

# Blockchain and Hyperledger Fabric

Dominic Duggan  
Stevens Institute of Technology

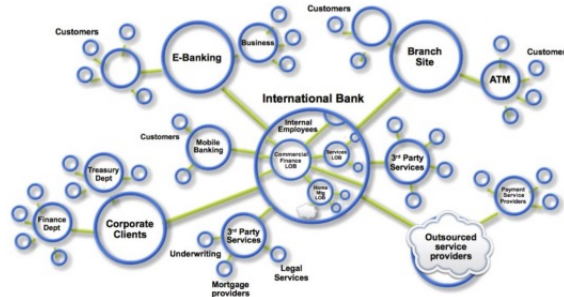
1

## **INTRODUCTION TO BLOCKCHAIN**

2

# Connected Markets

- Networks connect participants
  - Customers, suppliers, banks, consumers
- Markets organize trades
  - Public and private markets
- Value comes from assets
  - Physical assets (house, car ...)
  - Virtual assets (bond, patent ...)
  - Services are also assets
- Transactions exchange assets



3

3

# Ledger

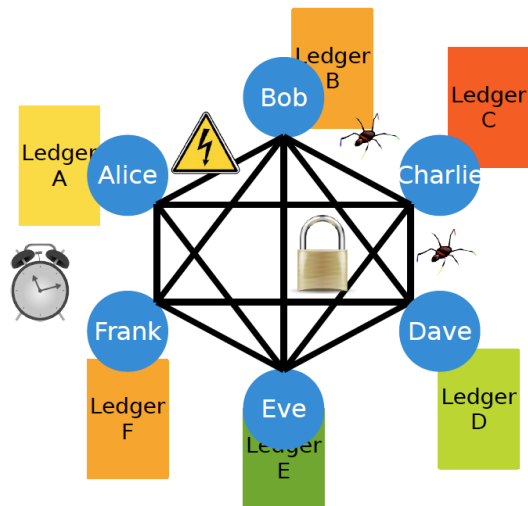
Datum		Entnahme von Abhebungen	Einzahlungen, Einzuführungen	Bestand vor Schuld	Bestand nach Einzahlung
1942					
1.1.	an 1.000,-	an 1.000,-		1.000,00	
2.1.	an 2.000,-	an 2.000,-		3.000,00	
3.1.	an 1.500,-	an 1.500,-		1.500,00	
4.1.	an 1.000,-	an 1.000,-		500,00	
5.1.	an 500,-	an 500,-		0,00	
6.1.	an 1.000,-	an 1.000,-		1.000,00	
7.1.	an 1.500,-	an 1.500,-		2.500,00	
8.1.	an 2.000,-	an 2.000,-		4.500,00	
9.1.	an 1.500,-	an 1.500,-		3.000,00	
10.1.	an 1.000,-	an 1.000,-		2.000,00	
11.1.	an 500,-	an 500,-		1.500,00	
12.1.	an 1.000,-	an 1.000,-		500,00	
13.1.	an 1.500,-	an 1.500,-		0,00	
14.1.	an 2.000,-	an 2.000,-		2.000,00	
15.1.	an 1.500,-	an 1.500,-		500,00	
16.1.	an 1.000,-	an 1.000,-		0,00	
17.1.	an 500,-	an 500,-		500,00	
18.1.	an 1.000,-	an 1.000,-		1.500,00	
19.1.	an 1.500,-	an 1.500,-		3.000,00	
20.1.	an 2.000,-	an 2.000,-		5.000,00	
21.1.	an 1.500,-	an 1.500,-		3.500,00	
22.1.	an 1.000,-	an 1.000,-		2.500,00	
23.1.	an 500,-	an 500,-		2.000,00	
24.1.	an 1.000,-	an 1.000,-		1.000,00	
25.1.	an 1.500,-	an 1.500,-		0,00	
26.1.	an 2.000,-	an 2.000,-		2.000,00	
27.1.	an 1.500,-	an 1.500,-		500,00	
28.1.	an 1.000,-	an 1.000,-		0,00	
29.1.	an 500,-	an 500,-		500,00	
30.1.	an 1.000,-	an 1.000,-		1.500,00	
31.1.	an 1.500,-	an 1.500,-		3.000,00	
1.2.	an 2.000,-	an 2.000,-		5.000,00	
2.2.	an 1.500,-	an 1.500,-		3.500,00	
3.2.	an 1.000,-	an 1.000,-		2.500,00	
4.2.	an 500,-	an 500,-		2.000,00	
5.2.	an 1.000,-	an 1.000,-		1.000,00	
6.2.	an 1.500,-	an 1.500,-		0,00	
7.2.	an 2.000,-	an 2.000,-		2.000,00	
8.2.	an 1.500,-	an 1.500,-		500,00	
9.2.	an 1.000,-	an 1.000,-		0,00	
10.2.	an 500,-	an 500,-		500,00	
11.2.	an 1.000,-	an 1.000,-		1.500,00	
12.2.	an 1.500,-	an 1.500,-		3.000,00	
13.2.	an 2.000,-	an 2.000,-		5.000,00	
14.2.	an 1.500,-	an 1.500,-		3.500,00	
15.2.	an 1.000,-	an 1.000,-		2.500,00	
16.2.	an 500,-	an 500,-		2.000,00	
17.2.	an 1.000,-	an 1.000,-		1.000,00	
18.2.	an 1.500,-	an 1.500,-		0,00	
19.2.	an 2.000,-	an 2.000,-		2.000,00	
20.2.	an 1.500,-	an 1.500,-		500,00	
21.2.	an 1.000,-	an 1.000,-		0,00	
22.2.	an 500,-	an 500,-		500,00	
23.2.	an 1.000,-	an 1.000,-		1.500,00	
24.2.	an 1.500,-	an 1.500,-		3.000,00	
25.2.	an 2.000,-	an 2.000,-		5.000,00	
26.2.	an 1.500,-	an 1.500,-		3.500,00	
27.2.	an 1.000,-	an 1.000,-		2.500,00	
28.2.	an 500,-	an 500,-		2.000,00	
29.2.	an 1.000,-	an 1.000,-		1.000,00	
30.2.	an 1.500,-	an 1.500,-		0,00	
31.2.	an 2.000,-	an 2.000,-		2.000,00	

