

Blockchain

Technische Grundlagen und Anwendungsmöglichkeiten



Roger Wattenhofer

Blockchain = Buchhaltung

Figure 9-3 Manual Journal Voucher.

Page <u>1</u> of <u>1</u>		MANUAL JOURNAL VOUCHER		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">PREPARED BY <u>WLR</u></td> <td style="width: 50%;">DATE <u>2/2/15</u></td> </tr> <tr> <td>APPROVED</td> <td>DATE</td> </tr> </table>		PREPARED BY <u>WLR</u>	DATE <u>2/2/15</u>	APPROVED	DATE
PREPARED BY <u>WLR</u>	DATE <u>2/2/15</u>								
APPROVED	DATE								
Batch <u>1101</u>	Batch Line <u>9</u>	Total Amount <u>11,200.20</u>							
Description <u>ACCRUED INTEREST INCOME</u>		Effective Date <u>1/31/15</u>	Type <u>A</u>						
Reference <u>JY3-JAN INTEREST</u>		Accounting Company <u>10-CORPORATE</u>							

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





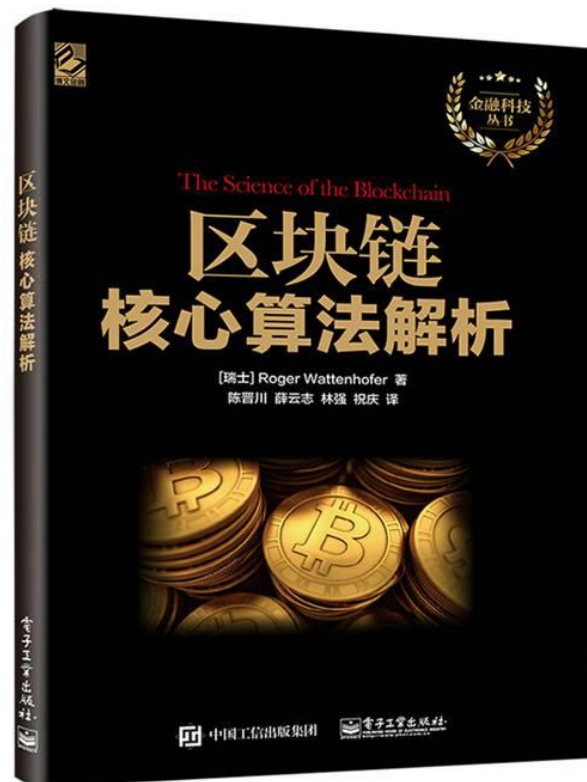
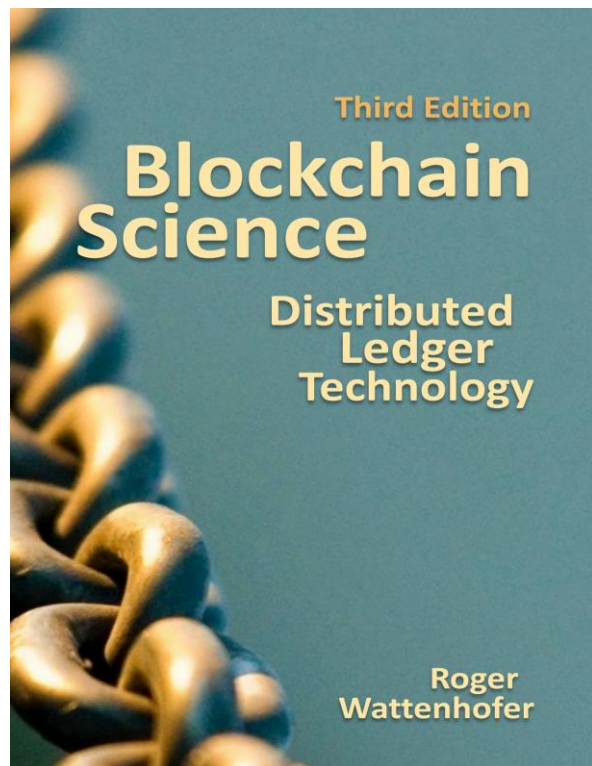
FinTech developers and managers understand that the *blockchain* has the potential to disrupt the financial world. The blockchain allows the participants of a distributed system to agree on a common view of the system, to track changes in the system, in a reliable way. In the distributed systems community, 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





