Blockchain and Hyperledger Fabric

Dominic Duggan
Stevens Institute of Technology

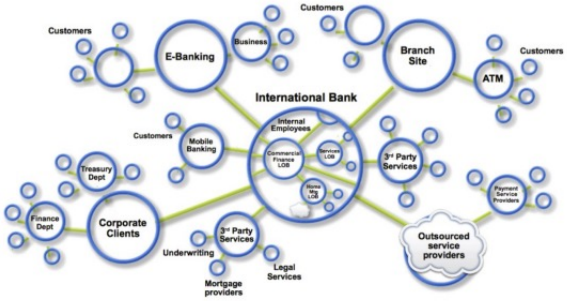
1

INTRODUCTION TO BLOCKCHAIN

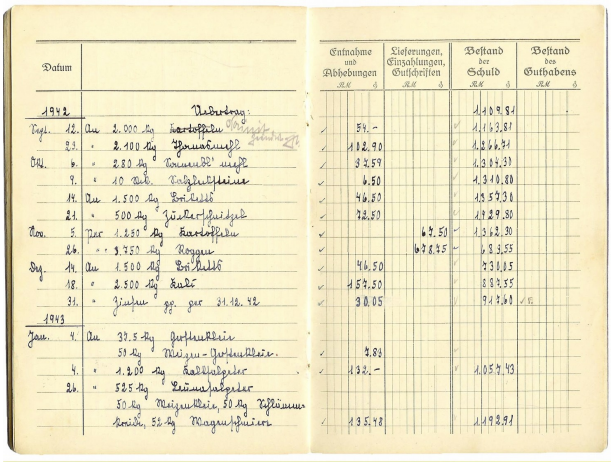
2

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

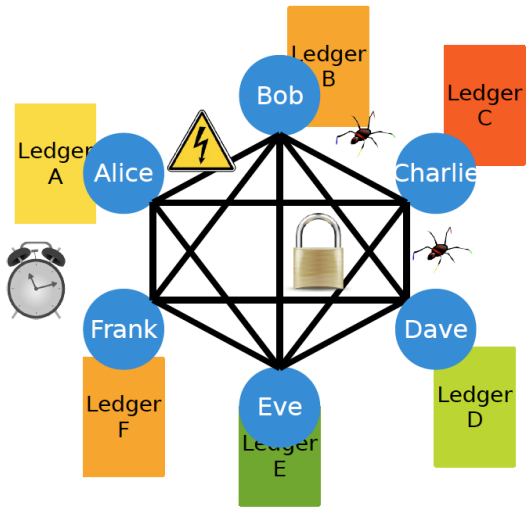


Ledger



- 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

Ledger

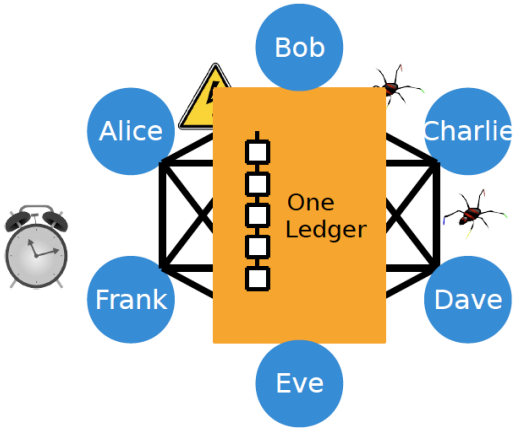


- Every party keeps its own ledger and state
- Problems, incidents, faults
- Diverging ledgers

