

A Perspective on Bitcoin and Blockchain

BART PRENEEL

IMEC-COSIC KU LEUVEN

BART.PRENEEL(AT)ESAT.KULEUVEN.BE

6 JUNE 2017



KU LEUVEN

imec

embracing a better life



Currencies = maintaining memory



“Envelope and contents from Susa, Iran, circa **3300 BCE.**”

“Each lenticular disc stands for “a flock” (perhaps 10 animals). The large cone represents a very large measure of grain; the small cones designate small measures of grain.”

Tensions between centralized and de-centralized ways to remember value exchanges, debts, and what is due

- **Centralization (clay tablet):** economies of scale, high-integrity, vulnerable
- **Decentralized (coins):** high-availability, difficult to destroy as a system, forgery

Hash functions (1975): one-way easy to compute but hard to invert



RIPEMD-160

SHA-256

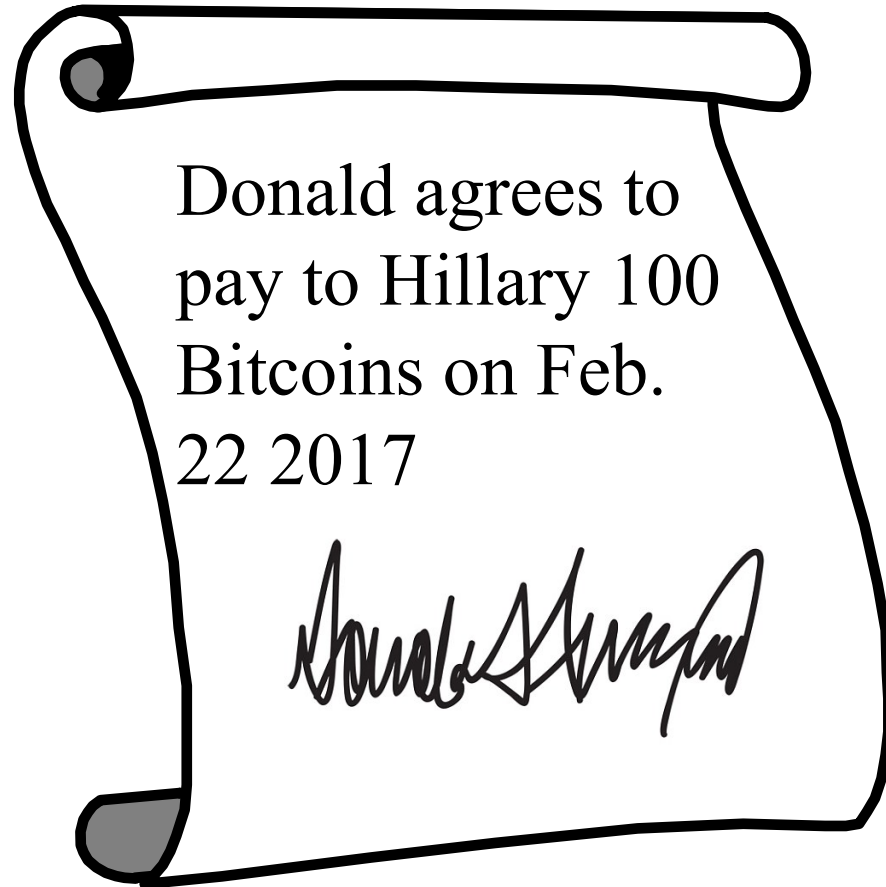
SHA-512

SHA-3

This is an input to a cryptographic hash function. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard to find an input hashing to a given value (a preimage) or to find two colliding inputs (a collision).