- Ledger records all business activity as transactions
  - Databases
- Every market and network defines a ledger
- Ledger records asset transfers between participants
- Problem: (Too) many ledgers
  - Every market has its ledger
  - Every organization has its own ledger

4

4

## Ledger

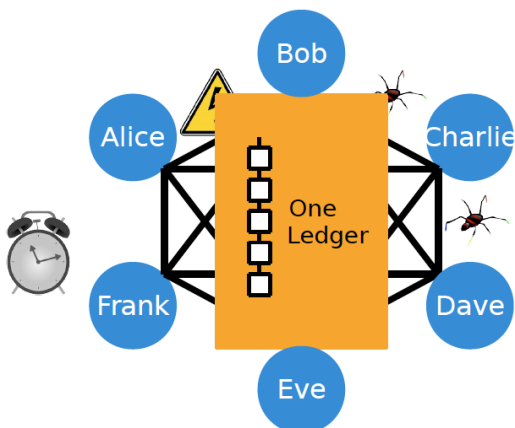


- Every party keeps its own ledger and state
- Problems, incidents, faults
- Diverging ledgers

5

5

## Blockchain: One Ledger To Rule Them All



- One common trusted ledger
  - Today often implemented by a centralized intermediary
- Blockchain creates one single ledger
- Replicated and produced collaboratively
- Trust in ledger from
  - Cryptographic protection, or
  - Distributed validation

6

6

## Blockchain: Definition

- "Blockchains are tamper evident and tamper resistant digital **ledgers** implemented in a **distributed** fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record **transactions** in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published." National Institute of Standards and Technology Interagency or Internal Report (NISTIR) 8202: Blockchain Technology Overview

7

## Simplifies Complex Transactions



Logistics

Real-time visibility  
Improved efficiency  
Transparency & verifiability  
Reduced cost



Property records

Digital but unforgeable  
Fewer disputes  
Transparency & verifiability  
Lower transfer fees



Capital markets

Faster settlement times  
Increased credit availability  
Transparency & verifiability  
No reconciliation cost

8

8

## Why Blockchain?

- Cryptography: key technology in the financial world for decades
  - Payment networks, ATM security, smart cards, online banking ...
- Trust model of (financial) business has not changed
  - Trusted intermediary needed for exchange
  - Cryptography mostly secures point-to-point interactions

9

9

## Why Blockchain?

- Bitcoin started in 2009
  - Embodies only cryptography of 1990s and earlier
  - First prominent use of cryptography for a new trust model (= trust no entity)
- The promise of Blockchain
  - Reduce trust and replace it by technology
  - Exploit “advanced” cryptographic techniques

