Blockchain Fundamentals

1. Trick to create cybercurrency
2. Technology for smart contracts
3. Database between organisations
4. Mechanism to create trust
5. Method to improve value chains
6. **Tool to (re-)organise an economy**

Dr. Johan Pouwelse
associate professor
TU Delft
peer2peer@gmail.com

Blockchain Fundamentals: create cybercurrency

Everybody can create money with this technology

No-Bank-Needed

trick 1: getting a few millions of believers

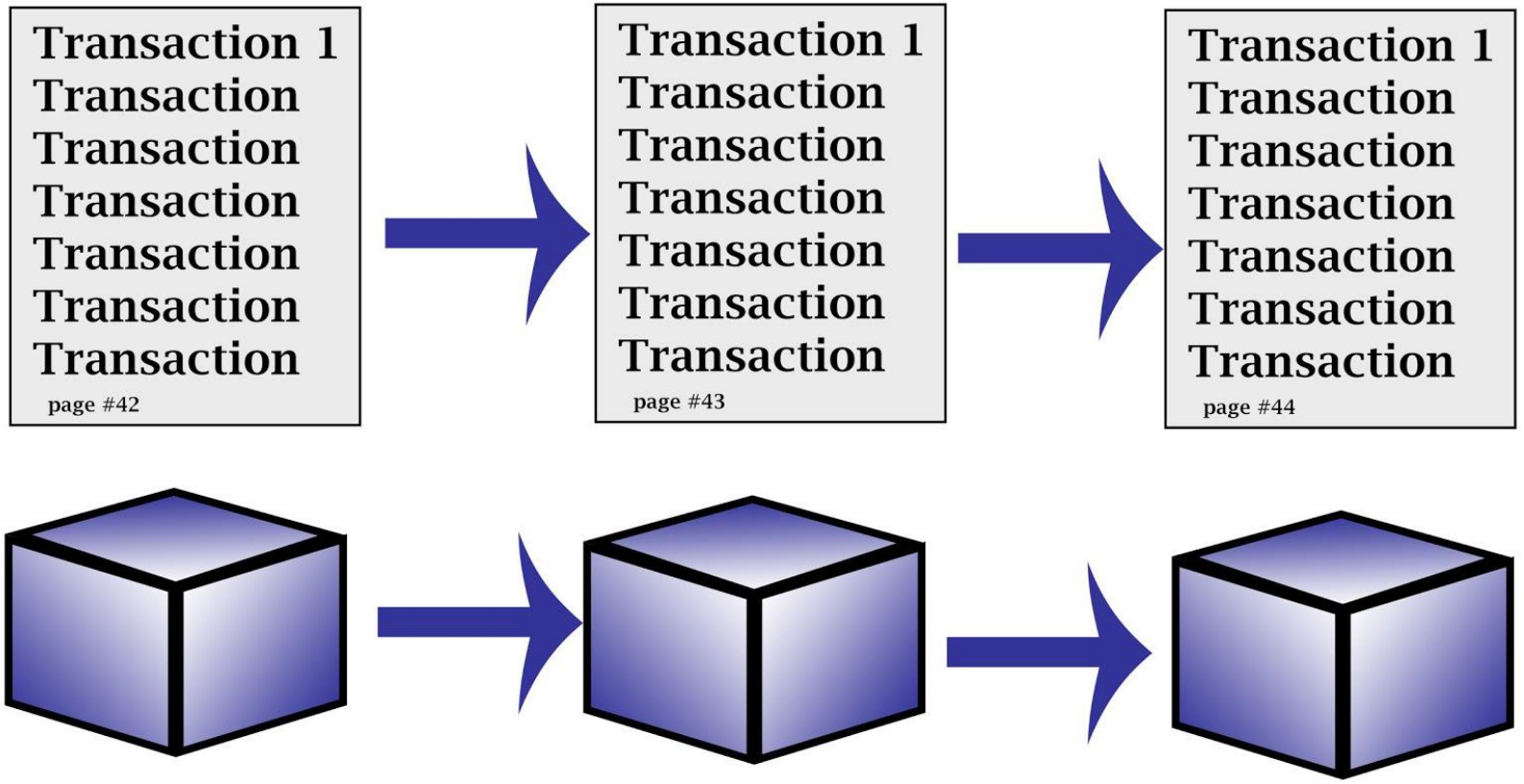
trick 2: nobody spends the same money more than once