Blockchain Basics

Transaction



Transaction



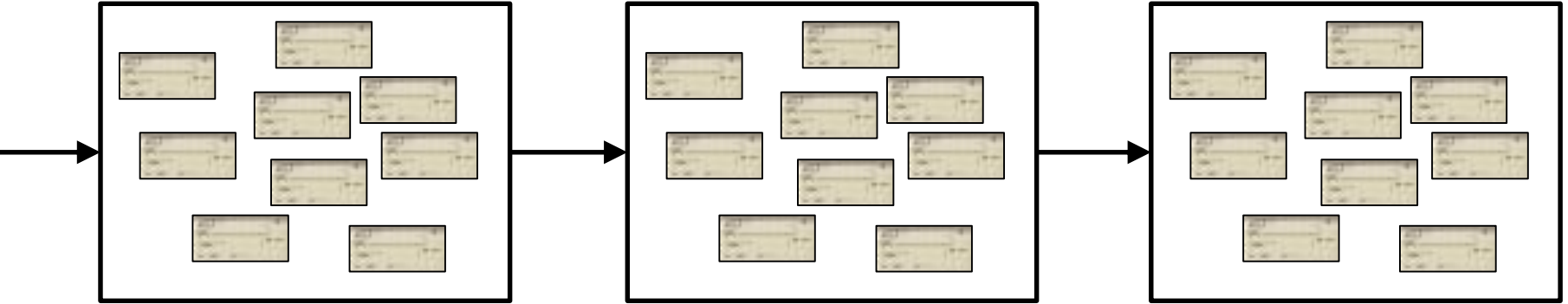
Transaction

JOHN DOE OR JANE DOE 123 MAIN STREET ANYTOWN, TN 01234 PHONE 555-1212		2670 87-823/641
_____		19
Pay to the Order of _____	\$ _____	
_____		Dollars  Security details on back.
<i>Bank of Yourtown</i> YOURTOWN, TN		6-73
For _____	_____	MP
⑆012345678⑆		⑈98765432⑈

