numbers”

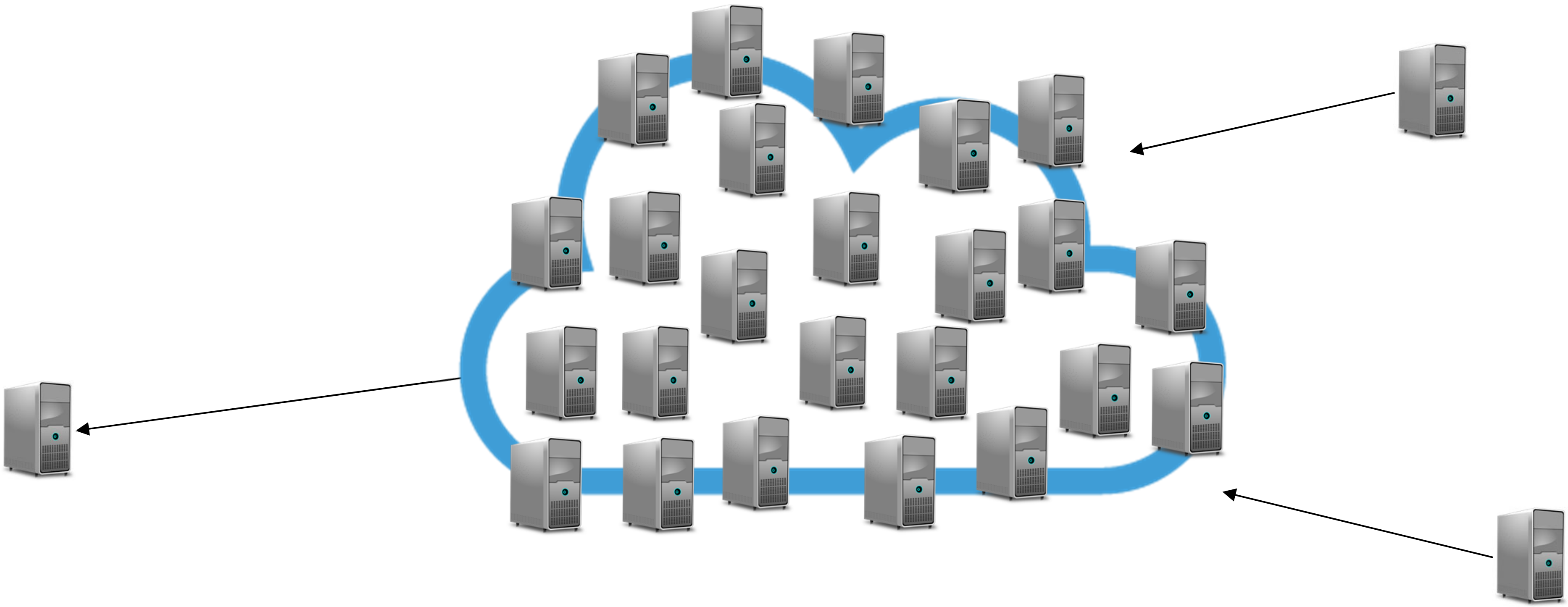
Encryption

Digital Signatures

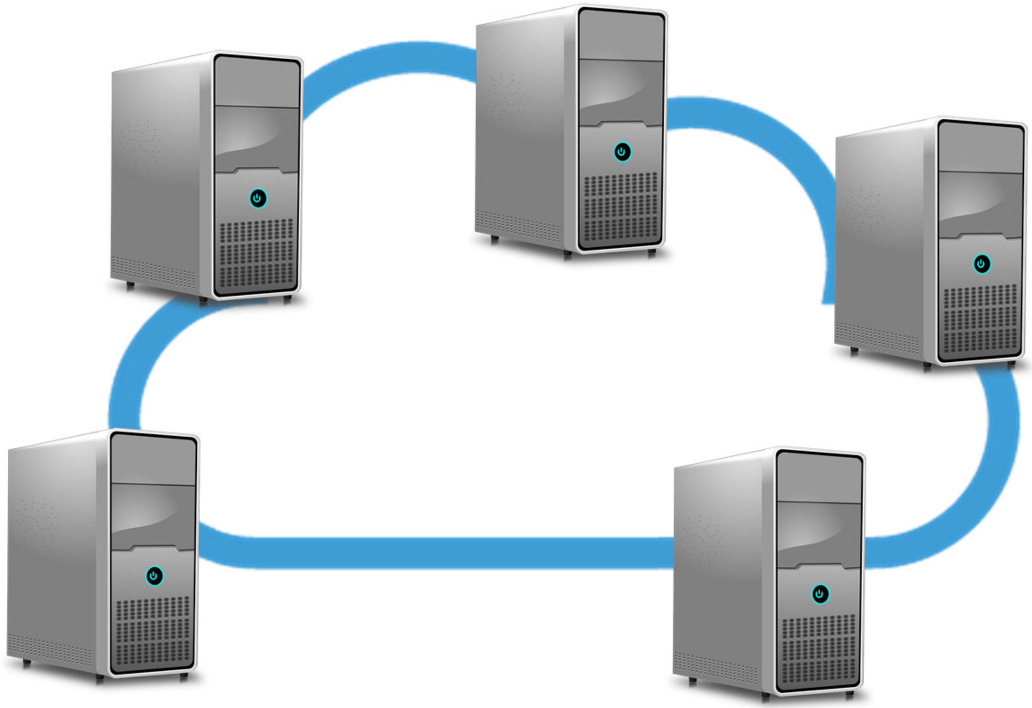
Generating a Secret

Blockchain Variants

Permissionless / Open



Permissioned / Closed



Ledger of Transactions

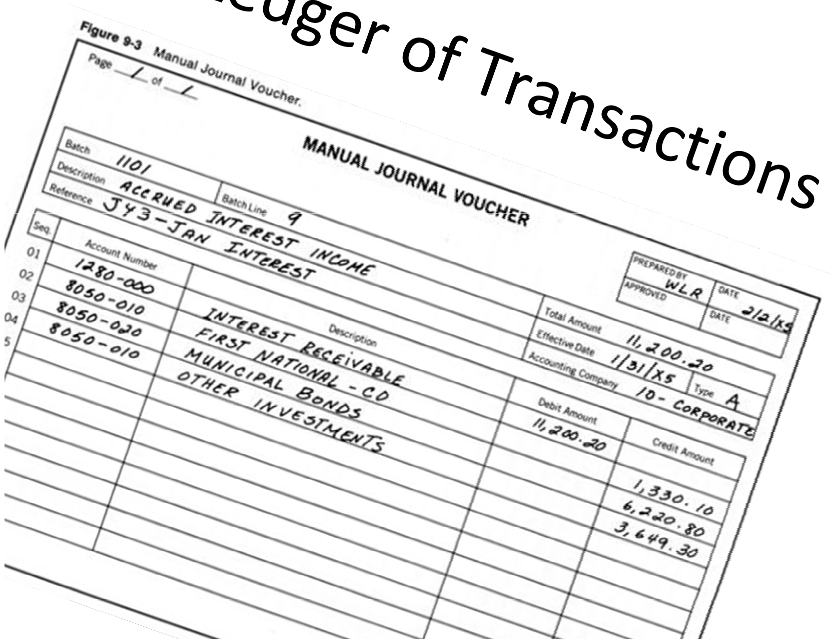


Figure 9-3 Manual Journal Voucher.