Digital signatures (1975): “equivalent” to manual signature



Public key



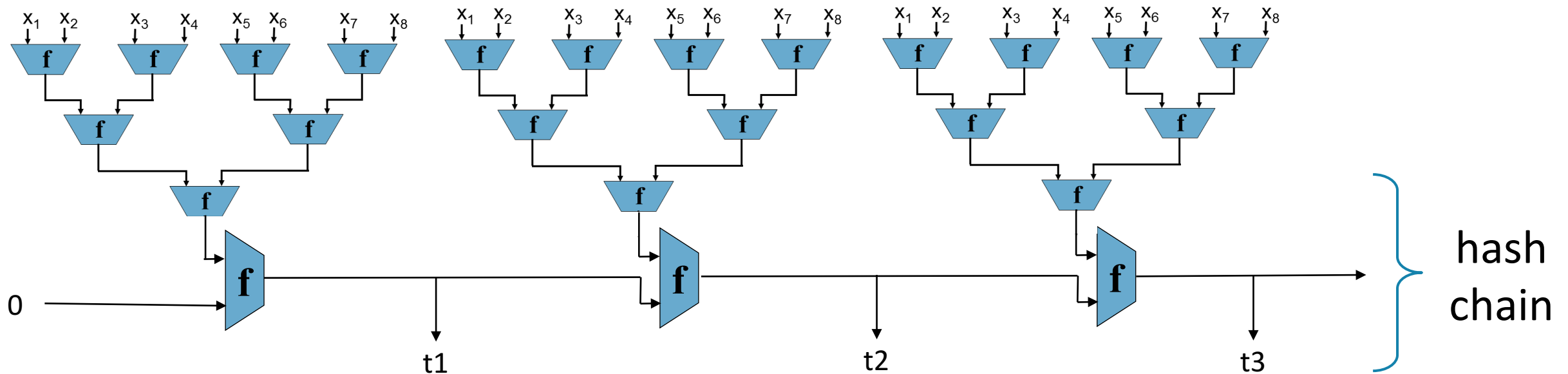
Private key

Timestamping (1990)

Collect documents and hash them with a Merkle tree

Chain these trees together with a hash chain

Publish intermediate values on a regular basis



Timestamping: Surety Technologies (°1994)

<http://www.surety.com/>



The screenshot shows the homepage of Surety Technologies. At the top, there is a navigation bar with links for Home, AbsoluteProof®, Contact, and Support, along with social media icons for RSS, Facebook, Twitter, and LinkedIn. A search bar with a 'GO' button is also present. Below the navigation bar is a red menu bar with links for What We Do, Solutions, Partners, News, About Us, Resources, and My AbsoluteProof. The main content area features a large banner for 'AbsoluteProof from Surety' with a red wax seal logo and the tagline 'The Leader in Data Integrity Protection'. A 'PLAY AGAIN' button is visible in the top left of the banner. Below the banner, there is a section titled 'Think of us as the "Digital Wax Seal"'. To the right of the banner, there are three highlighted services: Intellectual Property Protection, Digital Evidence Protection, and Electronic Record Authenticity, each with a brief description and a link to learn more. At the bottom, a footer bar states 'Protect the Integrity, Defend the Authenticity of Your Digital Information'.

Home | AbsoluteProof® | Contact | Support

What We Do | Solutions | Partners | News | About Us | Resources | My AbsoluteProof

Intellectual Property Protection
Protect your patents, copyrights, trademarks, and trade secrets »

Digital Evidence Protection
Preserve the integrity of your electronic evidence »

Electronic Record Authenticity
Defend the authenticity of your electronic records »

AbsoluteProof® from Surety®
The Leader in Data Integrity Protection
LEARN MORE >>

Think of us as the "Digital Wax Seal"