trick 3: avoid creating too much money

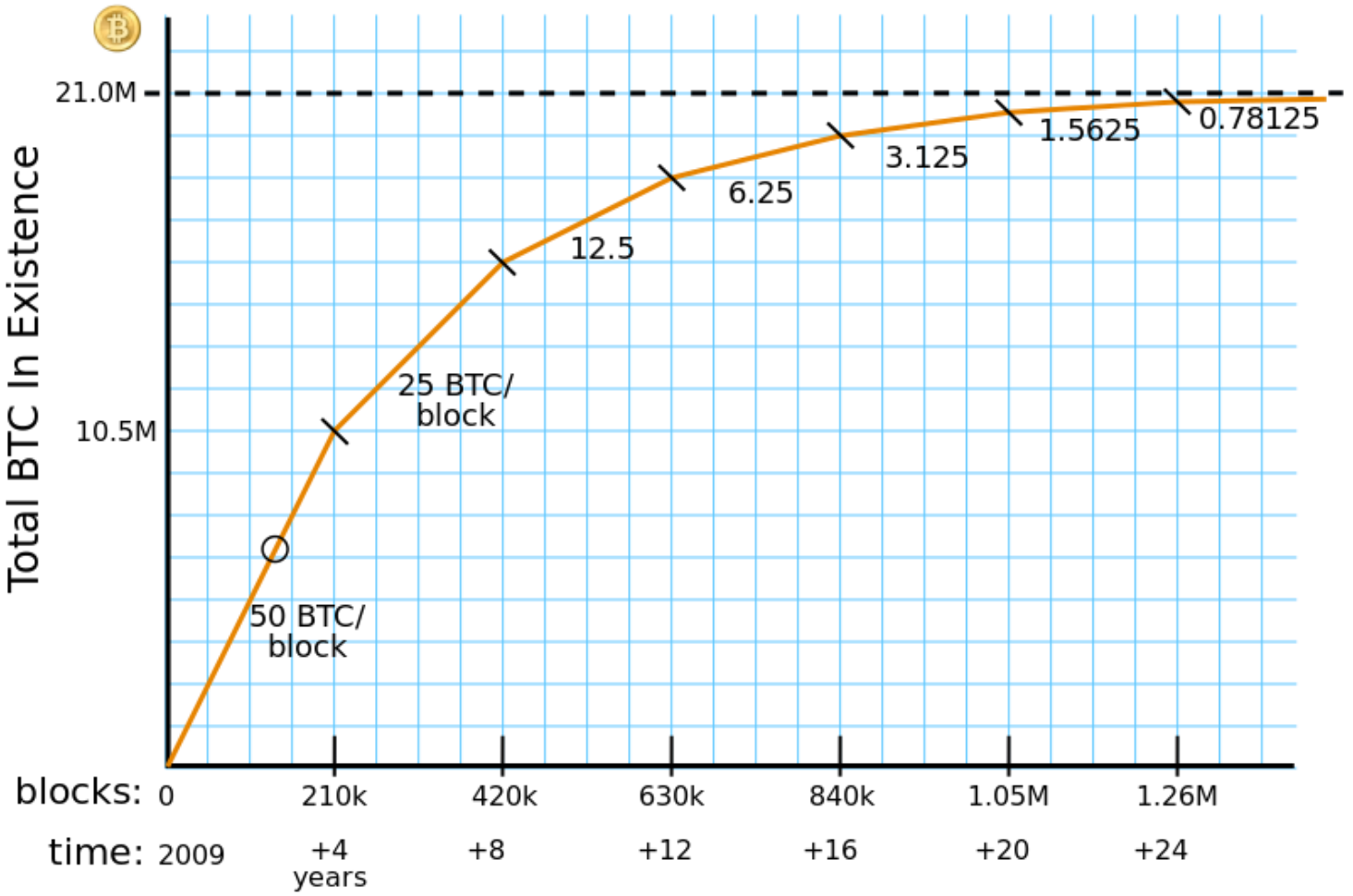
Future: enterprise-ready blockchain

trick 1 : getting a few millions believers

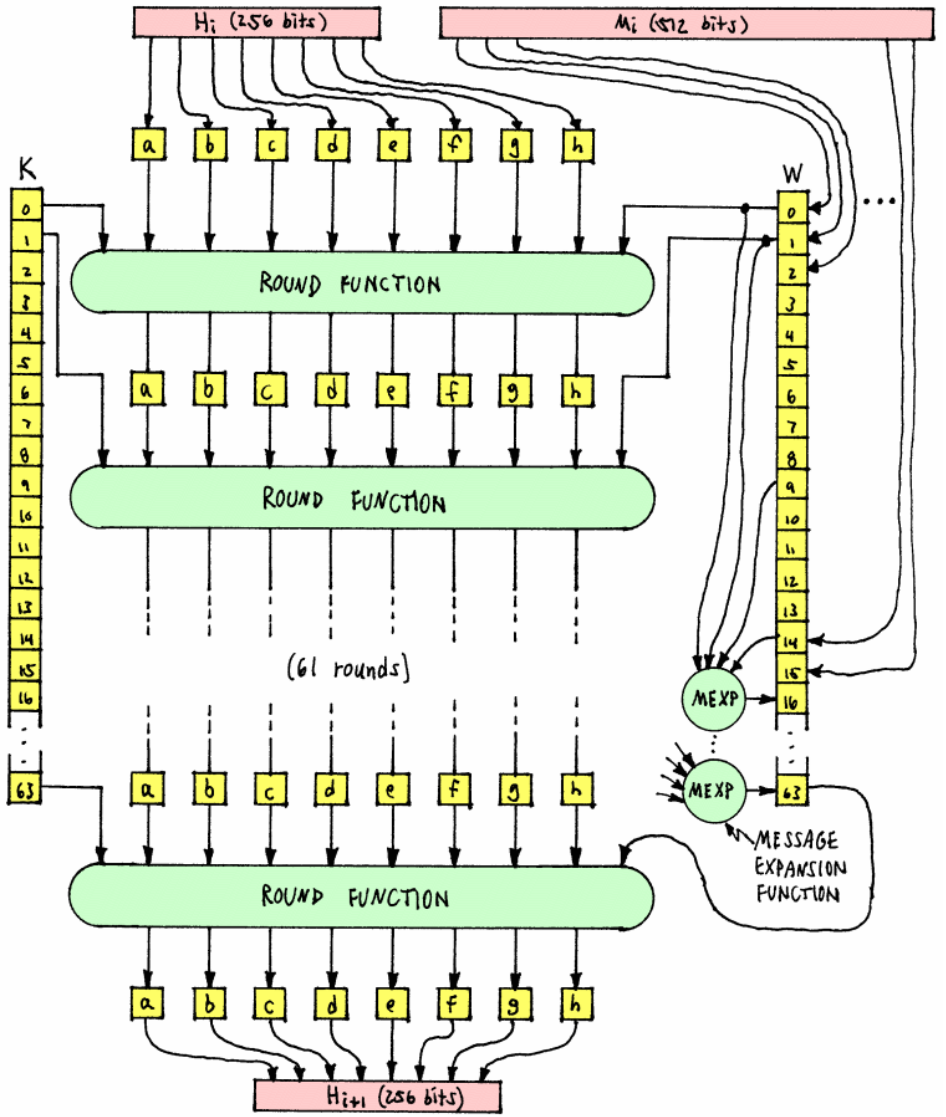
trick 2: nobody spends the same money more than once



trick 3: avoid creating too much money



Everybody can create money with this technology



000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Their platform, Their Rules, Their profit ?

Future: Enterprise-grade solution

July 2015: Ethereum, first smart contract

Jan 2009: Bitcoin, first cybercurrency

Aug 2007: BarterCast, first distributed accounting

2016 The Blockchain Ecosystem

Market Insight • Proposition Development • Customer Engagement • Product Launch

FirstPartner

Introduction

The blockchain combines cryptography & distributed computing to deliver secure, direct peer to peer transactions without the need for a central party. At its heart is the Distributed Ledger. This is a tamper proof, public, network-hosted, record of all consensus verifiedtransactions.

Initially realised via Bitcoin & similar "cryptocurrencies", focus & investment is now shifting to the potential of blockchain technology to revolutionise the infrastructure & processes of established Financial Institutions & other enterprises.

This Map summarises the key principles behind the blockchain & the emerging ecosystem addressing payments, banking & other potential use cases.