Page 1 of 1

MANUAL JOURNAL VOUCHER

Batch 1101

Batch Line 9

Description ACCRUED INTEREST INCOME

Reference J43-JAN INTEREST

PREPARED BY WLR DATE 2/2/X5

APPROVED DATE

Total Amount 11,200.20

Effective Date 1/31/X5

Accounting Company 10-CORPORATE

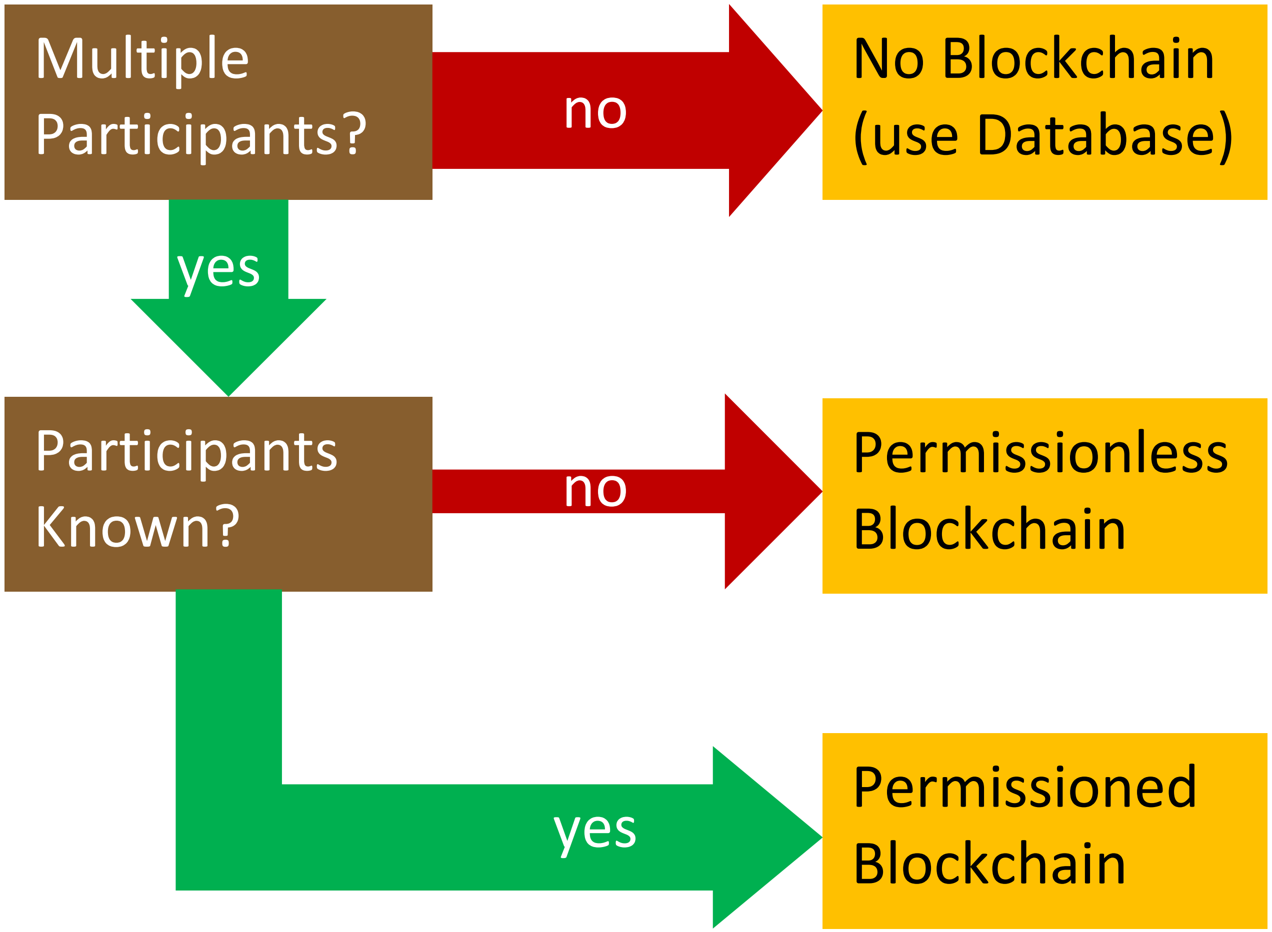
Type A

Seq.	Account Number	Description	Debit Amount	Credit Amount
01	1280-000	INTEREST RECEIVABLE	11,200.20	
02	8050-010	FIRST NATIONAL-CD		1,330.10
03	8050-020	MUNICIPAL BONDS		6,220.80
04	8050-010	OTHER INVESTMENTS		3,649.30
05				

Bitcoin

Do you need a Blockchain?

No.*

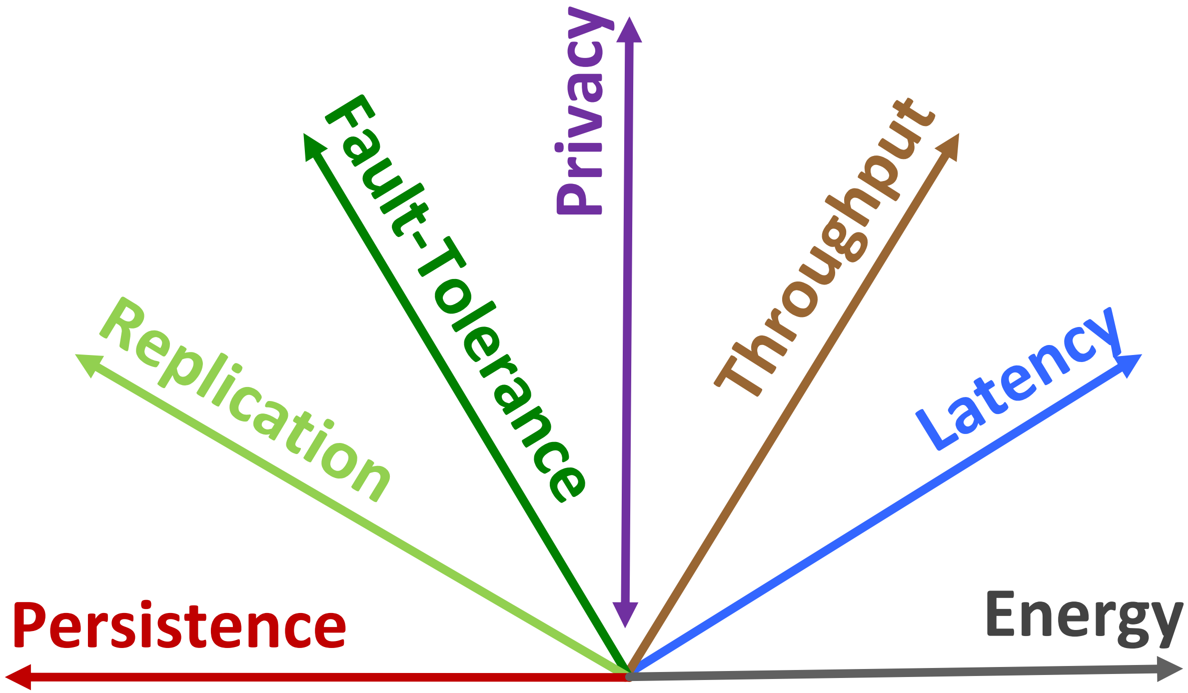

Multiple Participants?
no
No Blockchain (use Database)
yes
Participants Known?
no
Permissionless Blockchain
yes
Permissioned Blockchain

Rule of Thumb

Blockchains* may disrupt your business
if you use signatures.