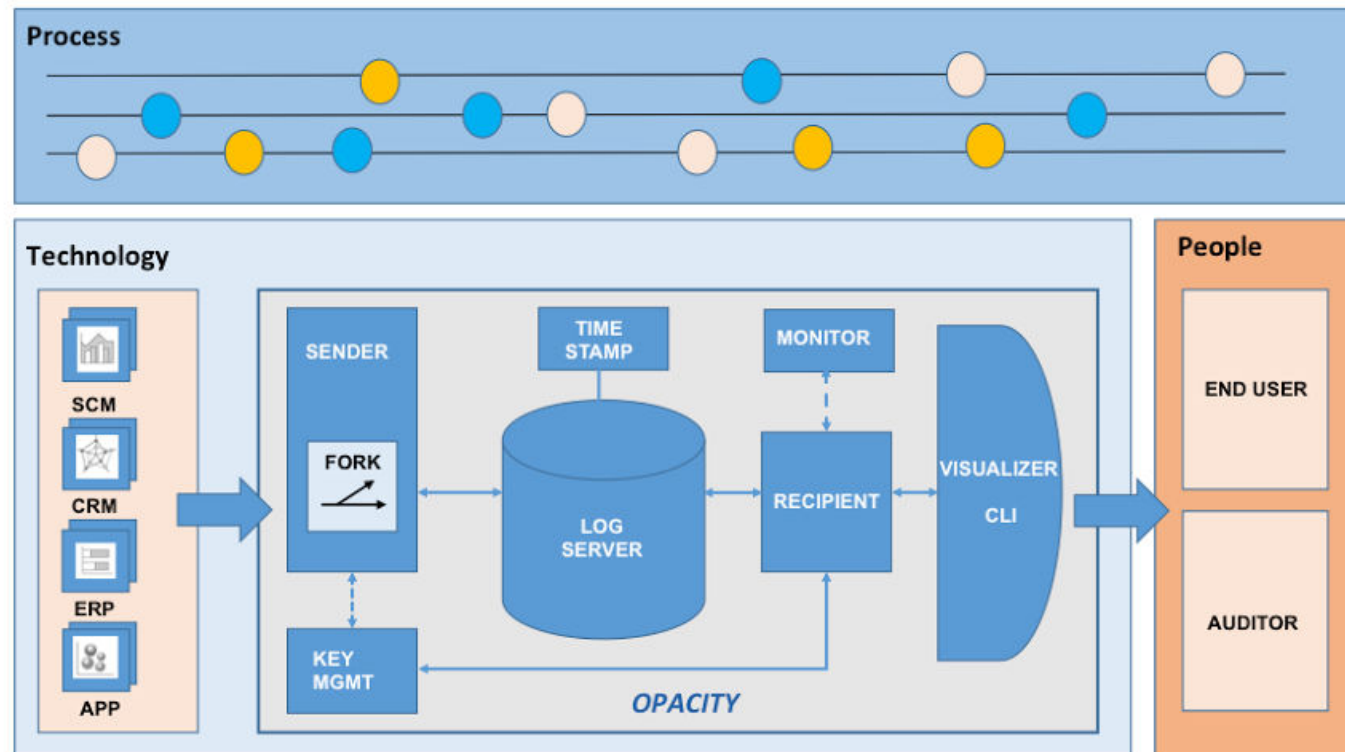
Protect the Integrity, Defend the Authenticity of Your Digital Information

Distributed logging + Privacy



OPACITY

<http://www.project-opacity.com/>





Bitcoin? (2008)

E-currency with **distributed** generation and verification of money

Transactions

- irreversible
- inexpensive
- over anonymous peer-to-peer network
- broadcast within seconds and verified within 10 to 60 minutes by inclusion in **hash chain**
- pay using **private key** (digital signature); verify with **public key**
- double spending prevention using a public decentralized ledger (chaining mechanism)

Pseudonymous

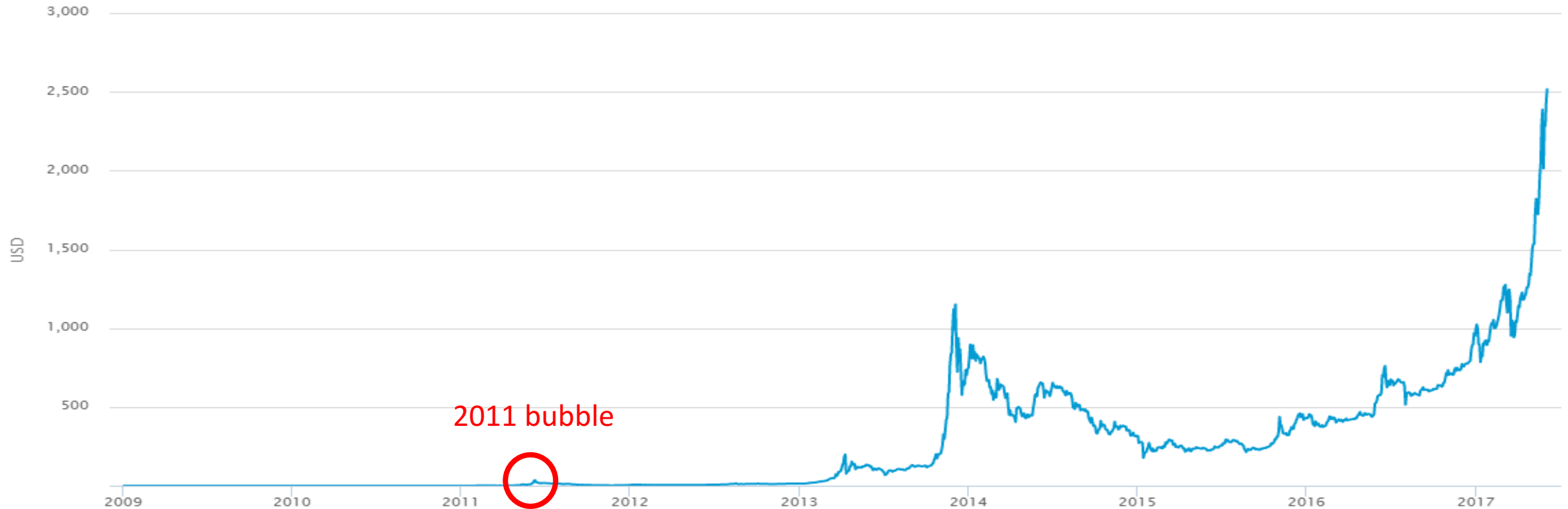
- Money is linked to **public key** – can generate arbitrary key pairs and move money around
 - But in many cases identification is possible