Blockchain numbers

$921 million Cumulative VC investment in Bitcoin & blockchain companies to Oct 2015. $462 million of this in 2015 alone.[1]

$121 million Largest cumulative funding total - raised by Bitcoin computer developer 21inc.[1]

805 Number of early stage Bitcoin & blockchain companies identified by Venture Scanner[2]

30+ Banks & Financial Institutions known to be testing, analysing or investing in the blockchain technologies[3]

11m Number of registered Bitcoin wallets in Sept 2015 - up from 6.6m in Sept 2014[4]

106,000 Number of merchants who accept Bitcoin[4]

$4.9bn Bitcoin capitalisation Nov 2015. Bitcoin accounts for around 90% of the capital value of all cryptocurrencies[5]

$2.7bn value of Bitcoin trading in Sept 2015[6]

475 Bitcoin ATMs installed worldwide[7]

Sources:
1 CoinDesk & Crunchbase
2 Venturescanner.com reviewed Nov 2015
3 FirstPartner research
4 CoinDesk State of Bitcoin Report Q3 2015
5 Blockchain.info checked 16th Nov 2015
6 Bitcoinity.org
7 Coin ATM Radar checked Oct 2015

Author | Richard Warren
rwarren@firstpartner.net

Like what you see?
Contact us for in-depth insight into your target markets!

Contacts | hello@firstpartner.net
+44 (0) 870 874 8700
@firstpartner
www.firstpartner.net

Copyright FirstPartner Ltd 2015

Payment Use Cases

Retailing | Person 2 Person | Remittances | Financial Inclusion | Interbank Clearing | Forex | Resilience | Trading & Markets

The Cryptocurrency Ecosystem

Specialist companies facilitating transaction validation, currency exchange, storage & payment on existing cryptocurrency newtworks (primarily Bitcoin)

Users | Merchants

Wallets: Blockchain, Xapo, Armory, bitreserve, case

Bitcoin Debit Cards: WageCan, ANDPRO

BitCoin ATM: LAMASSU, genesiscoin, BITACCESS

International Remittance: ABRA, BitPesa, R€BIT

Merchant Payment Processing: Bitcoin PoS, P€¥, DC PoS

Bitcoin Processing: Bitnet, GOCOIN, bitpay

Risk & Fraud Management: vogogo

PSPs Supporting Bitcoin: PayPal, adyen, Braintree, stripe

Exchanges: BITFINEX, kraken, LocalBitcoins.com, BITSTAMP, HUBBIT, BTC

Multiservice Companies (Mining, Exchange, Wallet, Processing): coinbase, CIRCLE, BITX, BTCC, PAMIUM

Mining

Mining Technology & Commercial Operations: 21 INC, KnCMiner, BitFury, spondoolies-tech, HASHRABBIT, BTCS

Mining Pools: - GhashIo - F2Pool - AntPool - SlushPool

Established Financial Ecosystem

Regulated financial institutions & platform vendors exploring blockchain technology as an alternative to centralised & correspondent payment processing

Money Transfer Operators: WESTERN UNION

Market Makers

Securities Markets: Nasdaq

Retail & Commercial Banks: BARCLAYS, Bank of America, Deutsche Bank, BNP PARIBAS, Fidor BANK, BBVA, citi, HSBC, ING, J.P.Morgan, UBS, RBS, Santander

Central Banks & Initiatives

Liquidity Provision | National Clearing | Compliance | Policy

The following major central banks have undertaken assessments or issued statements on regulation, potential risks to financial systems and/or benefits but none yet has a definitive policy stance.

- Bank of England
- Banque de France
- Deutsche Bundesbank
- European Central Bank
- The Federal Reserve
- Monetary Authority of Singapore
- People's Bank of China
- Reserve Bank of India

Card Schemes: VISA, MasterCard, AMEX

Interbank Networks: SWIFT, earthport

Enabling the Financial Services Blockchain

Commercial platforms & services targeting Financial Institutions

Securities & Derivatives & Asset Trading Platforms

Smart contracts & blockchain for transparent trading & post trade settlement

Mirror, clearmatics, symbiont, HEDGY, SETL

The R3 Consortium

Technology led initiative of 30+ banks to design & apply distributed ledger technology to global financial markets

Institutional Investment: TradeBlock, itBit, SolidX

Financial Infrastructure & APIs

Enable implementation of private Blockchains/ sidechains &/or the development & securing of financial applications

BLOCKCYPHER, eris INDUSTRIES, Gem, ripple, Digital Asset Holdings, Chain, Blockstack.io

Bitcoin Based Cryptocurrencies

Open Protocols for Institutions

The Distributed Ledger

Anatomy of a Transaction

1 Initiation — Transaction instruction -prior transaction(s) -recipient address -value & conditions -digital signature

2 Verification — the network — nodes or miners: -propagate -group into "candidate Blocks" -validate signatures -verify through "consensus"

3 Completion — Verified Block — "Value" — recipient — Blockchain

Protocol Components

The Currency

The medium for transaction settlement within the newtork & rewarding miners. Cryptographically generated, protocol rules determine issuance & destruction. May be tradeable "off the newtork" (e.g. Bitcoin) or only exist on network (e.g. XRP)

The Ledger

AKA the Blockchain. A Public record of all transactions - stored across a distributed P2P network of servers. Verified transactions are added in "blocks" and the history provides proof of value or assets "owned".