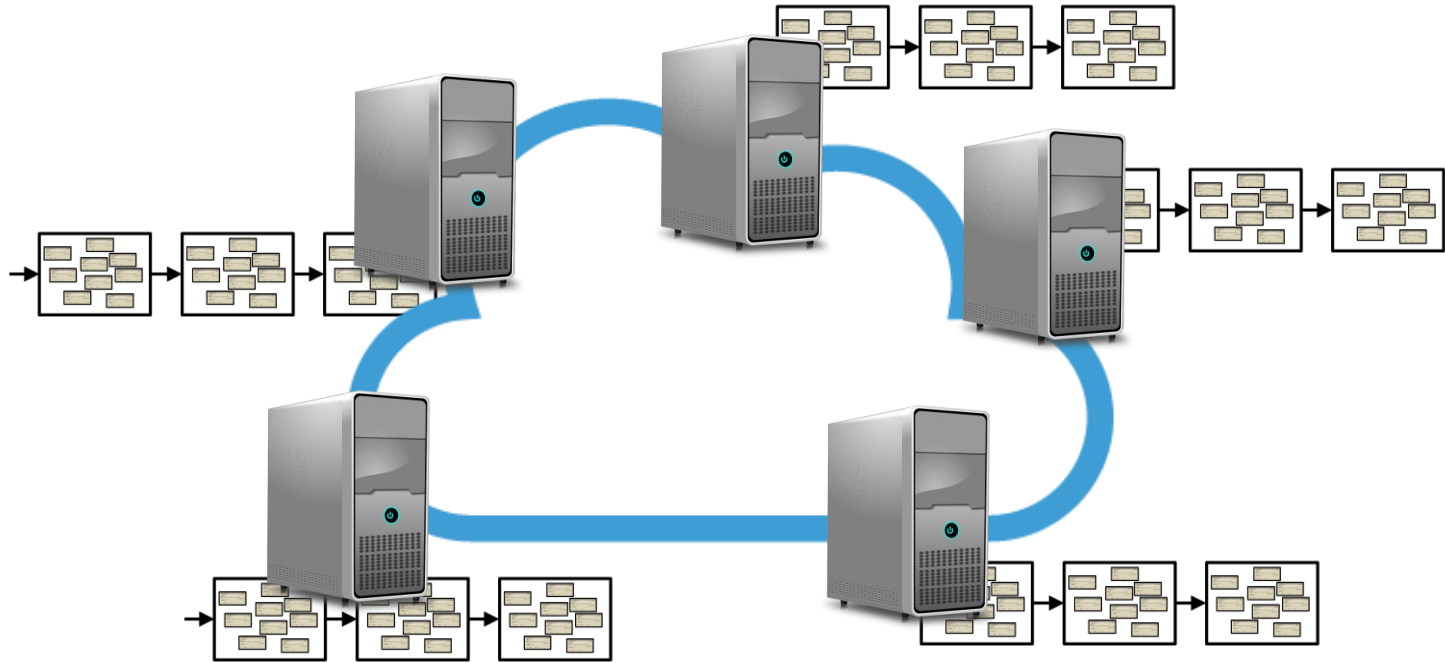
Block



Blockchain

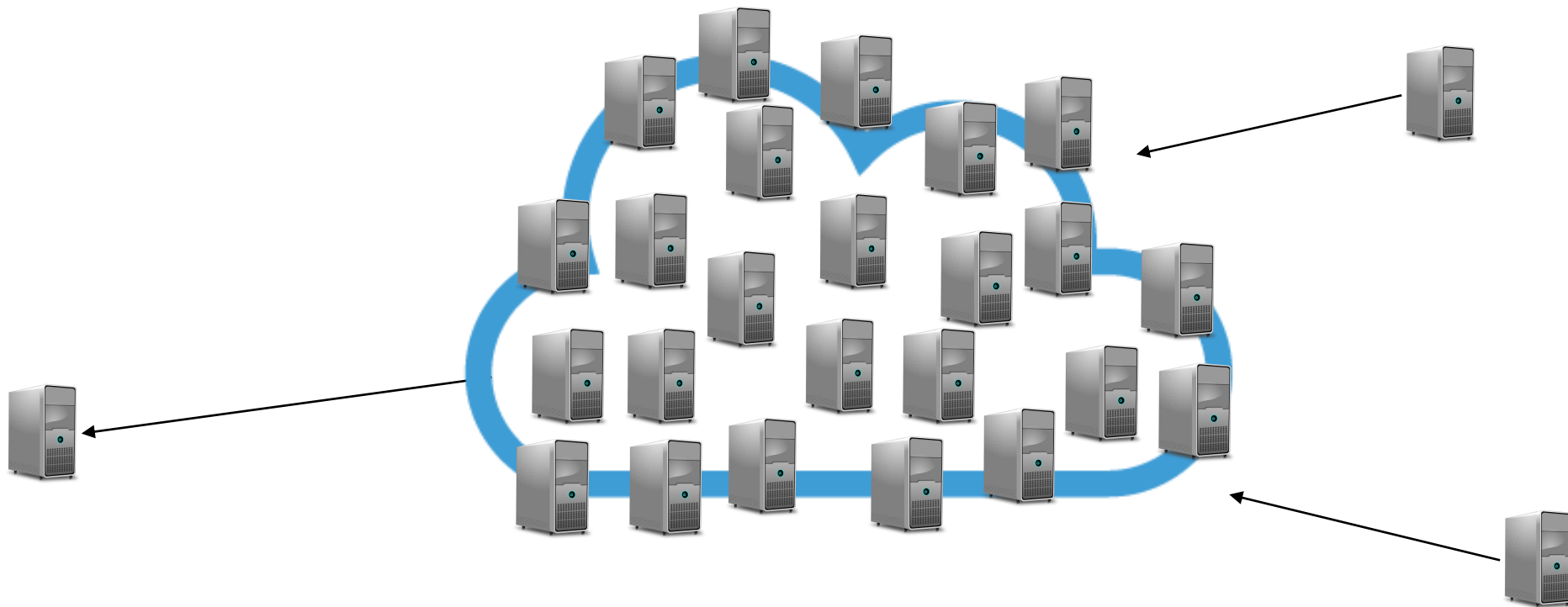


A Blockchain is Replicated

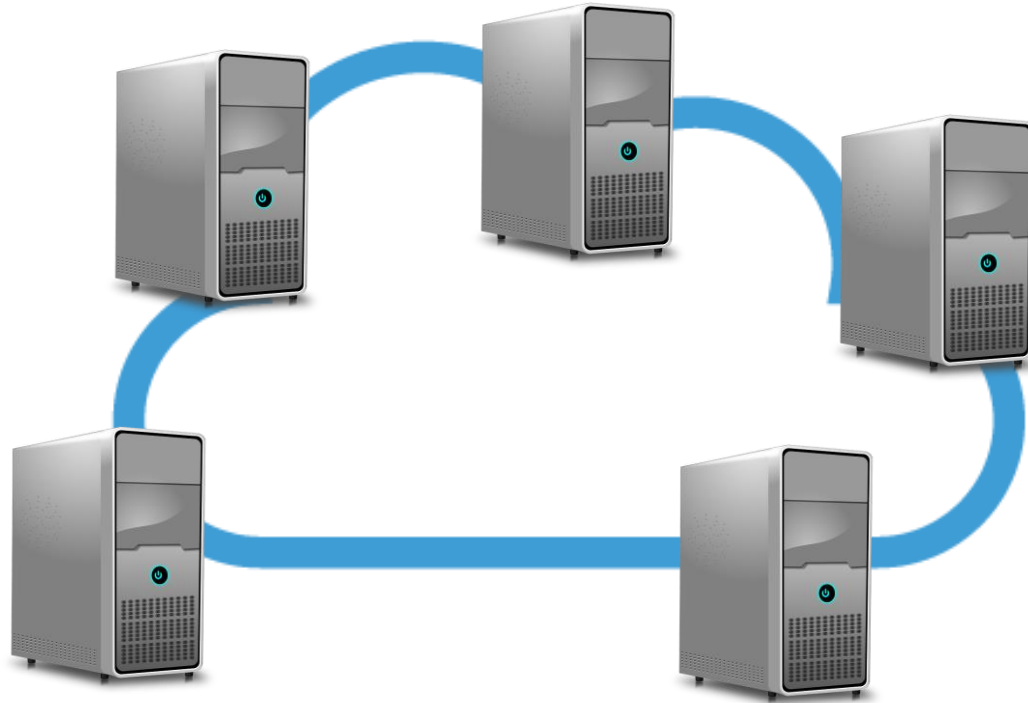


Blockchain Variants

Permissionless / Open



Permissioned / Closed



Do you need a Blockchain?