Market price in USD (market cap \approx 42.5 B\$)

1 Bitcoin = 2593\$

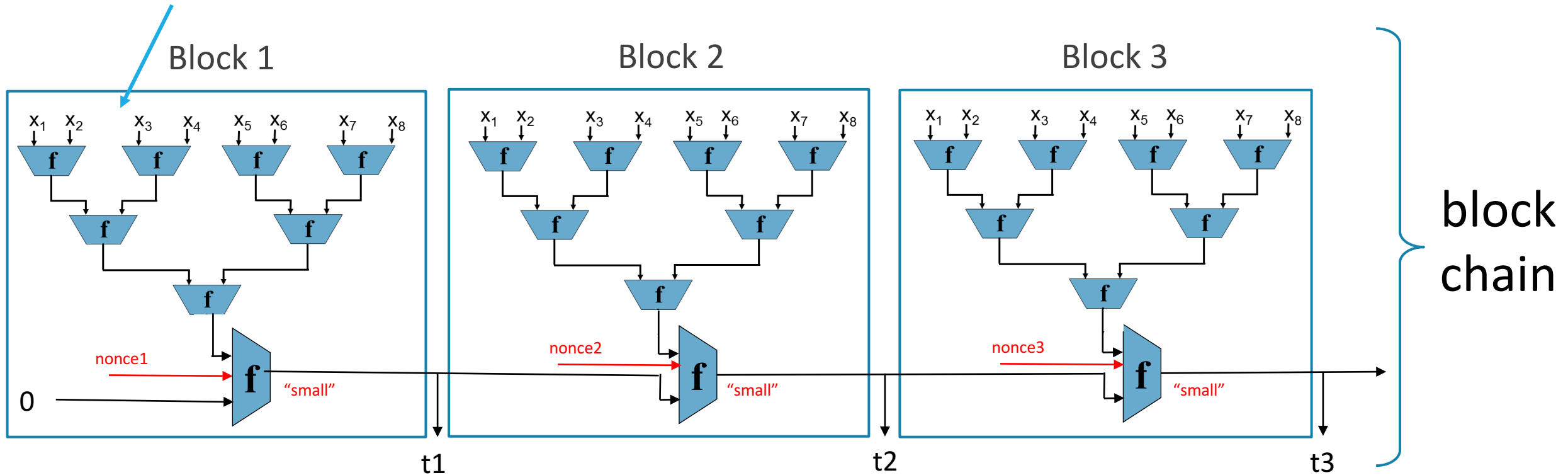
Market Price (USD)