Consensus

Prevents "double spend" or validation of fraudulent transactions:

Proof of work: miners compete to validate blocks by solving highly processor/RAM intensive cryptographic problems for reward

Distributed consensus: majority validation by trusted subnetworks of peer nodes within the network. Used by Ripple & Stellar

Proof of stake: achieves distributed consensus by network users proving their ownership of currency. Used by Peercoin & Ishares

Bitcoin
Created as an alternative to central bank controlled fiat currencies, Bitcoin was the first working Cryptocurrency. It remains dominant but lack of scalability and other inherent flaws will likely prevent mass adoption.
Validation: Proof of Work
Latency: 10 minutes
Currency: BTC - on and off-network
Issuance: Mining Reward. 21M Limit

Litecoin
Consensus: Proof of Work
Latency: 2.5 minutes
Currency: LTC - on and off-network
Issuance: Mining Reward. 84M Limit

Dogecoin
Consensus: Proof of Work
Latency: 1 minute
Currency: Doge - on & off-network
Issuance: Mining Reward. Unlimited

Ripple
Consensus based protocol designed specifically for existing financial institutions. Supplementing existing processes & directly suporting fiat currencies, lead use cases are international payments & inter financial institution settlement
Validation: Distributed consensus
Latency: 3 seconds
Currency: XRP on-network only
Issuance: All inception -100 BN units created.

Ethereum
Smart contract & distributed app focus
Validation: Proof of Work
Latency: 12 seconds
Currency: ETH on-network only
Issuance: Mining Reward.

Stellar
Ripple derivative. Financial focus
Validation: Distributed consensus
Latency: 2-5 seconds
Currency: Lumens on-network only
Issuance: 100 BN then 1% issued PA

Blockchain — Distributed P2P Networks

Crypto 2.0 - Building on the Bockchain

Smart Contracts

Encode & validate "conditions" for a transaction between parties. Potentially facilitate legally binding transactions over the blockchain

CLEARINGHOUSE, consensys, Counterparty, CODIUS

Colored Coins & Open Assets

Bitcoins altered to represent an asset. Exchanged via the Open Assets Protocol. Allows trading of physical & other assets

coin.u, ChromaWay, coinprism, Omni

Core Blockchain Protocols

bitcoin, stellar, ripple, DASH, ethereum, Peercoin, VIACOIN

Enabling Layers

Protocols, platforms & SDKs that build on top of core blockchain protocols to enable additional transaction types & services

Ripple: facilitating multiple financial institutions focussing on payment solutions

Protocol Commercialisation

Consensys: building on Ethereum based ecosystem & partnered with Microsoft for Ethereum Blockchain as a Service

FILAMENT, IBM, SAMSUNG, factom, MaidSafe, STORJ.IO, ShoCard, stampery, Bitproof.io

IoT — Registering and validating connected devices

Data — Distributed storage of and access to business data

e-Identity — Registering and validating individual identity

Legal — Executing smart legal contracts

lighthouse, OpenBazaar, La'Zooz, BLOCKPARTI, ALEXANDRIA, BISANTYUM

Crowd Funding — Raising finance & distributing equity

Market Places — Trading & sharing of physical & digital assets & services

Publishing — Digital asset rights management, distribution & payment

Proof of Ownership — Tamper proof registration & "stamping" of physical & digital assets

Other Use Cases

Data & Analytics: COINALYTICS, BLOCKCORP, blockr, KAIKO, bitcoin charts

Key Security/HSMs: gemalto, THALES

Balancingthe Benefits

Blockchain Benefits
- Ecosystem simplification
- Faster Interbank clearing & settlement
- Lower transaction costs
- Reduced counterparty risk
- Transparency & auditability
- Ease of software development/integration

Vs.

Risks
- Unproven technology
- Untested capacity/scalability
- Low transaction speed
- Possible consensus protocol flaws
- Cryptocurrency price volatility
- Uncertain regulatory status

Investors: ANDREESSEN HOROWITZ, BLOCKCHAIN CAPITAL, overstock, Google ventures, LIGHTSPEED VENTURE PARTNERS, AME CLOUD VENTURES, DIGITAL CURRENCY GROUP, PANTERA

Future

Are we 2 years away from the transformative blockchain effect?
Or 5 to 10 years?