No

Multiple
Participants?

no

No Blockchain
(use database)

Multiple
Participants?

no

No Blockchain
(use database)

yes

Participants
Known?

yes

Permissioned
Blockchain



no

Permissionless
Blockchain

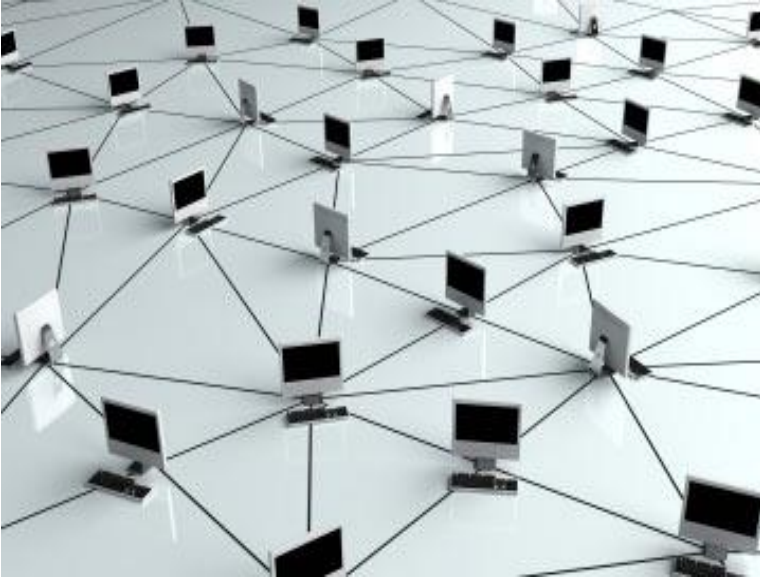


Rule of Thumb

Blockchains* may disrupt your business
if you use **signatures**.

*or blockchain-like tech

Blockchain Ingredients



Distributed Systems

&



Cryptography

Turing Awards

A network diagram showing multiple laptops connected by lines, representing a distributed system or network.

2008 Barbara Liskov

2010 Leslie Valiant*

2013 Leslie Lamport

A background image featuring a large blue padlock in the center, surrounded by a pattern of binary code (0s and 1s) and hexadecimal characters (A-F, 0-9) in a light blue color.

Rivest, Shamir & A. 2002

Micali & Goldwasser 2012

Hellman & Diffie 2015

Asymmetric Cryptography

“Magic with Numbers”