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

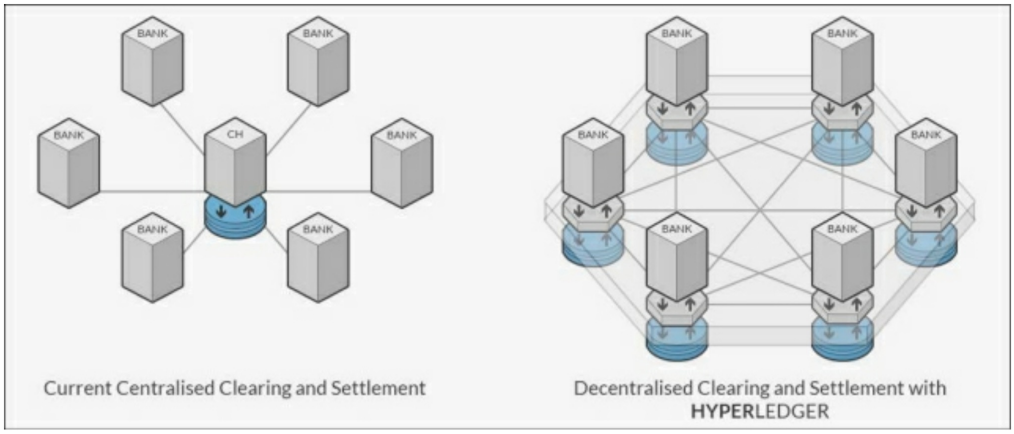
Cost of PoW

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

☆ Ethereum Mainnet measurements used as approximation

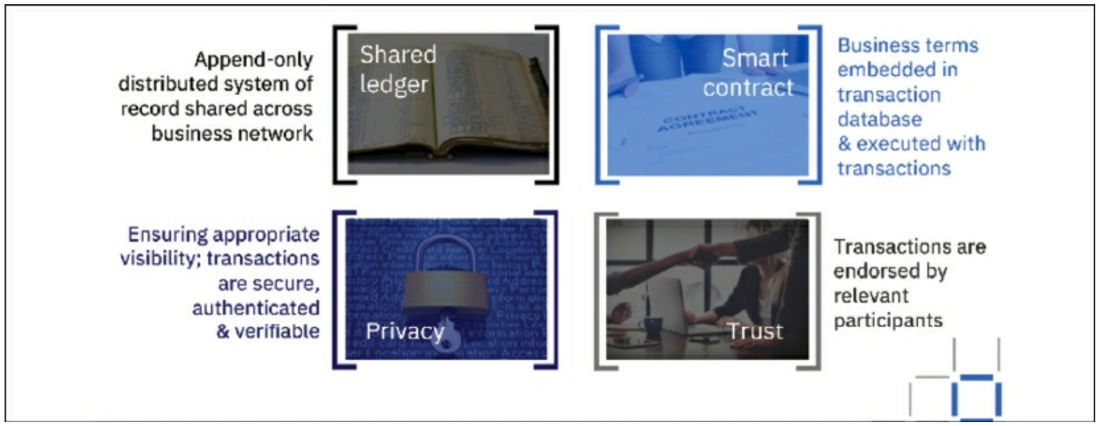
