Payment instructions and currencies

**Payment Instruments:** mechanism of how we **transfer value**
- cash
- letters of credit
- cheques
- bank transfer
- debit card

Each payment instrument has a **cost**
- actual monetary cost
- handling cost

**Instruments have different security properties**
- integrity/authenticity
- privacy: compare cash to bank or credit card payments
Early examples

Digicash (1990-1998)
  - collapsed under hyperinflation
  - Follow up BitTorrent
e-gold (1996-2008)
  - 1 million user accounts by 2002
  - liquidated

Main properties

Distributed generation and verification

Transactions
  - irreversible
  - inexpensive
  - over anonymous peer-to-peer network
  - broadcast within seconds and verified within 10 to 60 minutes by inclusion in hash chain
  - double spending prevention using a public decentralized ledger (chaining mechanism)

Pseudonymous (believed by many to be anonymous)
Bitcoin Ledger

Block Header
- Block hash
- Previous block hash
- Transactions hash

Transactions
- Transaction 1
- Transaction 2
- Transaction 3
- Transaction 4

………..

Block hash
Previous block hash
Transactions hash

Transactions
- Transaction 1
- Transaction 2
- Transaction 3
- Transaction 4

………..

Block hash
Previous block hash
Transactions hash

Transactions
- Transaction 1
- Transaction 2
- Transaction 3
- Transaction 4

………..

Bitcoin Transaction

Transaction A
- In
- Out
- Out

50 BTC
8 BTC
42 BTC

Transaction B
- In
- Out
- Out

10 BTC
5 BTC
15 BTC

Transaction C
- In
- Out
- Out

10 BTC
7 BTC
6 BTC
Bitcoin as a Currency

**Who has control of the money supply in a currency?**
- By convention it follows a well understood and committed curve that will max out
- Convention enforced by software

**Who gets the new money? Who deletes the old money?**
- No money is deleted (if you want a laugh: go suggest random deletions!)
- Money is created by hashing blocks and adding them to the block chain
- The miner gets the new coin

**How do we make sure we will always remember who has how much money?**
- Large block–chain is recorded by all (May 2016: 68 Gbyte!)
- Authoritative one is the longest – race for aggregate CPU power
**Bitcoin as a Timestamping mechanism**

**timestamping for digital signatures**
- business requirement
- essential for revocation

**technology: linear and tree hashing**
- cryptographic hashing to bind in time

**commercial: Surety technologies (1994)**
- centralized
- but: you can trust us because you don’t have to

---

**History of Bitcoin**

31/10/2008: Satoshi Nakamoto: “Bitcoin: A peer-to-peer electronic cash system”

3/01/2009: Satoshi releases Bitcoin source code and software clients; revised by many programmers since

2009-2010: Satoshi updates code and writes a large number of posts

23/04/2011: Satoshi vanishes from internet to “move onto other things”

First few years were very bumpy and shaky – almost disappeared

June 2012: Mt. Gox hacked - largest Bitcoin exchange (which trades Bitcoins for real world dollars and vice versa)

September 2012: Bitfloor hacked - $250,000 USD in Bitcoins

April 2014: Mt. Gox liquidated

Bitcoin banned in several countries: China (for banks), India, Russia, Sweden, Iceland
History of Bitcoin

January 2015: regulated exchange opened in New York

October 22 2015: European Court of Justice rules that Bitcoin purchases and sales are exempt from VAT under the provision concerning transactions relating to currency, bank notes and coins used as legal tender.