Encryption



Digital Signatures



Generating a Secret



Generating a Secret

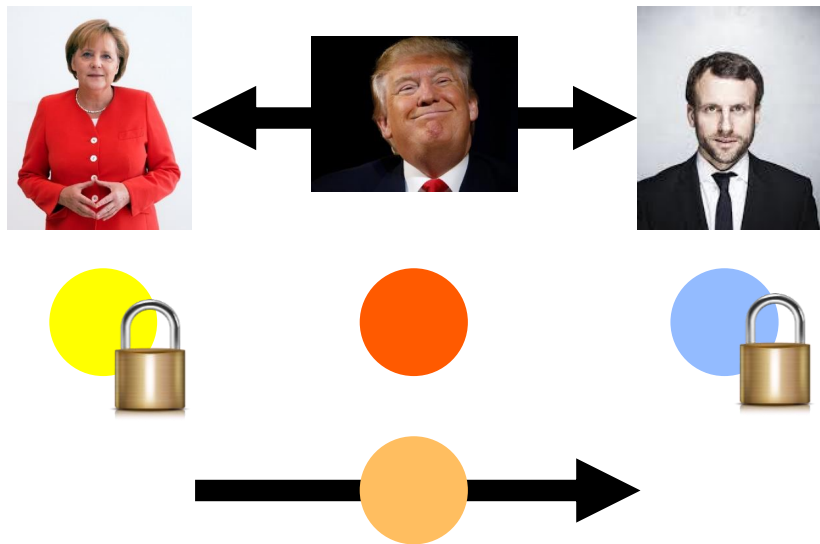


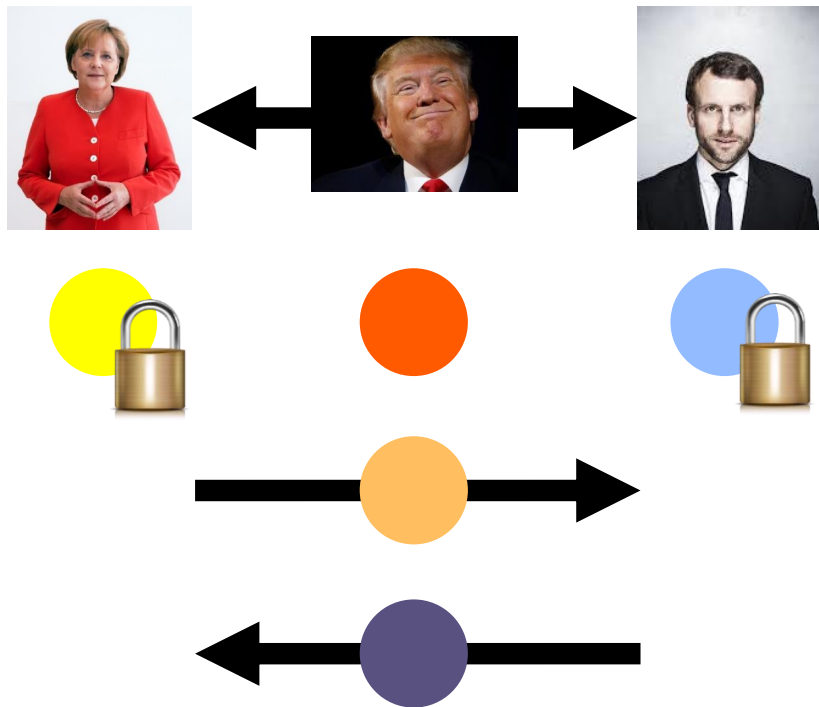
How?