13

Blockchain and Organization Infrastructure



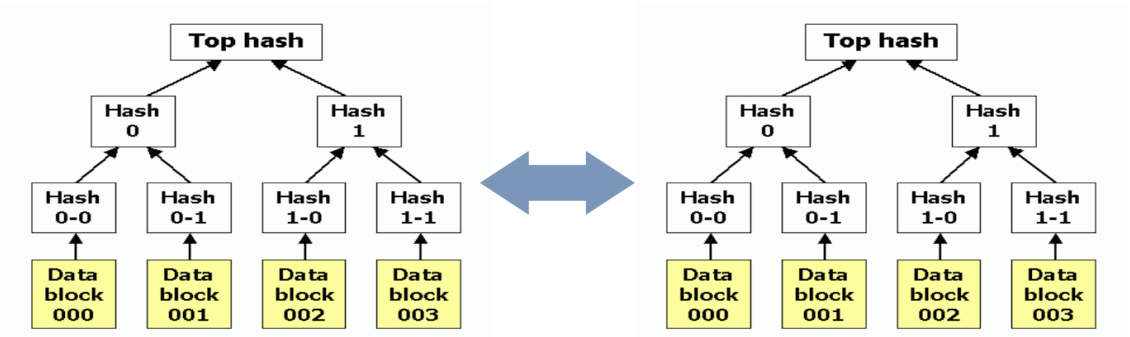
14

Blockchain Components



15

Integrity via Cryptography

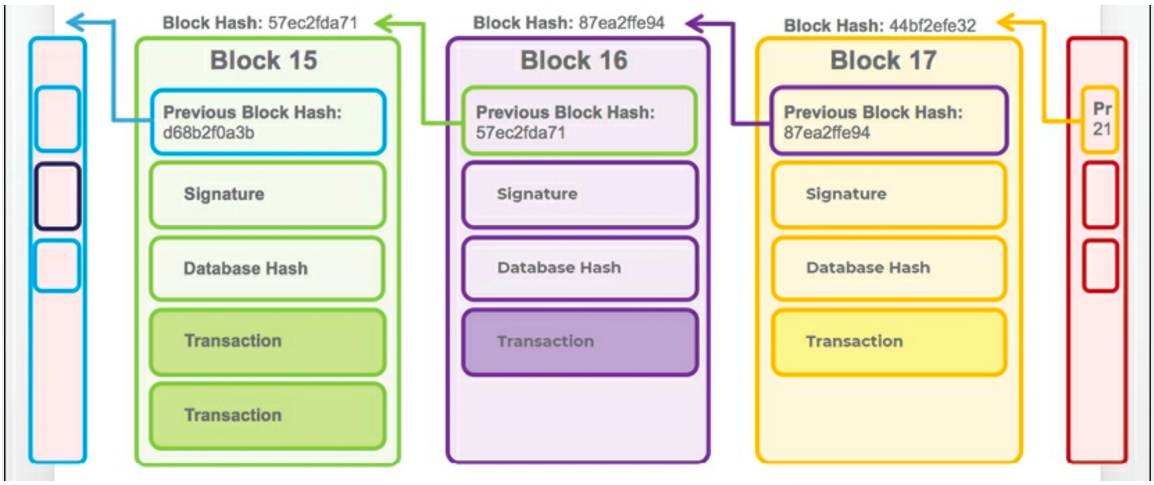


Merkle Hash Trees

16

16