Future

Are we 2 years away from the transformative blockchain effect? Or 5 to 10 years?

Unknown: nobody in the world has an enterprise-ready blockchain

Enterprise-ready blockchain requirements

Tamper-proof database

Scalability to thousands of participating organisations (open)

No forking, no transaction block limit, no fatal Bitcoin link

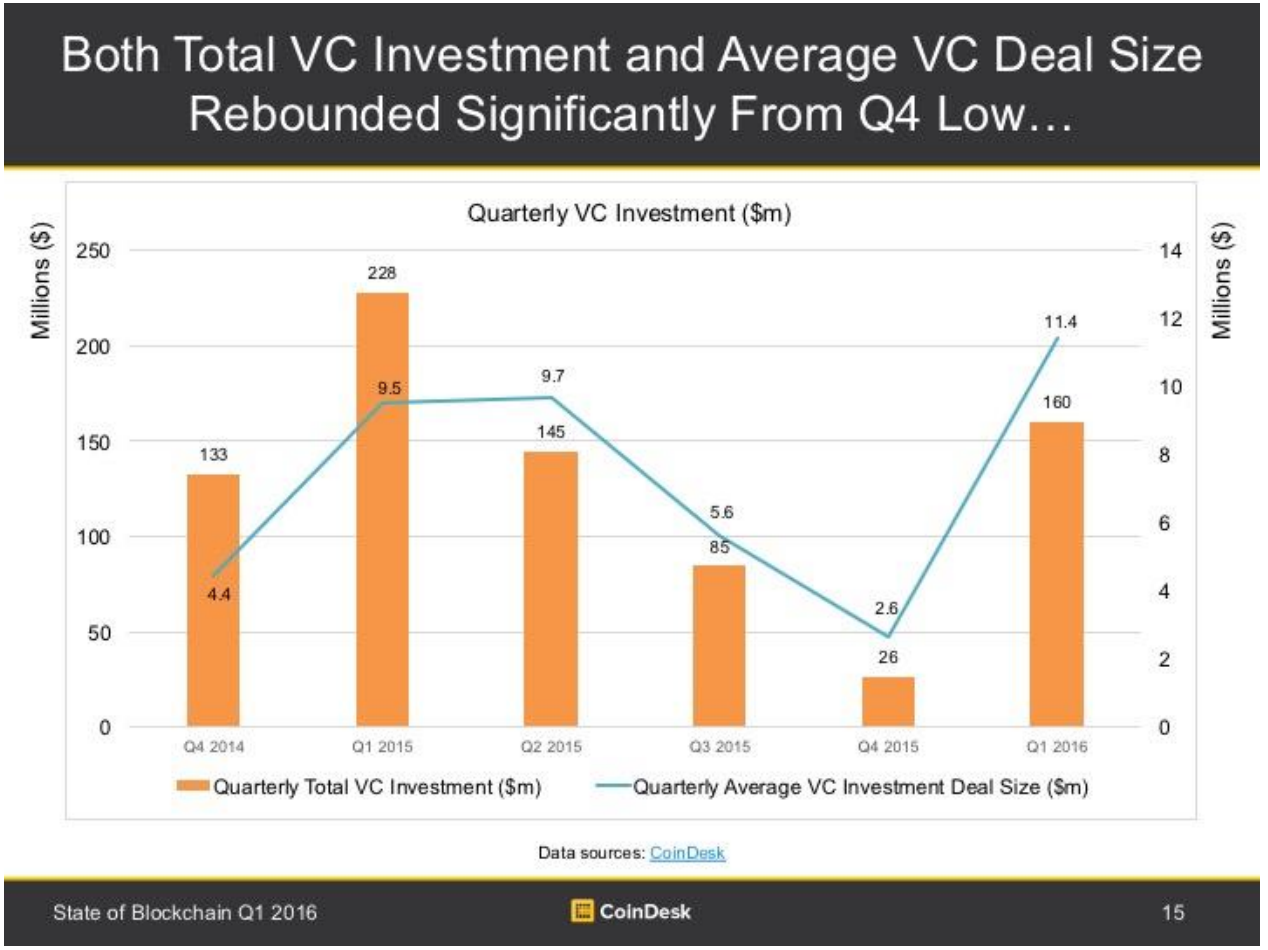
No proof-of-work mining, no proof-of-stake

No single vendor in control, no central platform

Fix privacy, keep transparancy, protect business secrets

Classics: Authentication, Identity management, Access control

$1.11 Billion VC bubble ?