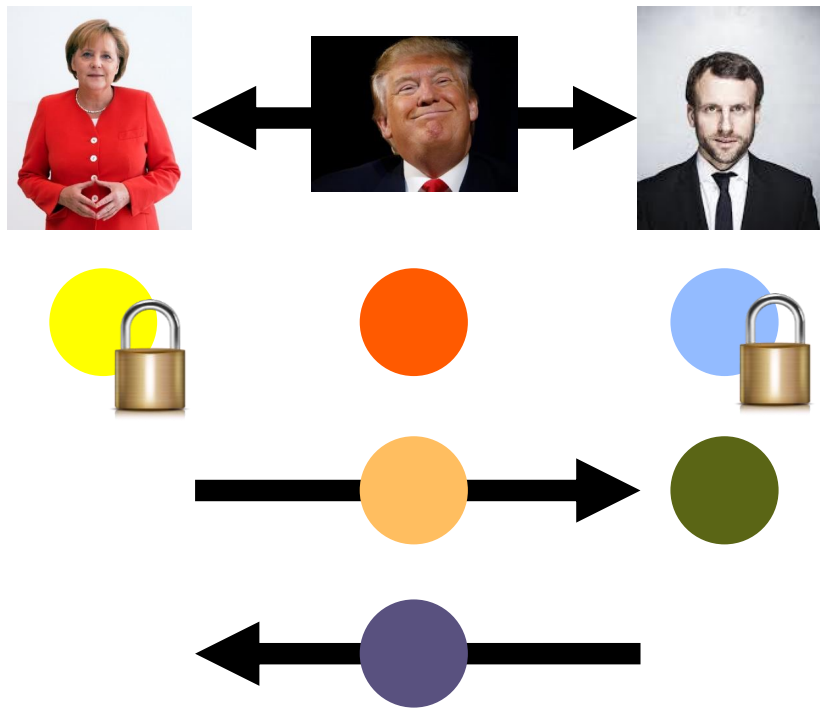


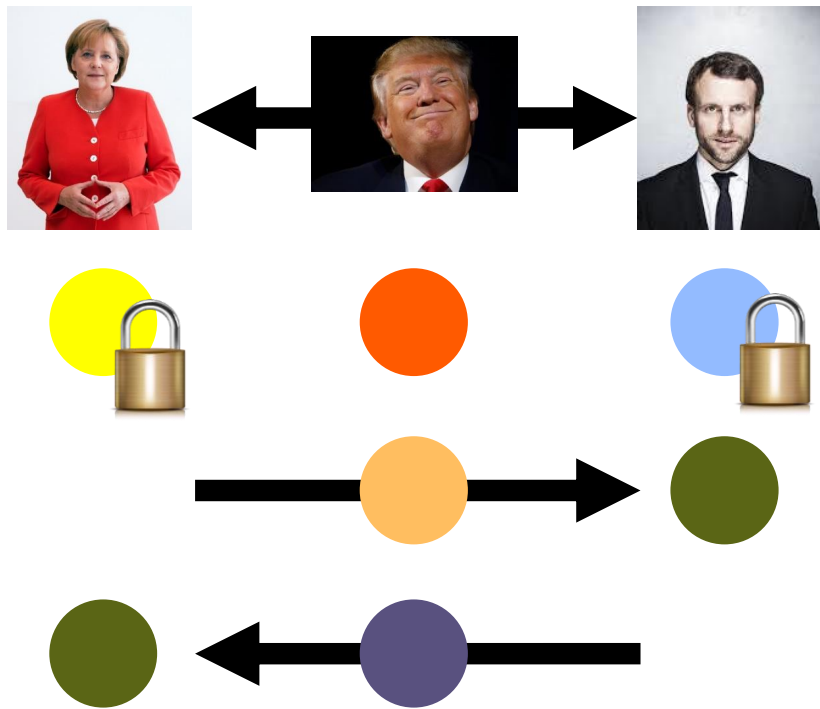








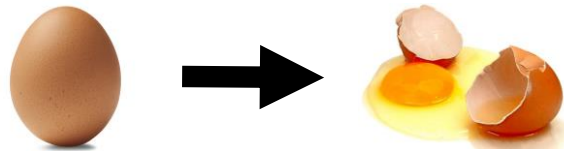




One Way Function



One Way Function



One Way Function

$$3 \cdot 5 \rightarrow 15$$

One Way Function

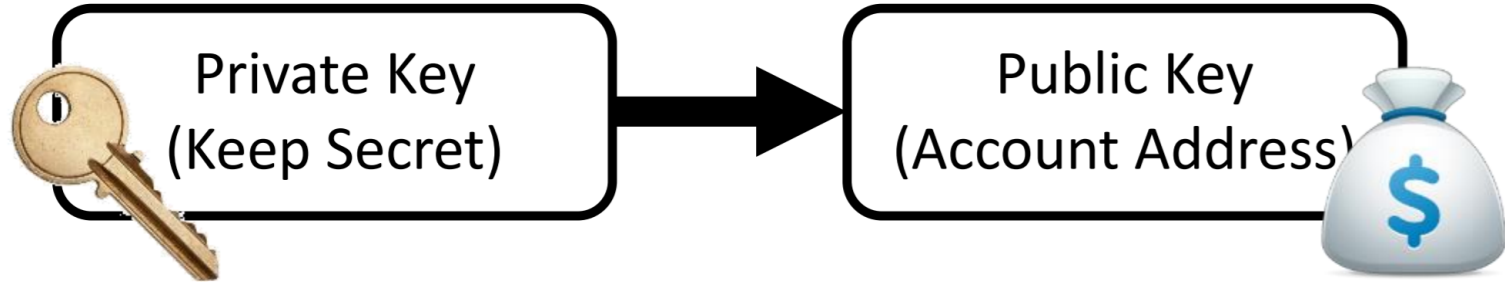
? · ? → 8616460799

One Way Function

$? \cdot ? \rightarrow 2353 \dots 91$

(620 digits)