*or blockchain-like tech

The Seven Blockchain Dimensions



Persistence

Database

↓

Immutable

↓

Provable 

Fault-Tolerance

Correct

↓

Crash

↓

Byzantine 

Latency

1 hour

↓

1 minute

↓

1 second

Throughput

10 tx/s

↓

10k tx/s

↓

10m tx/s

Replication

main+backup

↓

some nodes

↓

1000 nodes 

Energy

Proof-of-Work 

↓

Proof-of-Stake

↓

Permissioned

Energy Consumption

sonntagszeitung.ch | 17. Dezember 2017 Wissen 55

«Ich wäre nicht überrascht, wenn Bitcoin verboten würde»

ETH-Informationstechnologe Roger Wattenhofer über den Energiebedarf der Kryptowährung und bessere Alternativen

Prof. Dr. Roger

Economic Incentives

Market / Energy Value ≈ 3 GW

\$0.25M/h \$0.08/kWh

Proof-of-Work Energy

$$\underset{13 \cdot 10^{9}\ \text{GH/s}}{\text{Hashrate}} \quad \cdot \quad \underset{0.1\ \text{J/GH}}{\text{Energy/Hash}} \quad \approx \quad 1.3\ \text{GW}$$

- Genau weiss man das nicht. Aber man kann den Energiebedarf auf verschiedene Arten abschätzen. Man weiss, wie viele Rätsel pro Sekunde gelöst werden, und wie viel Energie die effizienteste Hardware für das Lösen der Rätsel benötigt. Damit kommt man auf ca. 1,3 Gigawatt. Die reale Leistung ist sicher höher, da man die Geräte auch noch kühlen muss, und nicht alle die beste Hardware benutzen. Andererseits: Wenn man die 1,2 Millionen Franken pro Stunde durch die Stromkosten in China von ca. 8 Rappen pro Kilowattstunde teilt, erhält man ca. 15 Gigawatt elektrische Leistung. Wenn man mehr als 15 Gigawatt aufwendet, lohnt sich das Mining nicht mehr. Wenn der Wert darunter ist, dann lohnt es sich, neue Hardware zu kaufen und anzuschliessen.
- Obere Schranke: Momentan ist der Bitcoin Preis ca. 17kF. Pro Block verdient (schürft) ein Miner 12.5 Bitcoins (plus Transaktionsgebühren). Alle 10 Minuten wird

Replication

main+backup

↓

some nodes

↓

1000 nodes 

Energy

Country 

↓

Server Room

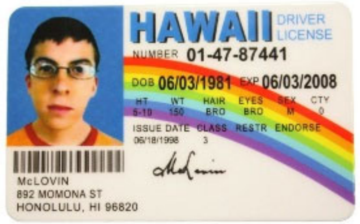
↓

Computer

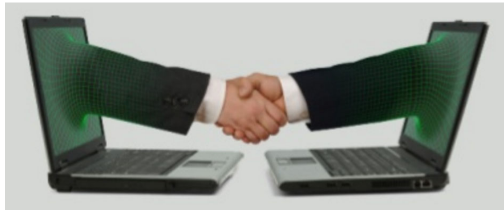
What About Privacy?

It’s Complicated.