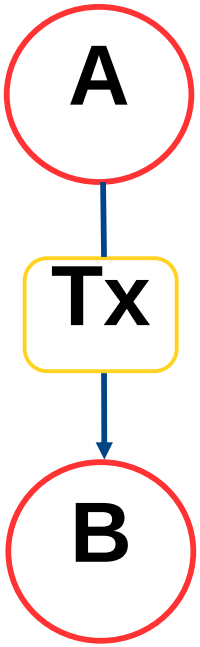


https://www.weusecoins.com/en/venture-capital-investments-in-bitcoin-and-blockchain-

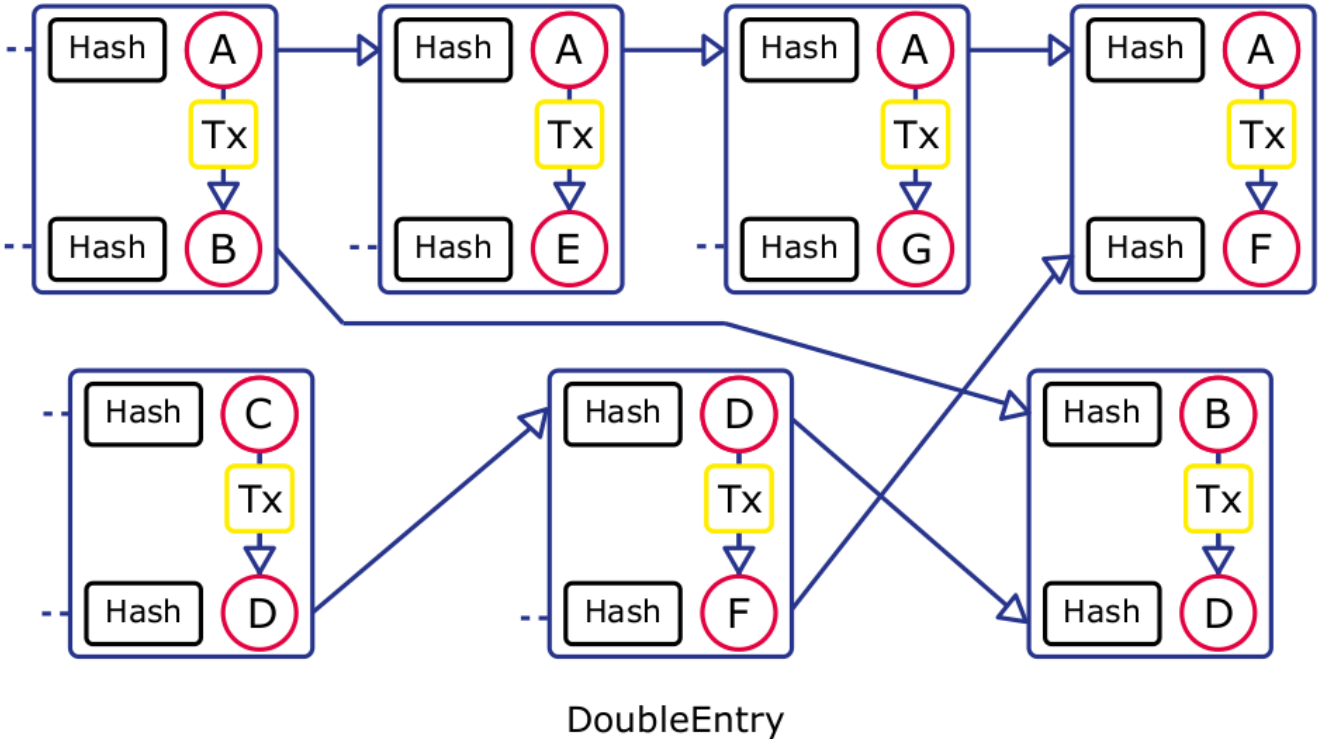
Delft Blockchain and application

2007: TUDelft & Harvard: bandwidth-as-a-currency

Delft Blockchain: Multi-chain

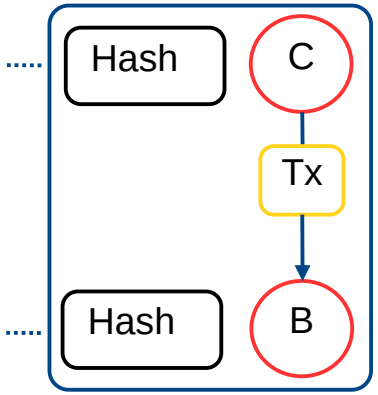


tamper-proof interaction history

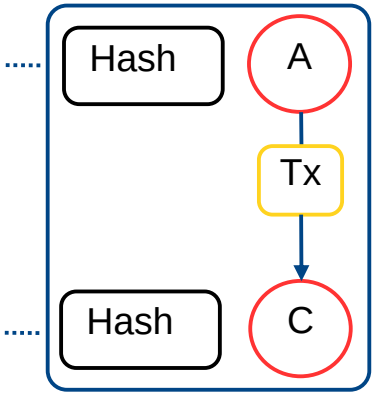


Blockchain arithmetic

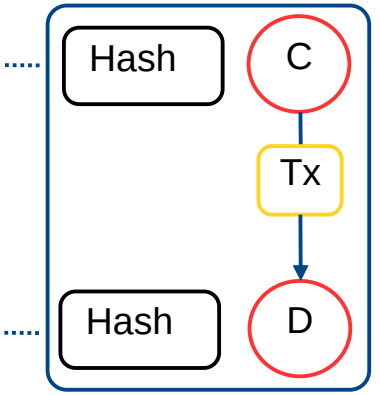
strategy-proof, attack-resilient
- support bulk and offline transactions
- accounting system for any asset



Tx = C gives 10 units



Tx = C takes 35 units



Tx = C gives 25 units