Your Bank Account



18E14A7B6A307F426A94F
8114701E7C8E774E7F9A4
7E2C2035DB29A20632172

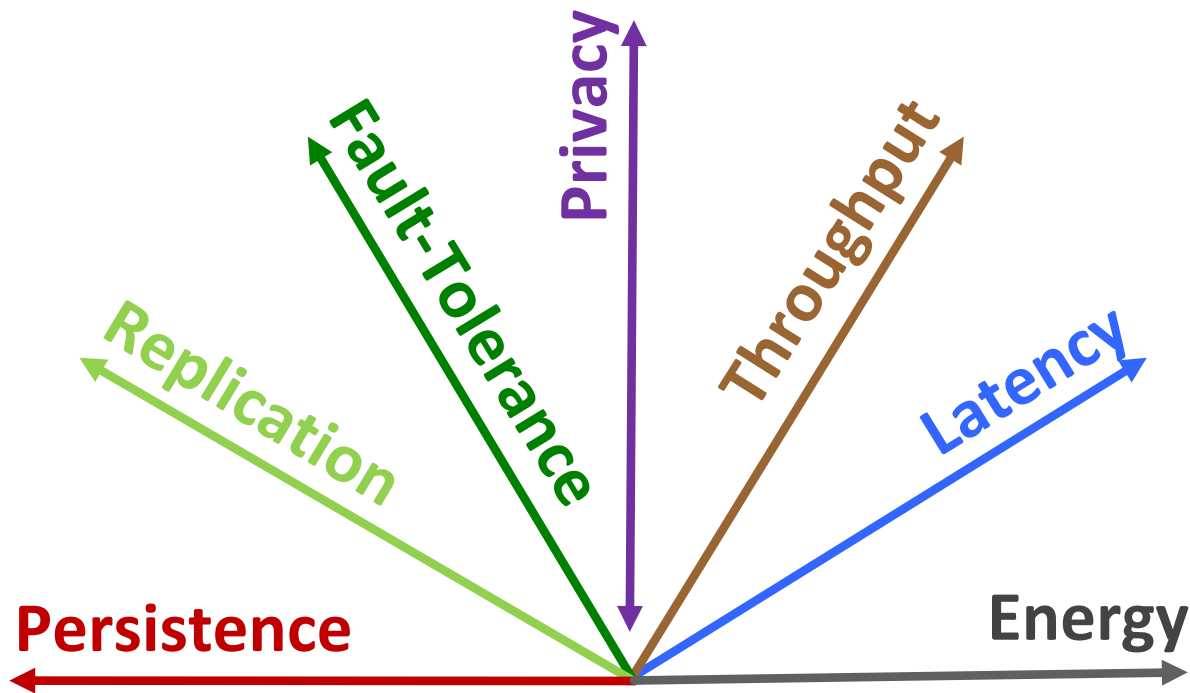
16UwLL9Risc3QfPqB
UvKofHmBQ7wMtjvMx

Hacker stahlen ETH- Doktoranden Bitcoin für 9 Millionen

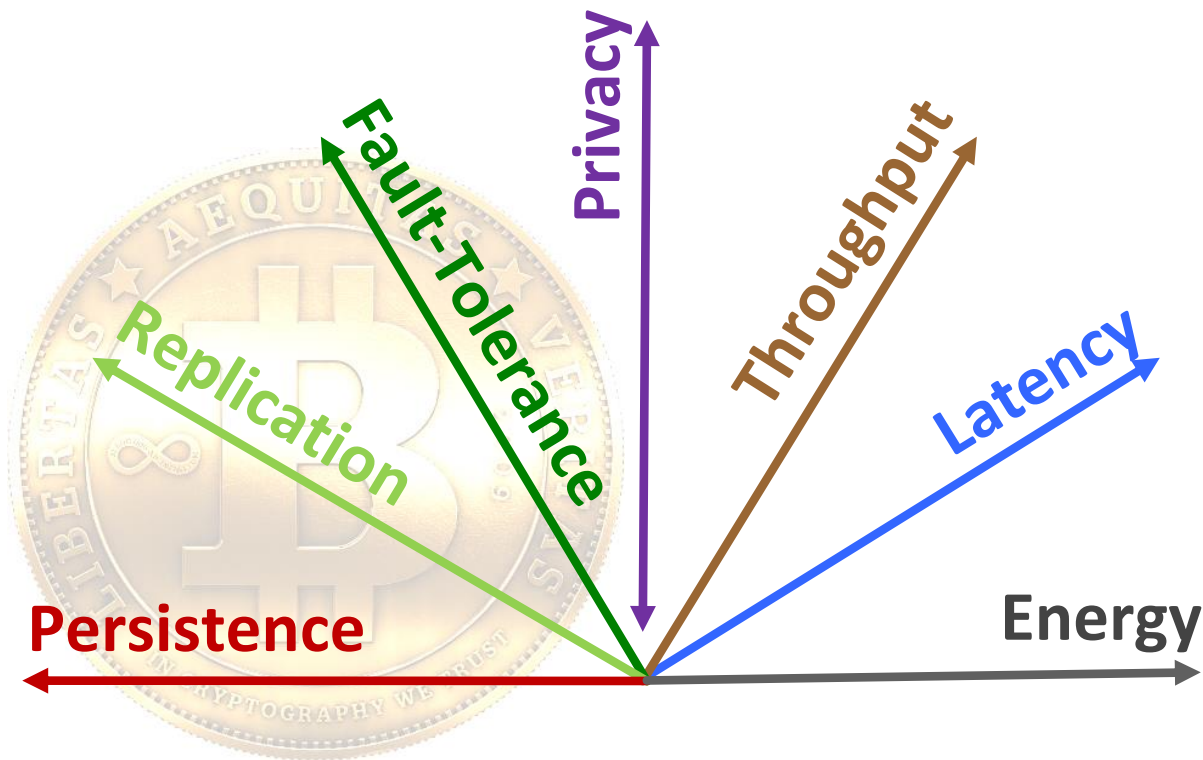
Von **Christian Bütikofer**
am 06.12.2013