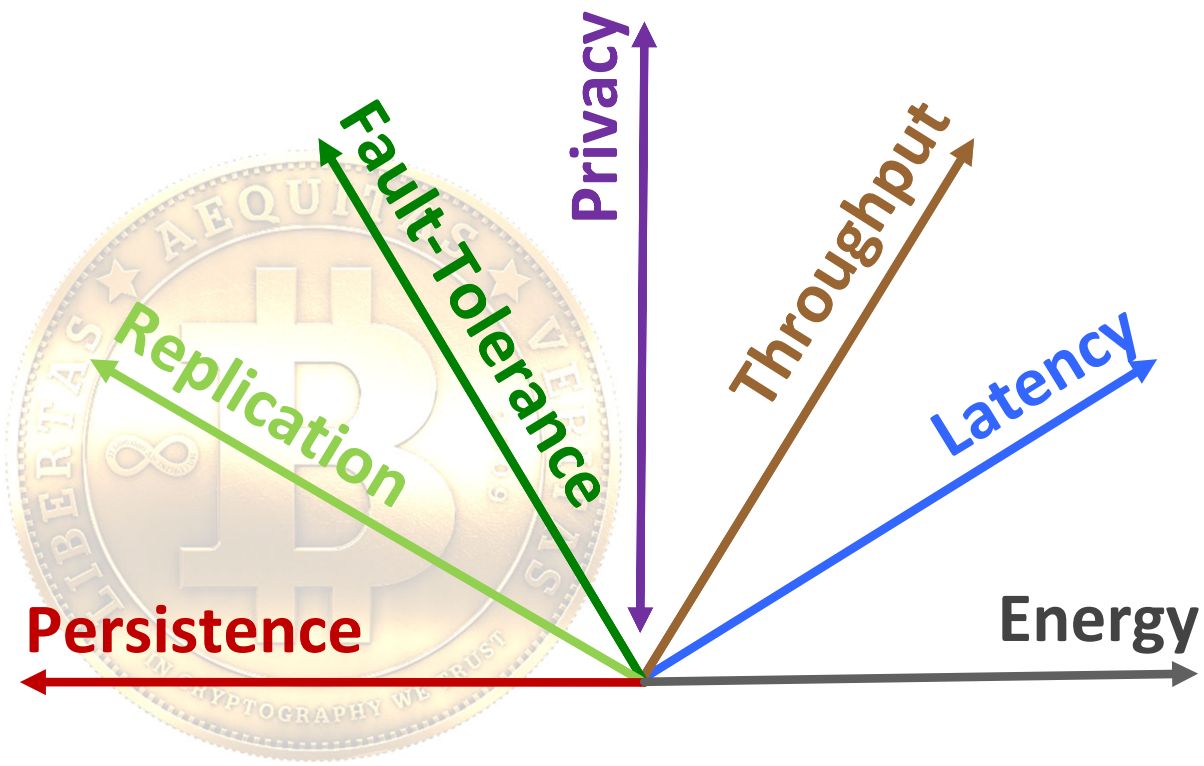
Privacy

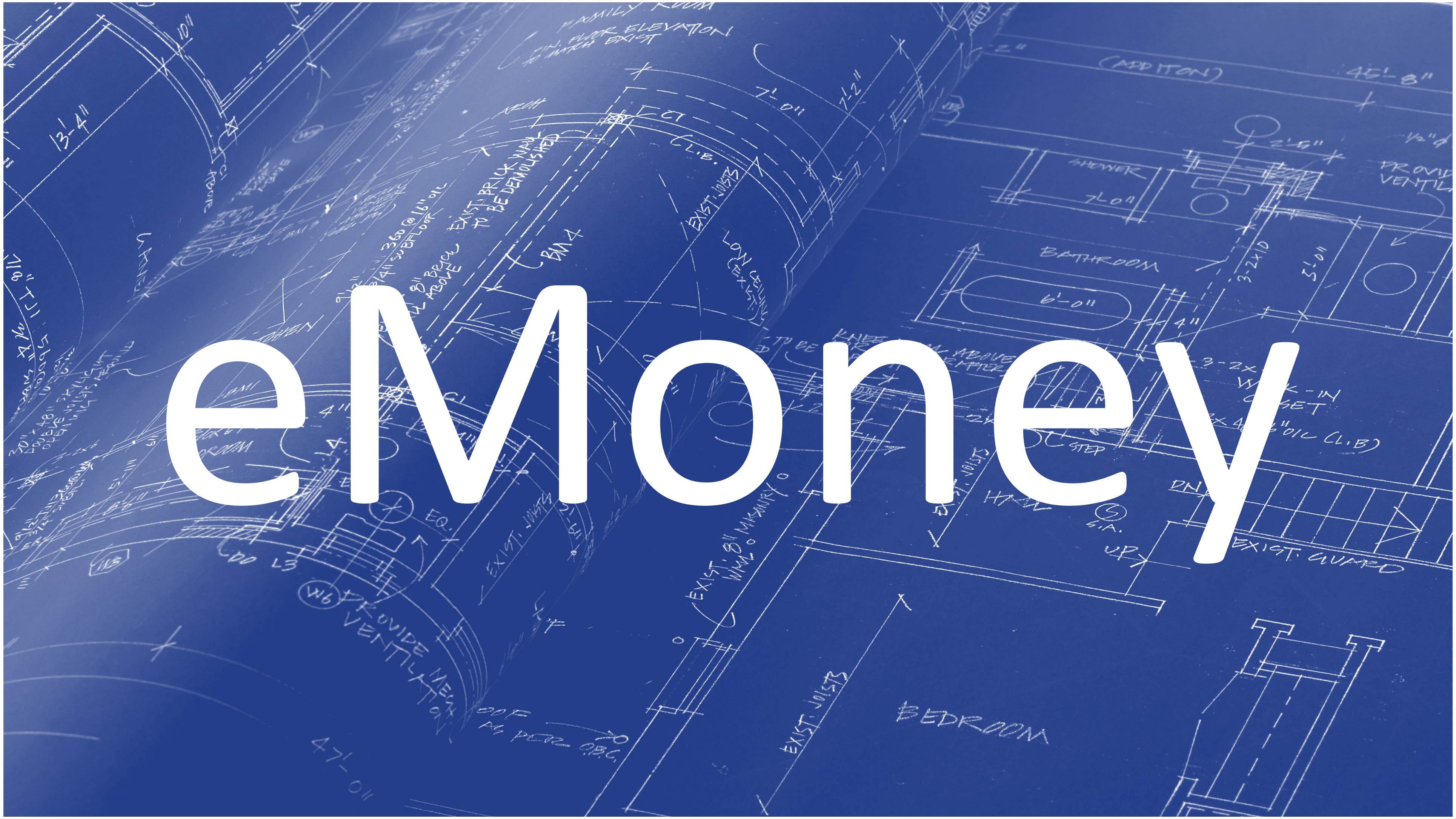


Anonymity ⟷ Identity



The Seven Blockchain Dimensions



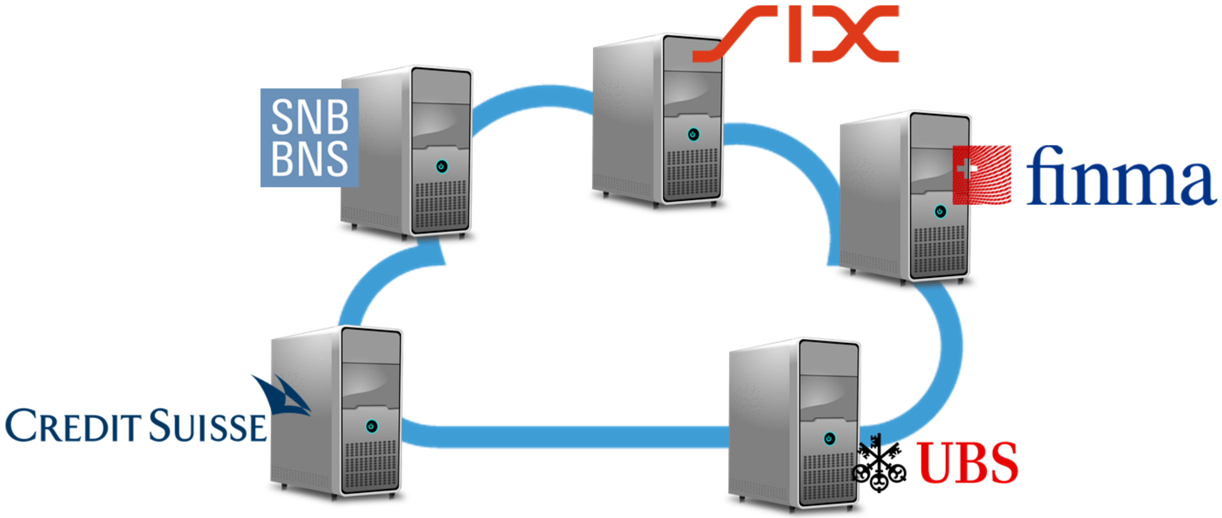

eMoney
SHOWER
BATHROOM