source: blockchain.info



Block Chain: a public decentralized ledger

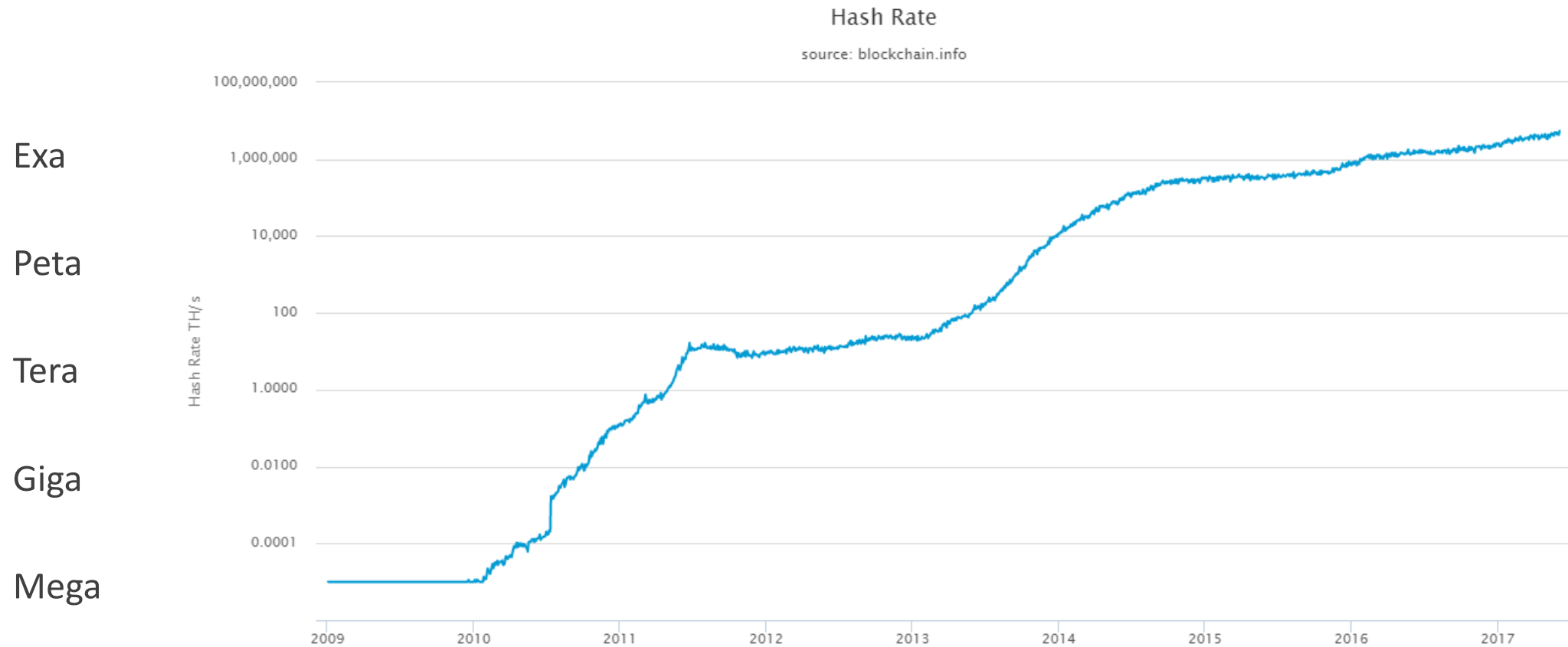
Bitcoin transactions



Also include in every block timestamp and difficulty level of puzzle

Mining hash rate of Bitcoin network

5.5 EH/s = 5.5 ExaHash per second = $5.5 \cdot 10^{18}$ hash/second = $2^{62.3}$ hash/second



Mining has become industrial



CPU



GPU



FPGA



ASIC



gold pan



sluice box



placer mining



pit mining

Mining equipment on Amazon



Sponsored ⓘ

[AntMiner S9 ~13.0TH/s @ .098W/GH 16nm ASIC Bitcoin Miner](#)

by AntMiner

\$2,199⁰⁰

FREE Shipping on eligible orders

In stock on February 27, 2017

★★★★☆ 9

- Hard Disk Size: **4.0 GB**
- Computer Memory Size: **512.0 MB**
- Hardware Platform: **Linux**
- System Ram Type: **ddr3 sdram**
- Hard Disk Interface: **solid state**



Sponsored ⓘ

[Antminer S9 14TH/s 0.10W/GH 16nm ASIC Bitcoin Miner](#)

by AntMiner

\$2,299⁰⁰

FREE Shipping on eligible orders

In stock on February 27, 2017

★★★★☆ 4

- Hard Disk Size: **4.0 GB**
- Computer Memory Size: **512.0 MB**
- Hardware Platform: **Web browser**
- System Ram Type: **ddr3 sdram**
- Operating System: **Linux**



[AntMiner S5 ~1155Gh/s @ 0.51W/Gh 28nm ASIC Bitcoin Miner](#)

by AntMiner

\$350.00 new (1 offer)

\$269.99 used (3 offers)

★★★★☆ 62

- Hardware Platform: **Linux**
- System Ram Type: **dimm**
- Operating System: **Linux**

Sponsored ⓘ



[Antminer S7 Version 7 ~5.06TH/s...](#)

\$850⁹⁵

★★★★☆ 3



[Bitmain Antminer R4 ~8.7TH/s at...](#)

\$1,796⁰⁰

★★★★☆ 1



Cost of Leaderless Consensus

Distributed consensus protocol:

- whichever coalition deploys most hash power, has control of the block chain
- $5.5 \cdot 10^{18}$ hash/second is a significant cost.
- not performing any useful task!