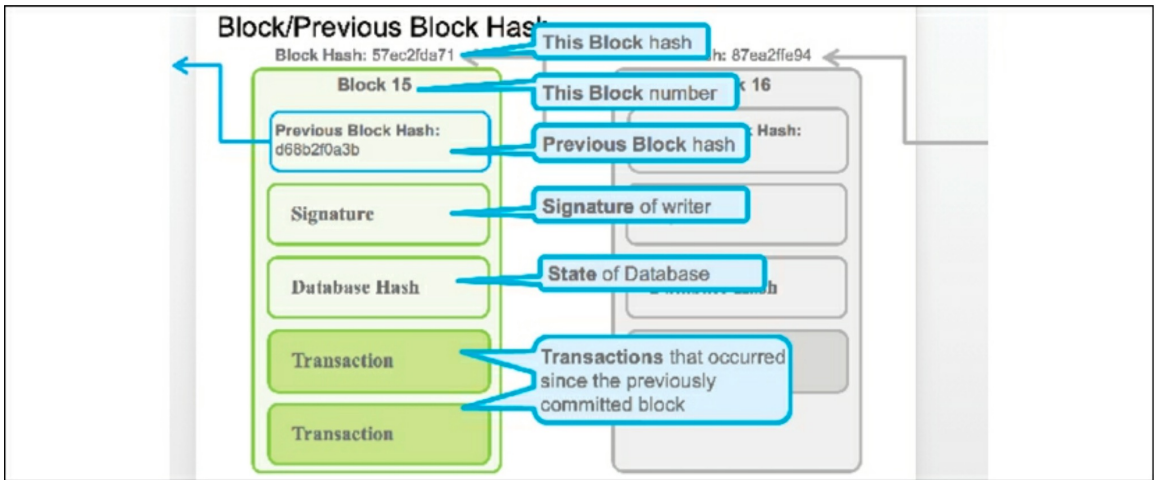
Blockchain



17

17

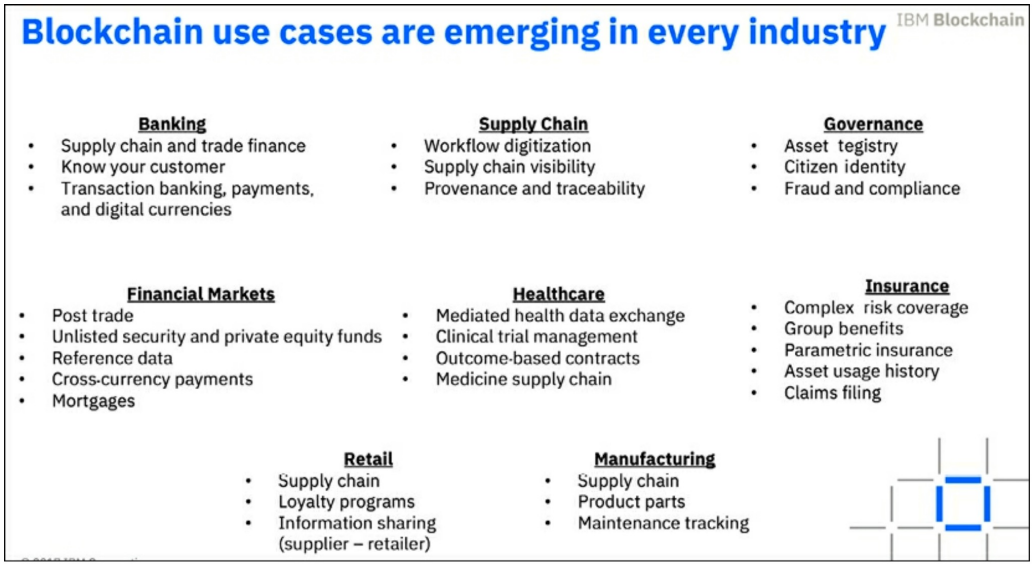
Block Internals



18

18

Block Internals



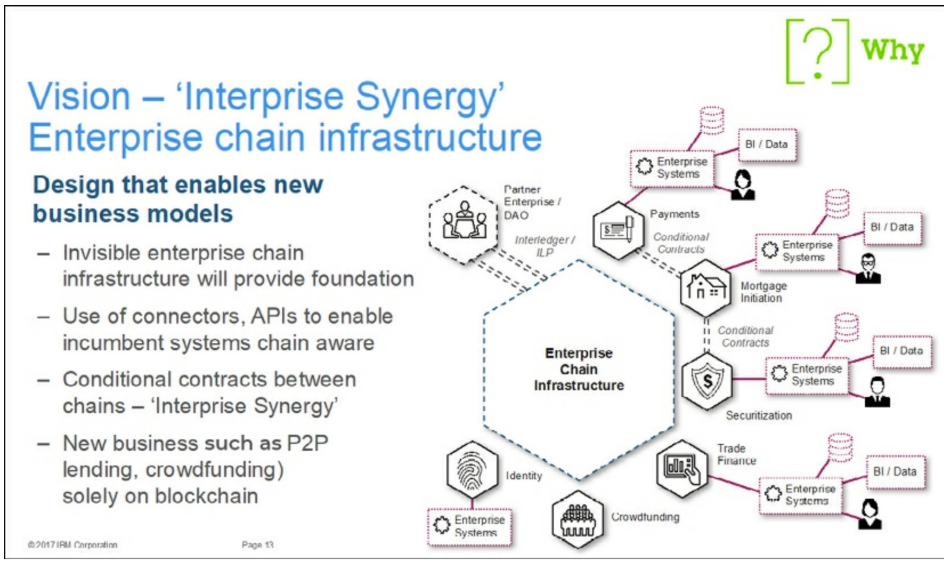
19

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



21