BEDROOM

Permissioned Blockchain

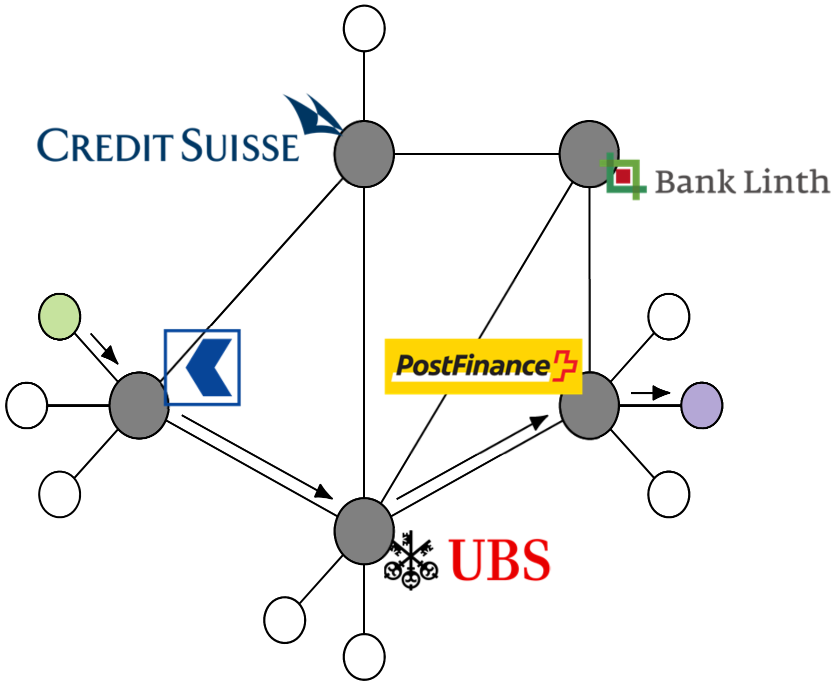
&

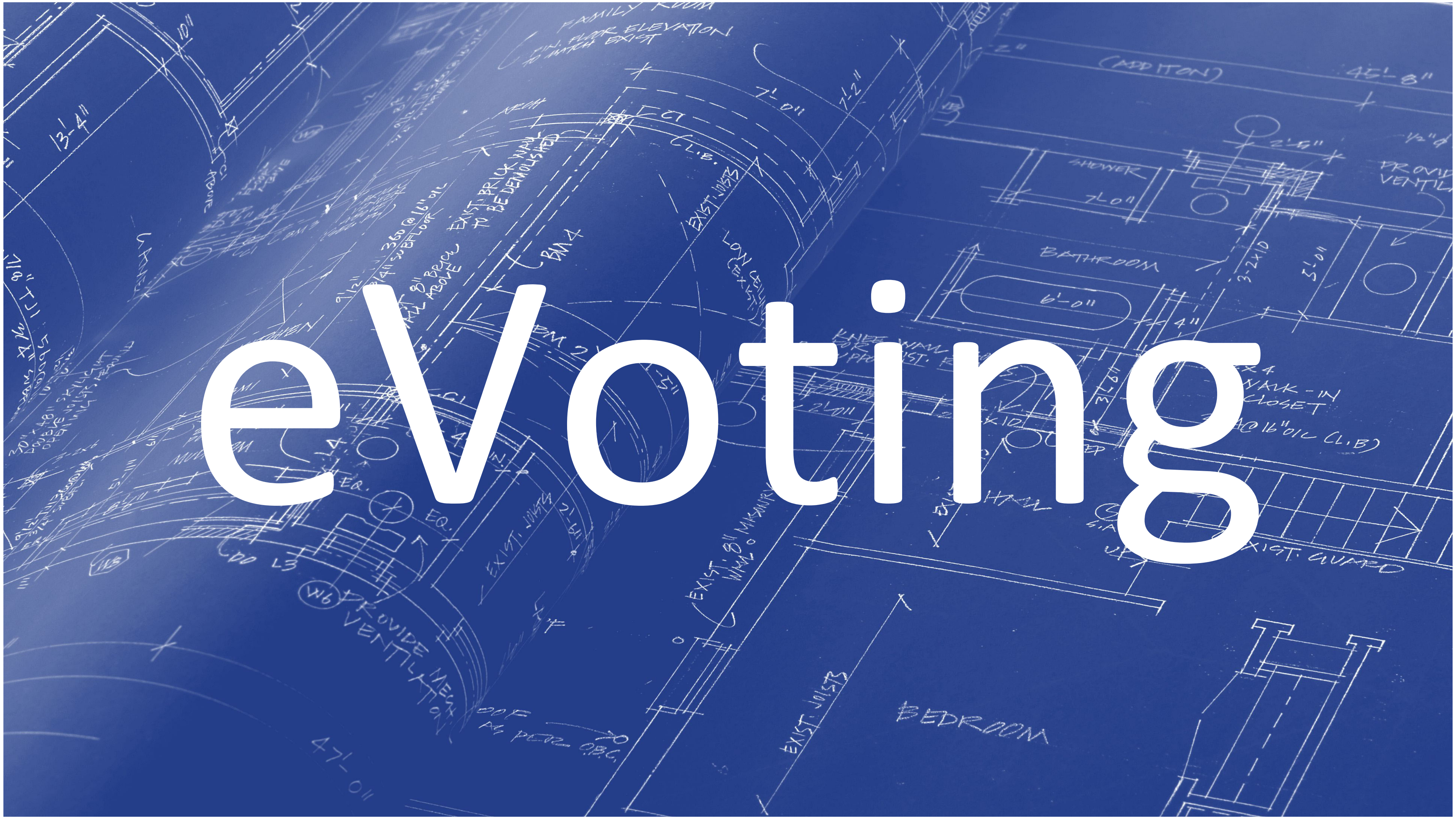
Payment Network

Permissioned Blockchain



Payment Network




eVoting

What’s Wrong with Paper?