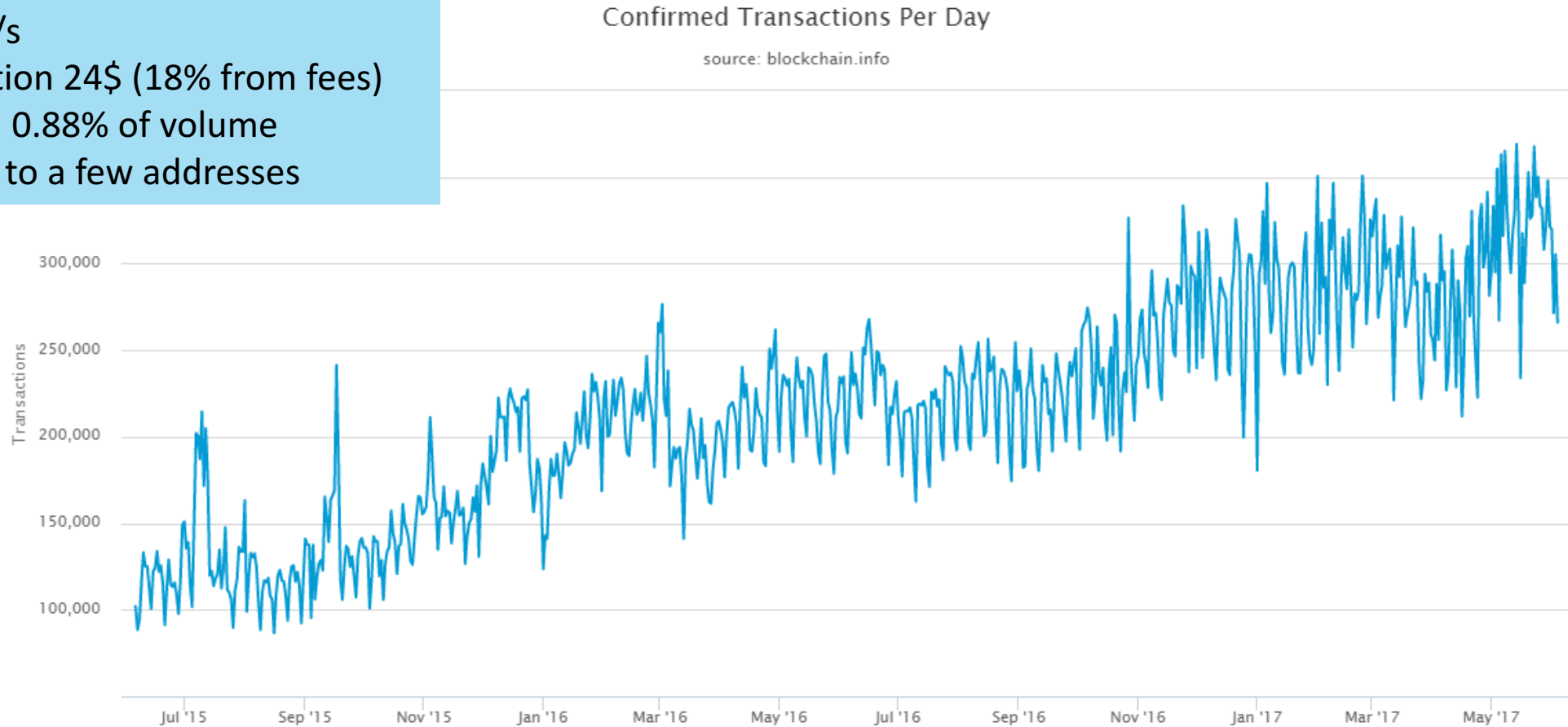
Electricity + Networking costs:

- 0.10 W/GH/s or 550 MWatt (1/2 of a nuclear plant)
- @10 cent per KWh: 1 block costs 9200\$ electricity (12.5 BTC = +/-32,400\$)

Profit calculator: <http://www.vnbitcoin.org/bitcoincalculator.php>

Number of Transactions Per Day

3.5 transactions/s
cost per transaction 24\$ (18% from fees)
transaction fees: 0.88% of volume
large share goes to a few addresses



Bank card payments: around 10.000 per second?