10

10

## Why Blockchain?

- Immutable global record
  - Distributed ledger of transactions
- Consensus
  - Agreement on order
- Possibility of failures
  - Crash
  - Byzantine (malicious?)
- Smart contracts
  - Application protocols

11

## Permissioned vs Permissionless

- Permissionless
  - Open participation
  - Utility-based compute model
  - Typically Proof of Work (PoW)
  - Ex: Bitcoin, Ethereum
- Permissioned
  - Restricted participation
  - Consortium-based compute model
  - Paxos, Byzantine Fault Tolerance (BFT)
  - Ex: Hyperledger Fabric

12

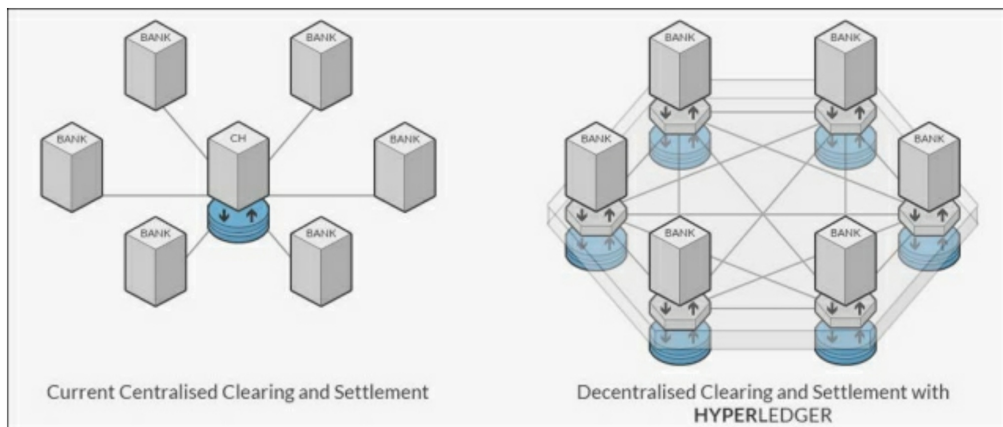
## Cost of PoW

Platform	Global (kW)		Per transaction (kW h/tx)	
<b>Eth. 2.0</b> <sup>☆</sup>	14.6 –	445.3	0.000 26 –	0.008 03
<b>Algorand</b>	6.2 –	189.3	0.000 17 –	0.005 34
<b>Cardano</b>	48.8 –	1491.7	0.037 16 –	1.135 62
<b>Polkadot</b>	1.6 –	49.9	0.003 78 –	0.115 56
<b>Tezos</b>	2.2 –	67.1	0.000 36 –	0.010 96
<b>Hedera</b>	3.5 –	6.9	0.000 02 –	0.000 04
<b>Bitcoin</b>	3 373 287.7 – 34 817 351.6		360.393 00 – 3691.407 00	
<b>VisaNet</b>	22 387.1		0.003 58	