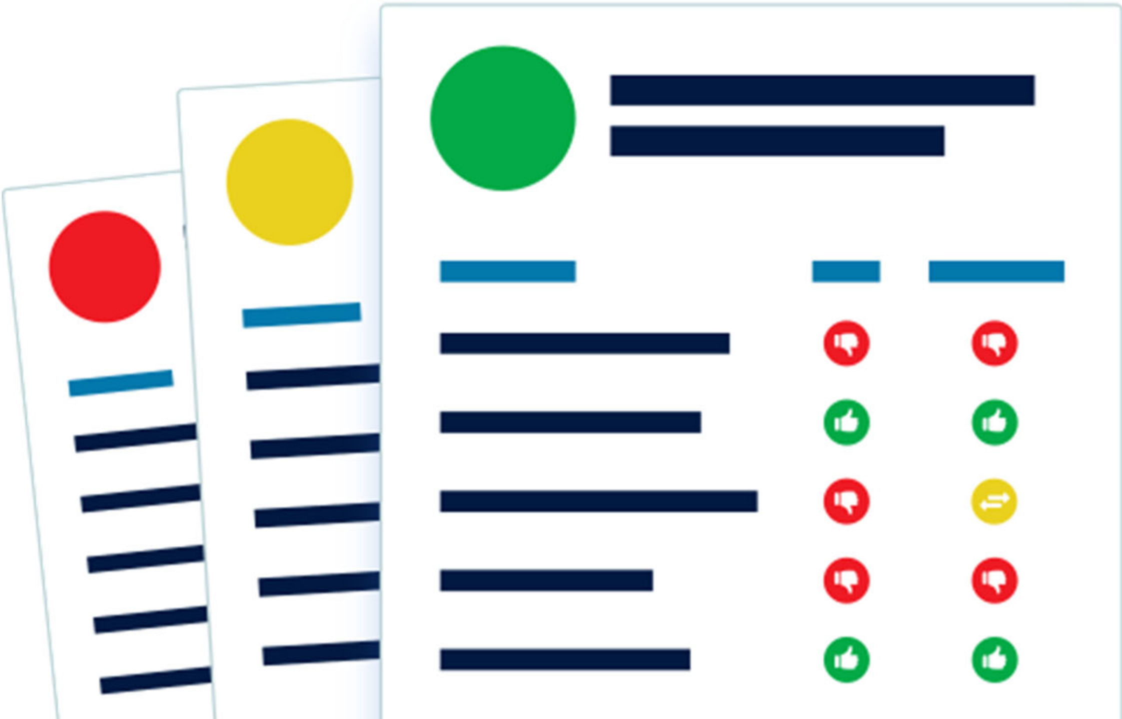
Cost

Verifiability

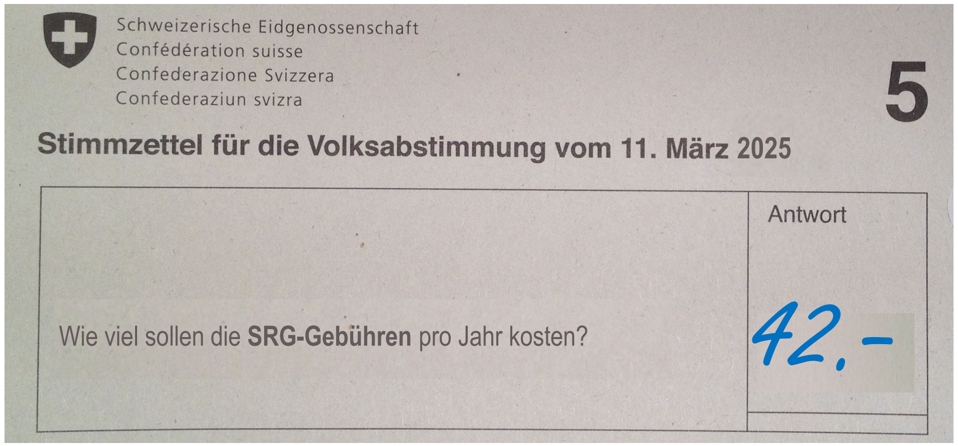
Neue Zürcher Zeitung

Rund 26 Prozent der Zürcher Wahlzettel waren nicht gültig

Election Help

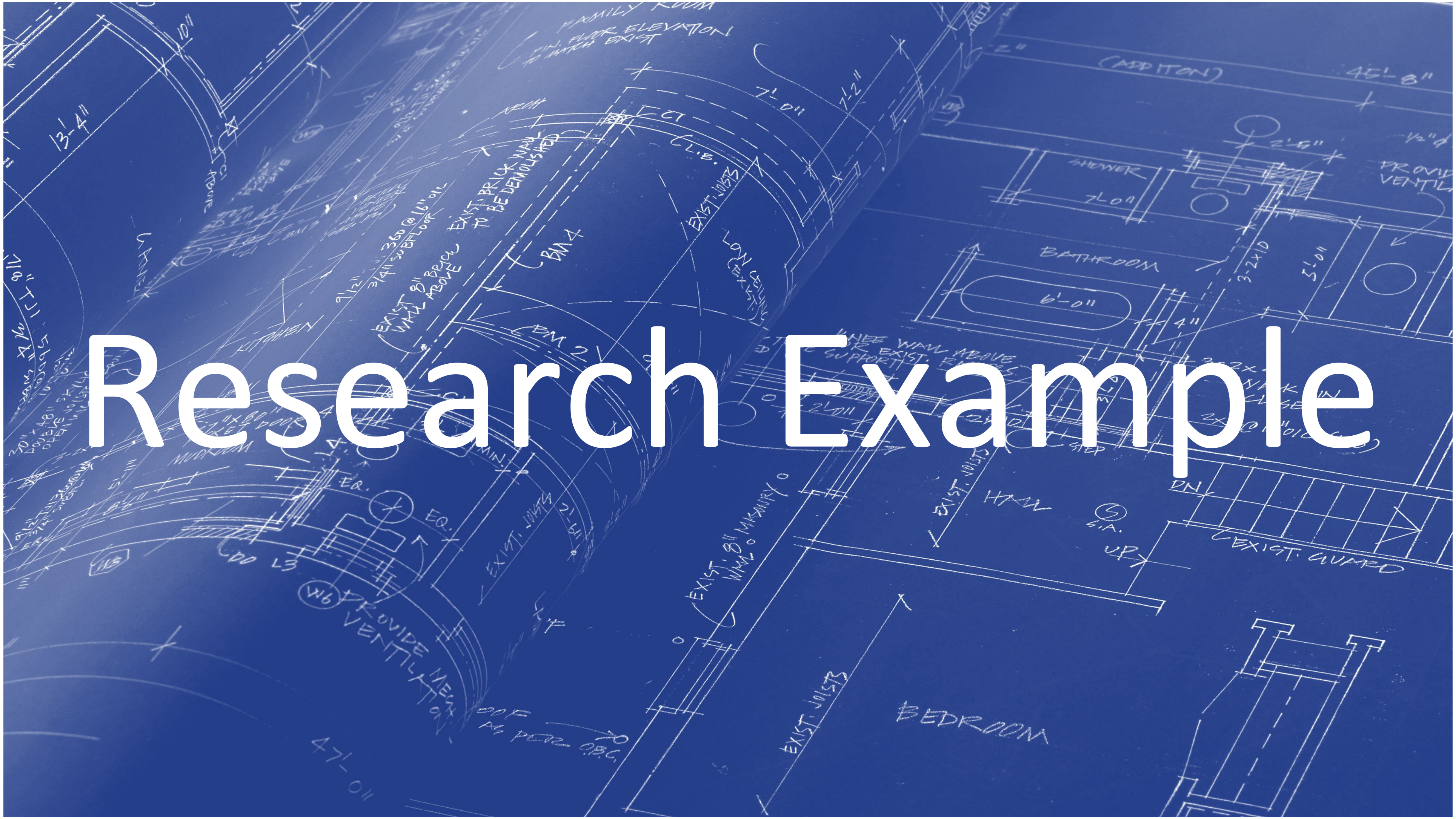


Democracy Beyond Yes or No



Anonymity with Identity Swapping

Research Example



Modeling Distributed Systems

Altruistic

Rational

Crash

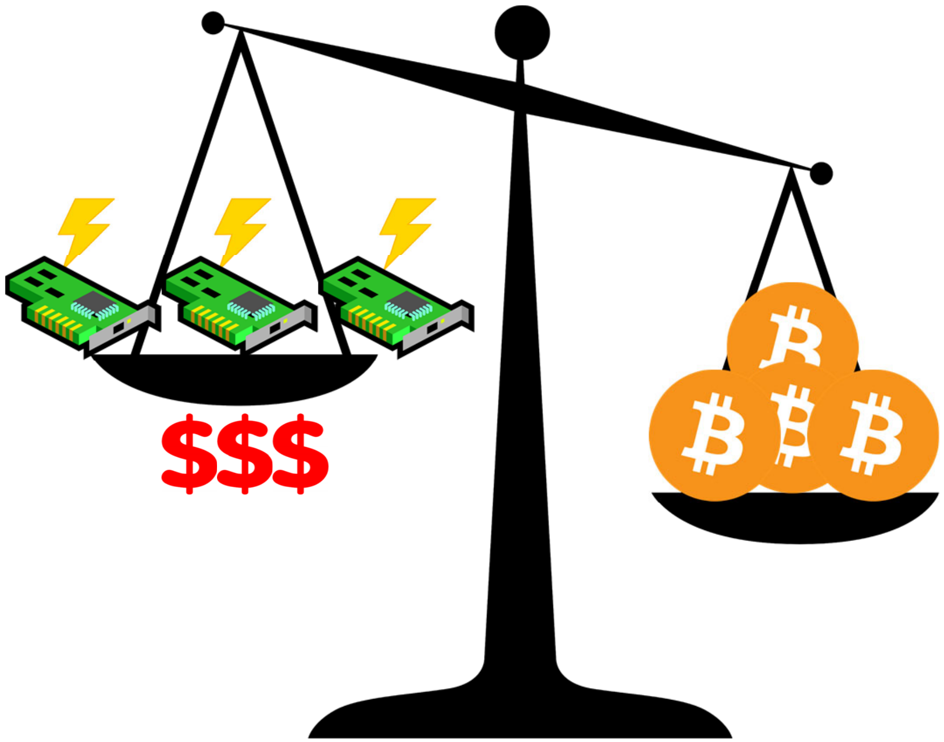
Byzantine