Alt CoinsToday: 700+ currencies derived from Bitcoin (see <http://mapofcoins.com/bitcoin>)





2017

Some observations on Bitcoin

Bitcoin community aspires to be mainstream but behaves as rebels

- this is not sustainable

Volatile

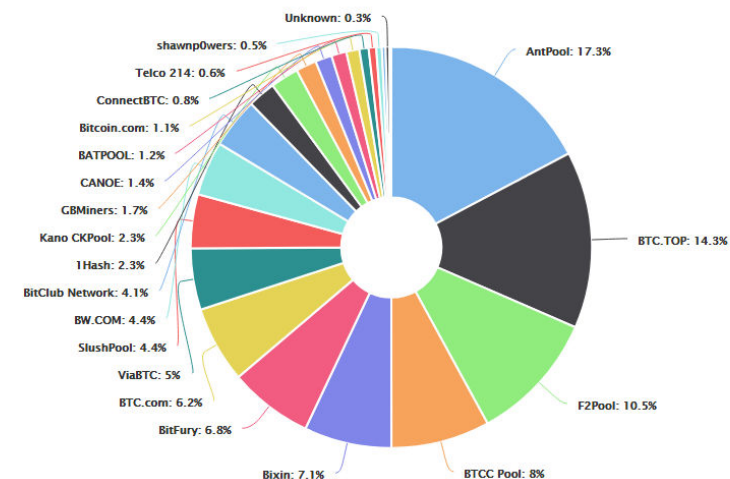
Paying and secure storage somewhat complex

No peace of mind for users: if you are hacked, tough luck

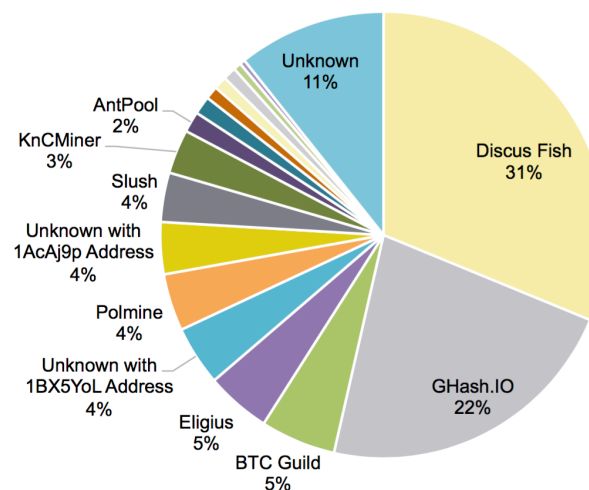
Most miners are in China (70%)

Incentives system complex

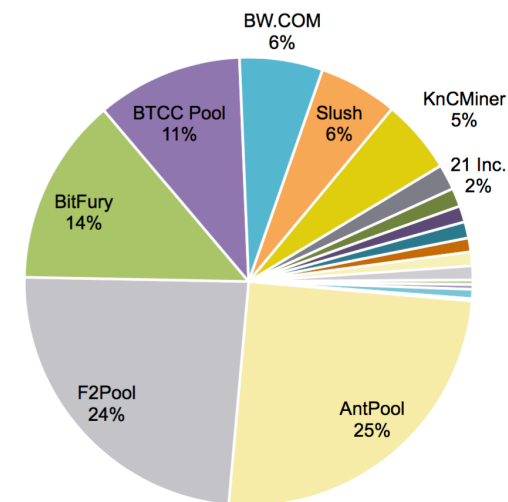
Not clear that the system will survive, but some ideas will for sure



2014



2015





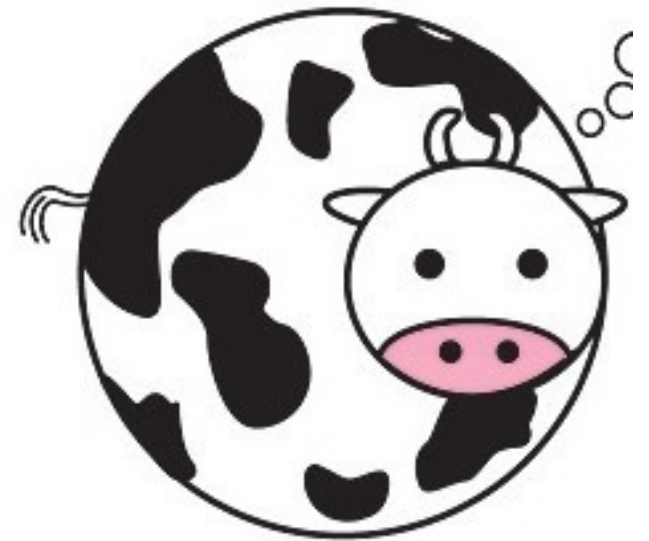
Open issues: Bitcoin

Is Bitcoin incentive compatible?