<sup>☆</sup> Ethereum Mainnet measurements used as approximation

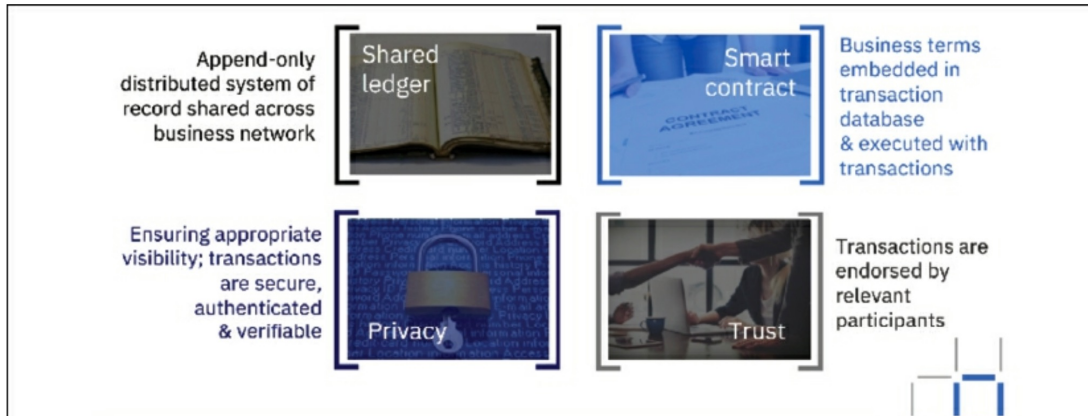
13

## Blockchain and Organization Infrastructure



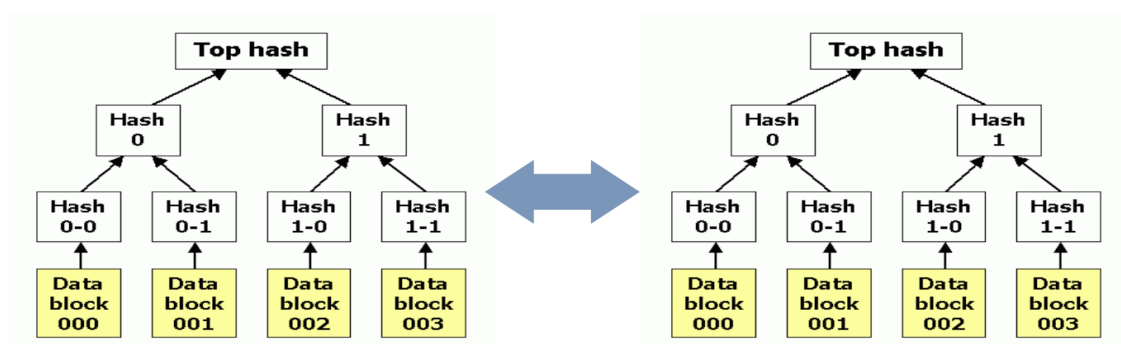
14

# Blockchain Components



15

# Integrity via Cryptography



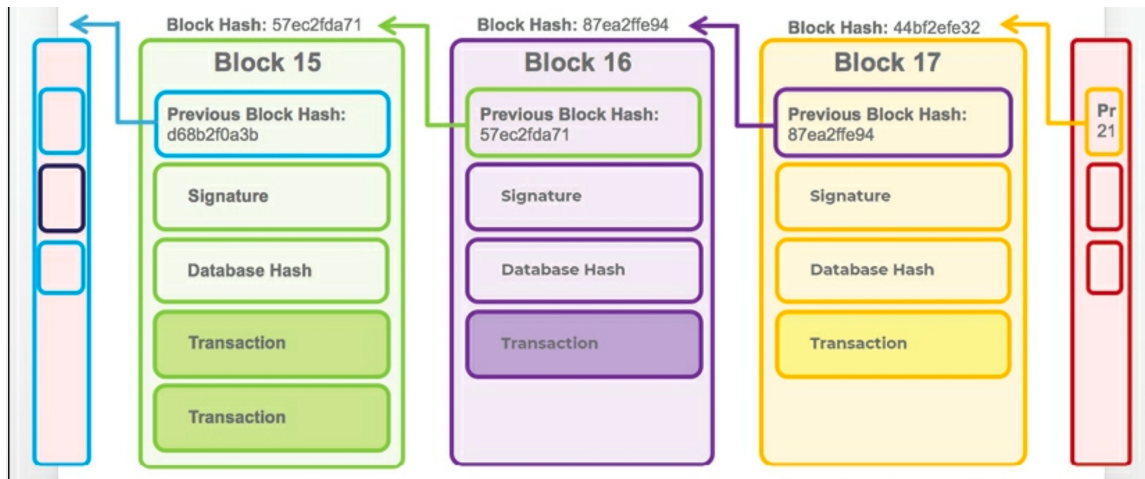
Merkle Hash Trees

16

16



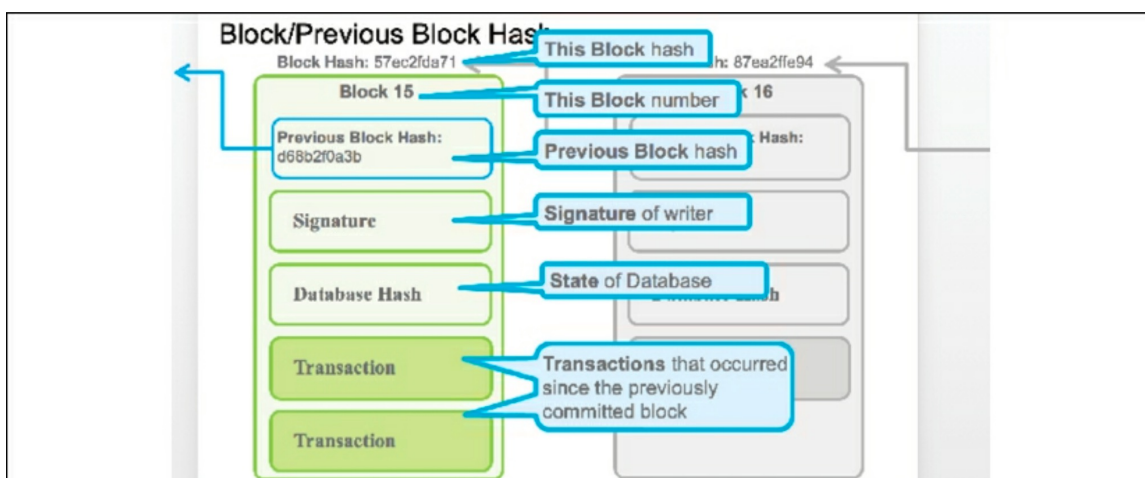
# Blockchain



17

17

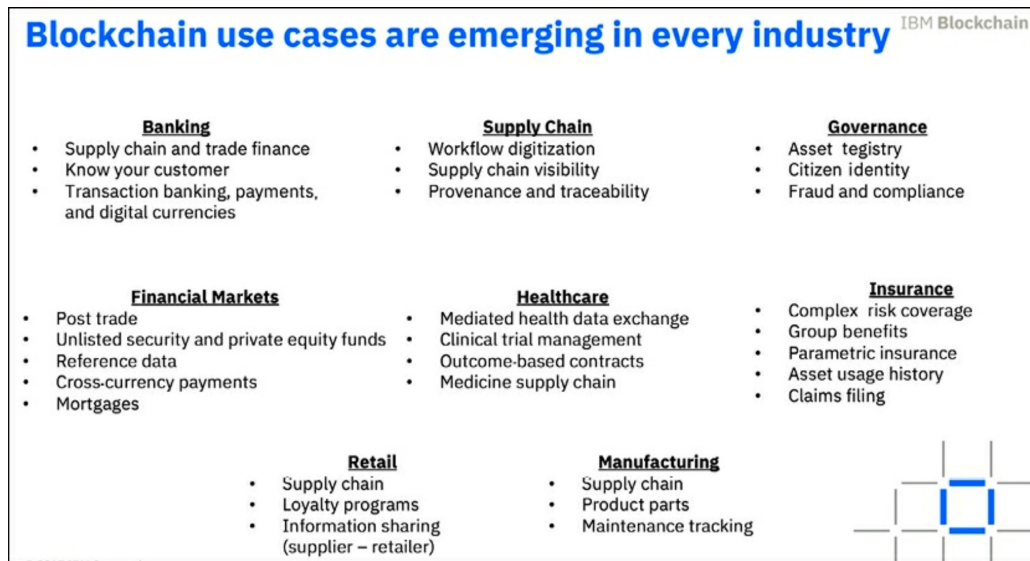
## Block Internals



18

18

# Block Internals



19

19

## Application Good Fit

- Trade, trust, ownership
  - Ownership, trade: Flow of assets
  - Trust: provided by blockchain
- Transactional
  - Multi-party