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

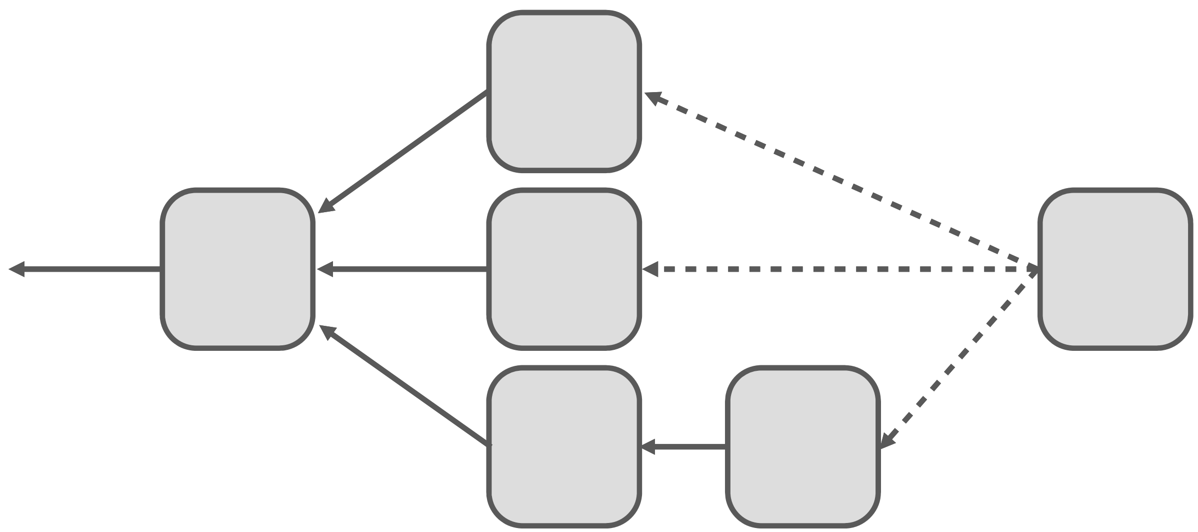
"The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes."

Mining is a Rational Business




A Blockchain Without Altruism?

Only One Type of Reference




Ene, mene,
eins, zwei, drei,
Bitcoins bringe
mir herbei.
Hash Hash.
@grauhut
BiBi BLOCKCHAIN

Thank You!

Questions & Comments?

www.disco.ethz.ch

Cryptography

- “Magic with Numbers”