- Convergence
- Fairness
- Liveliness

- Sybil attack: attacker controls many nodes in network, can refuse relaying or favouring his own blocks
- Selfish mining attack
- Bribery

Some proof exist in simplified models





Open issues: cryptocurrencies

Design of contracts (e.g. trading digital art)

Block chain technology for non-currency applications:

- typical applications: decentralized consensus required
- Namecoin: key-value registration and transfer platform, used for domain names etc...
- Ethereum: contract processing and execution platform using Turing-complete language

Can we avoid the enormous computational cost? (proof of stake)

Is a zero-governance currency possible?

Bitcoin needs governance for “hard” upgrades

Business

Financial world dislikes

- distributed control
- full transparency
- unclear governance (or anarchy)
- uncontrolled money supply

Restrict: write, verify or read (fully private block chain)

Distributed Ledger: a range of solutions

Public Blockchain

- No central point of control by individuals, corporations or governments
- Permissionless to participate
- Consensus based on “proof of work”
- Examples:
 - *Bitcoin*
 - *Ethereum*

Consortium/Hybrid Blockchain

- Controlled by > 2 individuals, corporations or governments
- Permission on participation from consortium necessary
- Arbitrary consensus mechanism
- Readability of the blockchain can be public or restricted to the consortium
- Example: *RSCoin (UC London)*

Full private Blockchain

- Controlled by one individual, corporation or government (no consensus needed)
- Permission on participation from owner necessary
- Readability of the blockchain can be public or restricted to one

Distributed Ledger

distributed database - only needed if

- multiple mutually distrustful writers
- no intermediate party that is trusted by all players
- interactions or dependencies between the transactions

Financial sector: disintermediation?

- 20% seriously investing
- 20% planning to invest
- 20% watching the space very closely

Aite Group: blockchain market could be worth as much as \$400m in annual business by 2019

Distributed Ledger: open questions

Explore the continuum between fully open and fully restricted ledgers?

Develop a methodology to design restricted distributed ledgers as a function of the business requirements

Which advanced cryptographic and scripting techniques can be used in private or permissioned ledgers to improve privacy and to allow for complex transactions such as smart contracts?

2016 The Blockchain Ecosystem

Market Insight • Proposition Development • E

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 verified transactions.

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.

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

805 Number of early stage Bitcoin & blockchain companies identified by Venture Scanner²

30+ Banks & Financial Institutions known to be testing, analysing or investing in the blockchain technologies³

11m Number of registered Bitcoin wallets in Sept 2015 - up from 6.6m in Sept 2014⁴

106,000 Number of merchants who

Payment Use Cases



The Cryptocurrency Ecosystem

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



The Distributed Ledger

Anatomy of a Transaction

1 Initiation

Protocol Components

The Currency

The medium for transaction settlement within the network & recording chain. Cryptographically generated, protocol rules determine issuance & destruction. May be tradeable "off the network"

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



Ripple

Consensus based protocol specifically for settling transactions. Supplement processes & directly use currencies, used via centralised institutions with Validators: Distributed consensus
Latency: ~3 seconds

<http://www.ecrypt.eu.org/csa/documents/D3.2-Cryptocurrencies.pdf>



H2020-ICT-2014 – Project 645421

ECRYPT – CSA

ECRYPT – Coordination & Support Action

D3.2

Cryptocurrencies
– Challenges and Research Directions

Pointers

<http://www.ecrypt.eu.org>

<http://www.bitcoin.org>

<http://www.blockchain.com>

<http://www.vnbitcoin.org/bitcoincalculator.php>

<http://randomwalker.info/bitcoin/>

<http://www.coindesk.com/>

Nathaniel Popper, Digital Gold, Harper, 2015

Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcoin and cryptocurrency technologies, Princeton University Press, 2016

A. Biryukov, D. Khovratovich, I. Pustogarov: Deanonimisation of Clients in Bitcoin P2P Network. ACM Conference on Computer and Communications Security 2014: 15-29

S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker, S. Savage: A fistful of bitcoins: characterizing payments among men with no names. Internet Measurement Conference 2013: 127-140

Financial Cryptography conference series

TELEPHONE: +32 16 321148

ECRYPT CSA

27