  - Distinguish blockchain from database
- Non-monopolistic business networks
  - No centralized control
- *From enterprise problem to industry problem*

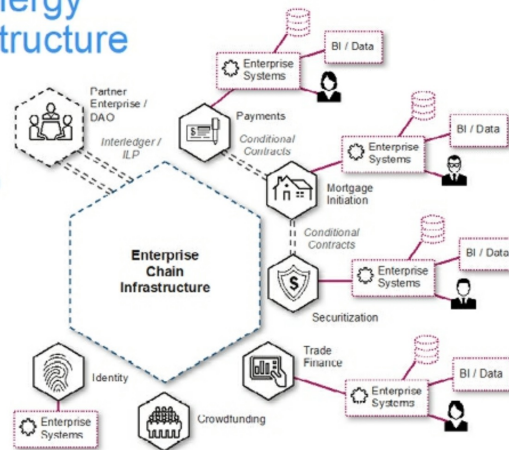
20

# Enterprise Blockchain Infrastructure

## Vision – 'Interprise Synergy' Enterprise chain infrastructure

### Design that enables new business models

- Invisible enterprise chain infrastructure will provide foundation
- Use of connectors, APIs to enable incumbent systems chain aware
- Conditional contracts between chains – 'Interprise Synergy'
- New business such as P2P lending, crowdfunding) solely on blockchain



©2017 IBM Corporation

Page 11