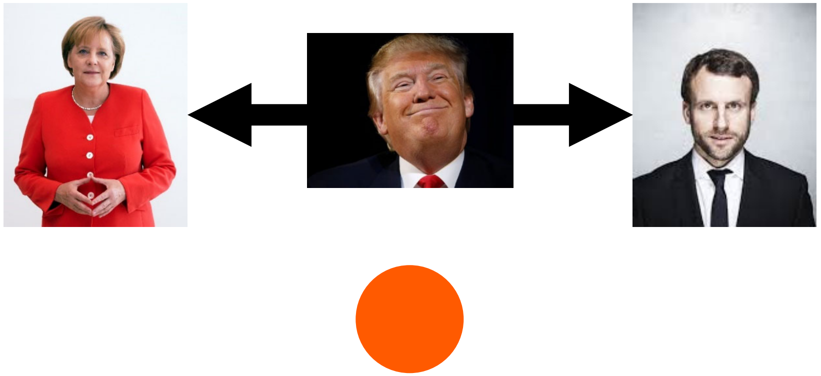
Encryption

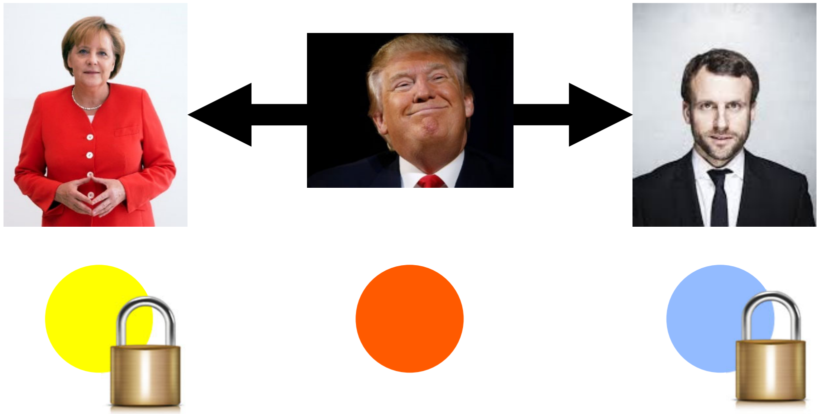
Digital Signatures

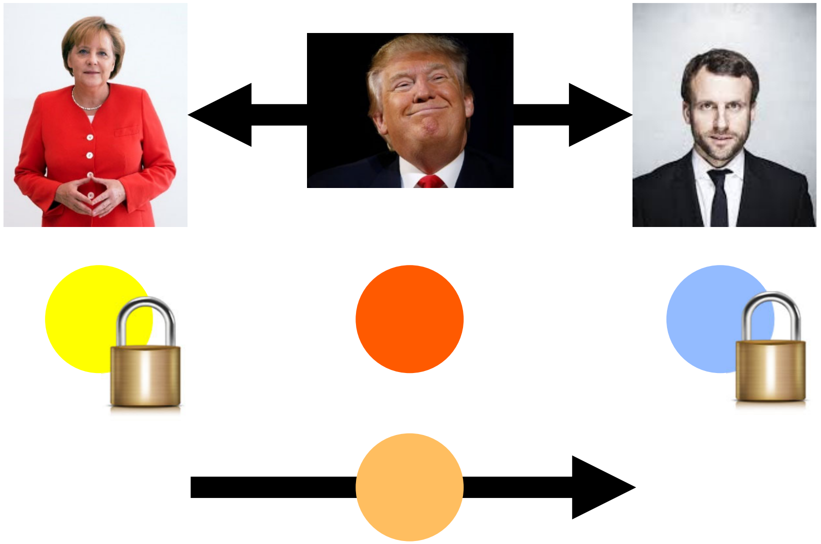
Generate a Secret

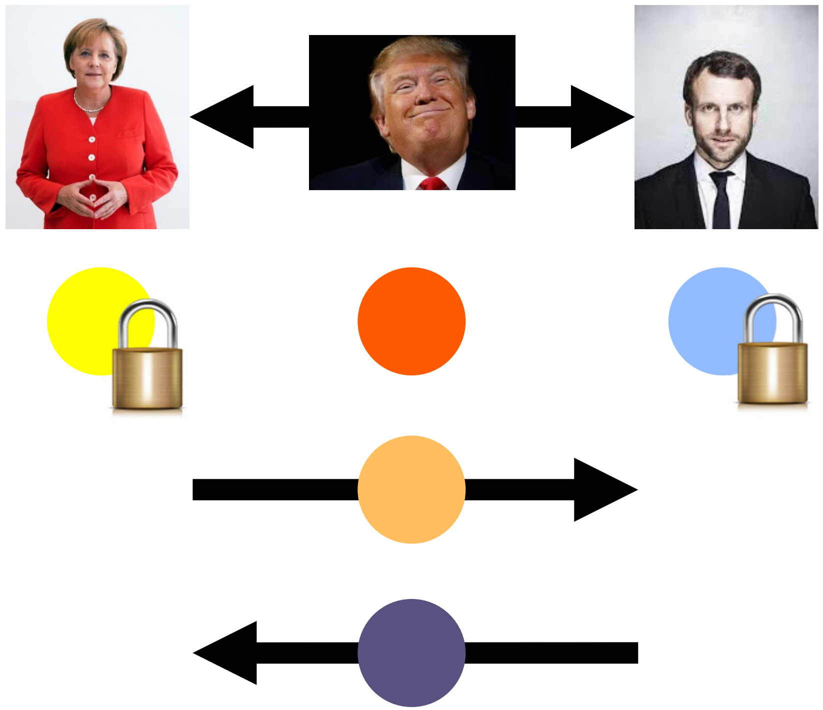
Generate a Secret

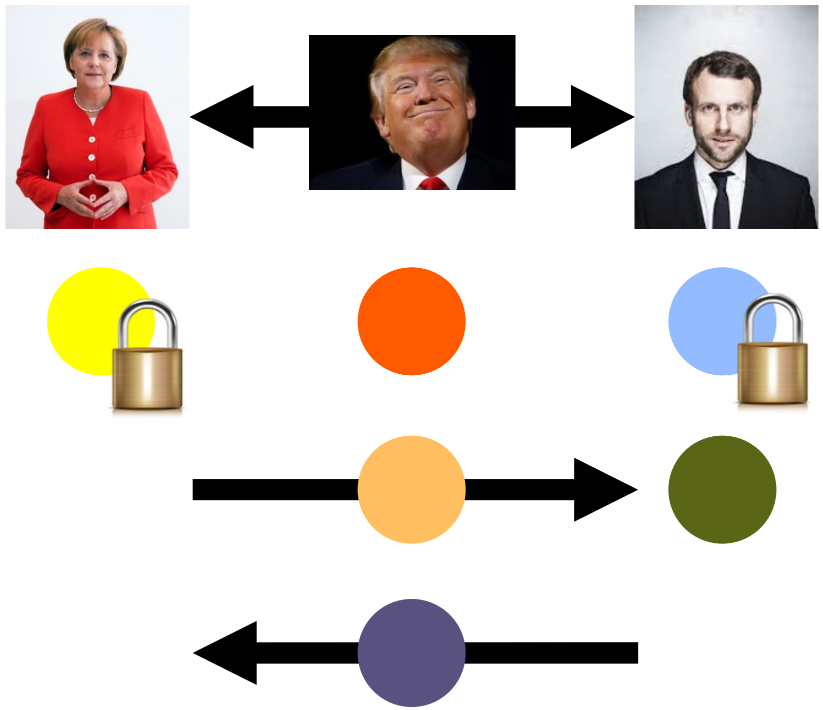
How?

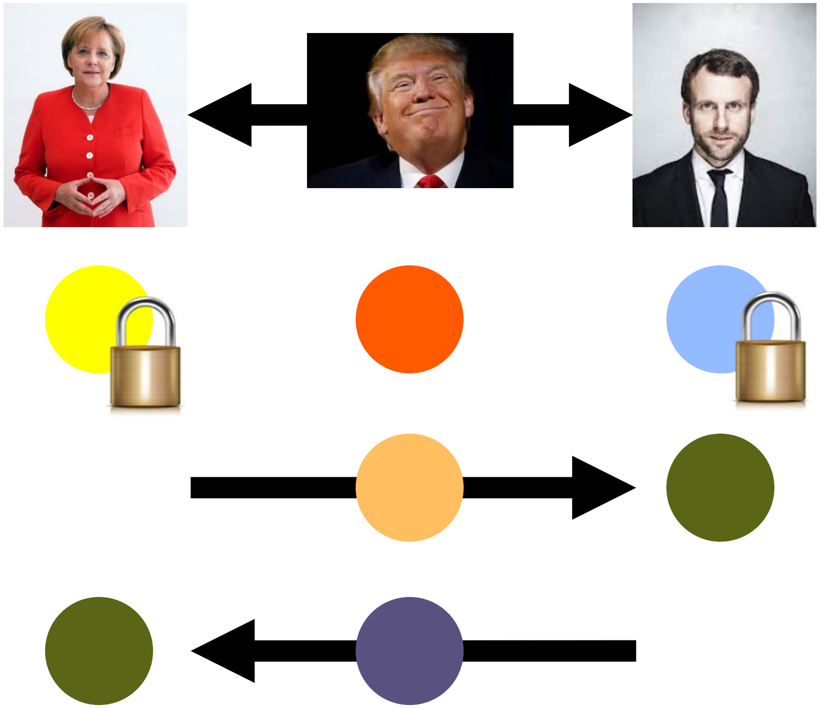






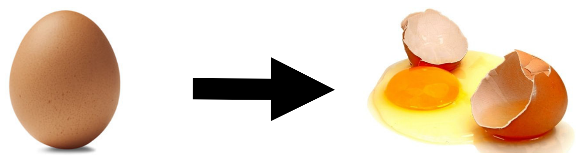






One Way Function

One Way Function



One Way Function

- $3 \cdot 5 \qquad 15$

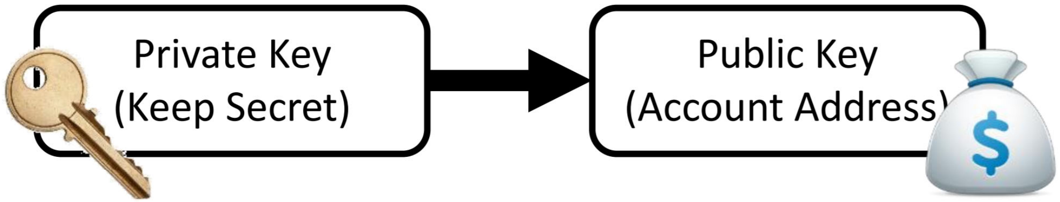
One Way Function

- $? \cdot ?$ 8616460799

One Way Function

- $? \cdot ? \rightarrow 2353 \ldots 91$

Your Bank Account




```
18E14A7B6A307F426A94F
8114701E7C8E774E7F9A4
7E2C2035DB29A20632172
```

```
16UwLL9Risc3QfPqB
UvKofHmBQ7wMtjvMx
```

«Ich wäre nicht überrascht, wenn Bitcoin verboten würde»

ETH-Informationstechnologe Roger Wattenhofer über den Energiebedarf der Kryptowährung und bessere Alternativen

Prof. Dr. Roger Wattenhofer vom Departement Informationstechnologie und Elektrotechnik der ETH Zürich