Tx + Tx + Tx = 10 + -35 + 25 = 0 units

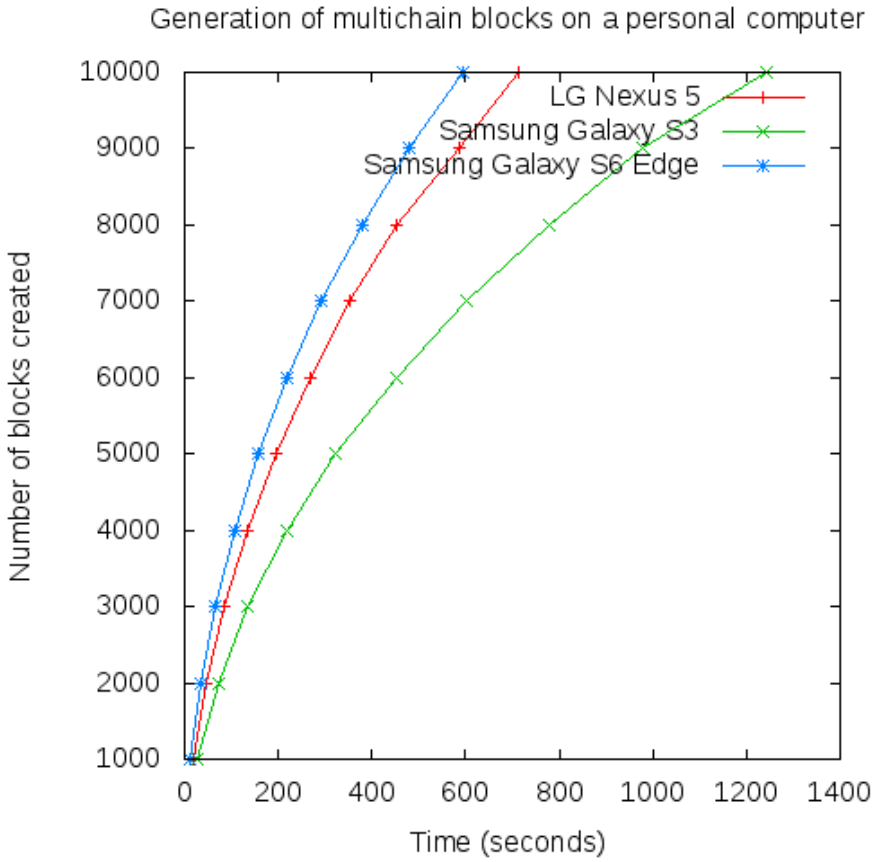
Tribler

- Our academic experimental playground
- Evolution of cooperative systems
  - Internet-Deployed since Feb 2006
  - 1.8M Tribler installs
- First distributed ledger
- Counting contributions (upload/download bytes)

"Researchers have created invincible file sharing software", Fox News, Feb 10 2012

Source: Seuken et al."work accounting mechanisms: theory and practice", 2010, Harvard + Delft + Berkeley, www.eecs.harvard.edu/~seuken/publications/AccountingMechanisms_Seuken10.pdf

Multi-chain: Internet deployment



Hope you got from here

to understanding of this one ...

www.blockchain-lab.org