The Seven Blockchain Dimensions



The Seven Blockchain Dimensions



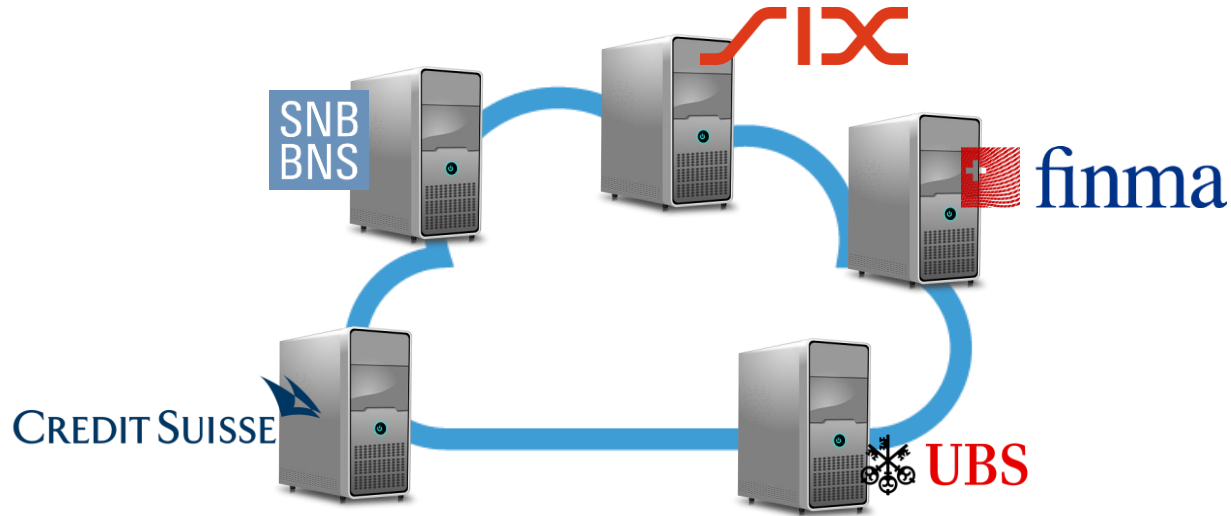
eMoney

Permissioned Blockchain

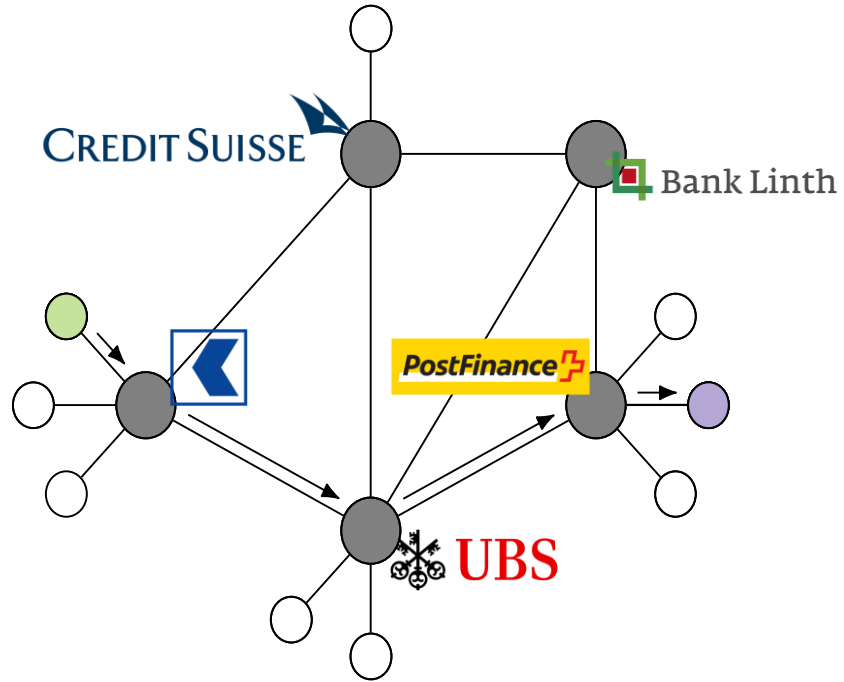
&

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



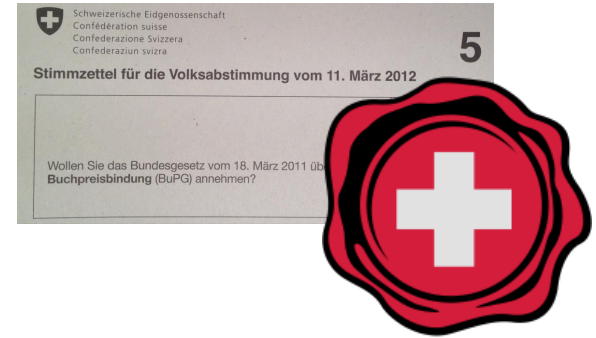
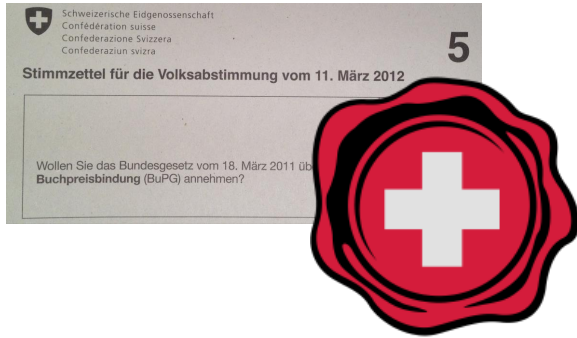
Democracy Beyond Yes or No

	Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	5
Stimmzettel für die Volksabstimmung vom 11. März 2025		
Wie viel sollen die SRG-Gebühren pro Jahr kosten?		Antwort
		42.-

Anonymity?



Swapping Voting Card



Open Problem: Mass Vote Buying



REPUBLIK

The Tricky Business of Democracy

...stigious electronic voting project, Swiss Post is
...logy provided by the Spanish company ScytL.
... shows that the e-voting market
...aled elections and
...ting.

A cartoon illustration of a young girl with blonde hair in a high ponytail with a red bow, wearing a green t-shirt and white socks with red shoes. She is standing on a green field, holding a broomstick, and looking towards the right. The background is a blue sky with white clouds and sparkling light effects. A speech bubble is on the right, and a circular logo is in the bottom left corner.

Ene, mene,
eins, zwei, drei,
Bitcoins bringe
mir herbei.
Hash Hash.

@grauhut



Thank You!

Questions & Comments?