May 2016: Craig Wright claims to be Satoshi – still unverified

Market price in USD

https://blockchain.info/stats
Market Capitalization
https://blockchain.info/stats

Global financial assets about 300 trillion $

Mining Hash Rate of Bitcoin Network
https://blockchain.info/stats

1.5 \times 10^{18} \text{ Hash/sec} = 2^{60.4/\text{sec or } 2^{76.8/\text{day}}
Mining Difficulty Level
https://blockchain.info/stats

Target: mining 1 block should take roughly 10 minutes
- update level every 2016 blocks

Miners Revenue
Number of Transactions Per Day

1560 per 10 minutes or 2.6 per second

Visa: a few 1000 per second

Cost of Leaderless Consensus

Hidden consensus protocol:
- whichever coalition deploys most hash power, has control of the block chain
- 1 billion GH/s is a significant cost

Equipment:
- Oct’15: rent ASICS for 0.001 BTC per GH/s (or 0.22$)
- In Dec 2013, 6M GH/s were added ($240M in equipment alone)
- This is not performing any useful task!

Electricity + Networking costs:
- 0.39 W/GH/s or 175 MWatt (20% of a large nuclear plant)
- @10 cent per KWh: 1 block costs 3000$ electricity (25 BTC = 6700$)

Storage:
- Blockchain today almost 70 Gbyte

Is Bitcoin Anonymous?

- Betcoin gambling site was hacked in April 2012
- 3,171 BTC were stolen in total (2902, 165, 17, and 87 BTC)
- Did not move until March 15 2013 (BTC goes up)
- Aggregated with other small addresses into one large address
- Then began a peeling chain
- After 10 hops, a peel went to Bitcoin-24,
- And in another 10 hops a peel went to Mt. Gox

in total, 374.49 BTC go to known exchanges, all directly off the main peeling chain, which originated directly from the addresses known to belong to the thief.


Alt Coins

Follow same design as Bitcoin, but with separate block chain and network
- Hundreds alternatives to Bitcoin, most of which are not very successful
- Different monetary policy
- Different proof of work or consensus mechanism
- Specific features, such as strong anonymity

08/2011: IXCoin is Bitcoin with increased reward (failed)
09/2011: Tenebrix changes proof-of-work algorithm to scrypt (failed)
  - Memory intensive algorithm resistant to mining with GPUs and ASICs
10/2011: Litecoin uses scrypt as proof-of-work and faster block generation (still alive)
Alt Coins

Today: 700+ currencies derived from Bitcoin (see http://mapofcoins.com/bitcoin)

Monetary policy:
- Freicoin: negative interest rate to encourage spending

Consensus mechanism:
- Proof-of-stake: stake currency to generate interest

Dual purpose mining:
- Primecoin: finding primes; Curecoin: protein-folding; Gridcoin: BOINC grid computing

Anonymity:
- Zerocoin/Zerocash: use zk-SNARKS

Ripple: private platform
- centralized variant for fast transactions in any currency
Open issues

Bitcoin contracts (e.g. trading digital art)

Security of Bitcoin network: why does it work?
- Sybil attack: attacker controls many nodes in network, can refuse relaying or favouring his own blocks
- Selfish mine attack

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?

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

All miners are in China
Incentives system complex
Not clear that the system will survive, but some ideas will for sure
Business

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

Financial world dislikes

- distributed control
- full transparency
- unclear governance
- uncontrolled money supply

IBM Open Ledger – Hyperledger
(public software)

Accenture, ANZ Bank, CLS, Credits, Digital Asset, Fujitsu, Initiative for CryptoCurrencies and Contracts, Mitsubishi UFJ Financial Group, State Street, SWIFT, VMware and Wells Fargo

Business

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

Financial world dislikes

- distributed control
- full transparency
- unclear governance
- uncontrolled money supply

RSCoin's radical shift from traditional cryptocurrencies is to centralize the monetary supply

University College London
Opacity: *distributed logging technology*

Strong security and privacy guarantees
- security and privacy by design

Transparency

Accountability

Safely outsource storage

Selective disclosure

---

Pointers

- [http://www.bitcoin.org](http://www.bitcoin.org)
- [http://www.blockchain.com](http://www.blockchain.com)
- [http://randomwalker.info/bitcoin/](http://randomwalker.info/bitcoin/)
- [http://bitcoinbelgie.be](http://bitcoinbelgie.be)


Financial Cryptography conference series