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
Cash

bearer instrument
off-line payments
low and medium value
privacy, coins not traceable
widely accepted

bank: risk of forgery, cost of transport
user: theft and loss, change, physical presence
government: money laundering

€/$/£ Counterfeiting

2014/5
> 17 billion notes in circulation
fraudulent: 838,000 or 1 in 20,000
+/- €800 billion genuine in 2011
new 5/10/20 € bill in May’13/Sep’14/Nov’15

UK pound: 1 in 4170 counterfeit!
1995: $15.5 million (1% digitally produced)
2005: $61 million (45% digitally produced)
Fraudulent: 1 to 2 in 10000
$1000 billion genuine in 2013
Common features e.g. $/€

Pattern detected by scanners and copiers

Payment by Instruction

Financial Institutions (clearing and settlement)

Issuer Acquirer

Communicate through account

Authorization on-line/off-line

Payment instruction (credit card slip, cheque)

Customer

Merchant
Payment by Instruction

Convenient
Reduced risk
Identify users: manual signatures, magstripe cards, smart cards
Traceable
Verification expensive:
- credit/debit card: on-line, tamper resistant modules
- check: off-line, delay, processing cost

Electronic Cash [David Chaum]

Financial Institutions (clearing and settlement)
Issuer Acquirer
Withdrawal or load
Payment (cash transfer)
Deposit on-line/off-line

Customer Merchant
Electronic Cash

Convenient, no physical presence
Reduced risk
Cost effective for low value
Untraceable and unlinkable
More expensive than traceable systems, new technology

Verification inexpensive:
- on-line: no tamper resistant modules
- off-line: reduced risk, doublespending

E-cash is not a new currency: real money (value) sits in the bank

Currencies

A way of:
- storing and remembering value (money) across time and across exchanges

“Fiat” money
- has no intrinsic value aside its value as a currency
- gold, cigarettes, mobile phone credits are not fiat currencies.

Facilitates exchange
- acts a unit of value for exchanges
- economically efficient alternative to barter (goods-for-goods) or commodity money (gold)
Currencies

**Money is like a commodity:** it may go up, down or stay the same
- laws of supply and demand: deflation, inflation, ...

**Control of supply:** who has control? Euro: European Central Bank (ECB)
**Creation/deletion:** who gets the new money? Who deletes the old money?
- give/delete money to those that already have money
- give/delete money to those that do work
- give/delete money at random, or equally to all

**Memory:** how do we make sure we will always remember who has how much money?

**Initial allocation:** If money is like a good: how do we bootstrap it? Who has it to start with? (does it matter?)

---


---

Early examples:
**MojoNation (2000-2002) and BitTorrent**

**MojoNation**
- Peer-to-peer file storage service paid with “Mojo”
- Employed Bram Cohen (BitTorrent) and Zooko
- Collapsed under hyperinflation

**BitTorrent**
- Simplification of MojoNation
- One can think of BitTorrent’s tit-for-tat incentives as being **time-limited, file-specific,** and **non-transferrable** bilateral accounting
- No need for “full” currency

- 1 million user accounts by 2002
- centralized ledger of transactions
- currency backed by real commodity, gold
- network of international e-gold resellers

Becomes a crime magnet: difficult to identify customers yet easy to transfer internationally
- US Patriot Act (2001) requires money transmitters to be regulated
- In 2008 directors face charges of money laundering and operating without a license. They are found guilty and get away with fines, and suspended sentence.

Asserts liquidated: $90M in gold (more than the central banks of bottom 1/3 countries)
- California (2010) and other states: all digital value transfer systems are money transmitters

Risk of centralized system out of control

Centralized systems backed by a nation state

- manage the initial allocation
  - bootstrap through coercion or taxation or buying power of state
- create a constituency to allocate new money
- manage the money supply
  - it has to come from somewhere
  - credibility and legitimacy to not abuse the supply
- maintain the ledger of who holds what amount
  - fabricate and issue unforgeable coins or notes

David Graeber. **Debt: The First 5,000 Years.** Melville House.
What is Bitcoin?

from the original email announcing the system:

- Double-spending is prevented with a peer-to-peer network
- No mint or other trusted parties
- Participants can be anonymous
- New coins are made from Hashcash style proof-of-work
- The proof-of-work for new coin generation also powers the network to prevent double-spending

Hashcash: idea of Adam Back: find numerically small hash value

What is Bitcoin?

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)... but see e.g.

ACM Conference on Computer and Communications Security 2014: 15-29
What is Bitcoin?

- Maintaining public decentralized ledger (block chain)
- Of transactions that transfer value (bitcoin) from
  - one or more “senders” or inputs
  - to one or more “recipients” or outputs
  - protected by a digital signature
- Integrity of ledger is secured by miners
  - audit transactions
  - use proof-of-work to arrive at consensus about the transactions
  - successful miner receives reward creating new bitcoin

History of Bitcoin

- 31/10/2008: Satoshi Nakamoto publishes paper “Bitcoin: A peer-to-peer electronic cash system”
  - decentralized "proof-of-work" algorithm to
  - conduct a global "election" every 10 minutes
  - to arrive at consensus about the state of transactions
  - solving double spend problem
- 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”
History of Bitcoin

June 2012: massive devaluation

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 inappropriately transferred to a single account

August 2013: bug in Random Number Generator in Java on Android results in theft of Bitcoins

April 2014: Mt. Gox liquidated

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

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.

Market price in USD
Market Capitalization

2011 bubble

Bitcoin Ledger

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

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

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

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

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

Transactions
- Transaction 1
- Transaction 2
- Transaction 3
- Transaction 4
- .......
Mining and Proof-Of-Work

Transactions in a block are hashed and assembled in a Merkle tree
- hash function used is double SHA-256, so SHA-256(SHA-256())

Header then consists of
- previous block header hash
- timestamp
- difficulty level
- Merkle tree root
- nonce

Mining: finding a nonce such that the double hash of the header results in a hash value lower than the difficulty level, e.g. a double hash value starting with loads of zeros.
- currently 68 zeros are required

The first transaction in a block is a coinbase transaction
- transfers reward + all transaction fees to the miner

Mining Rewards

Total number of Bitcoins is limited to 21 million, each divided in 8 decimal places leading to $21 \times 10^{14}$ units

Figure by Chris Pacia
Mining Difficulty Level

Target: mining 1 block should take roughly 10 minutes
- mining computing power changes over time
- update level every 2016 blocks

![Difficulty Graph]

Mining Hash Rate of Bitcoin Network

![Hash Rate Graph]
Mining Hash Rate of Bitcoin Network

5.10^{17} \text{ Hash/sec} = 2^{58} \text{ /sec or } 2^{75.2} \text{ /day}
Miners check for double spending before including a transaction.

Miners broadcast a new valid block to their neighbours immediately, who then propagate it to some of their neighbours etc....

The block chain normally is one long chain.

Distributed nature of the network can lead to forks:

- Miners choose on which of 2 possible extensions to work.
- Longest chain will become the main chain, transactions in orphan blocks are rebroadcast.
- The more block that follow the harder it becomes to change a particular block.
- Transaction is typically accepted after it is included in 6 blocks (60 minutes).
Cost of Leaderless Consensus

Hidden consensus protocol:
- whichever coalition deploys most hash power, has control of the block chain
- 450,000,000 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 (10% of an average nuclear plant)
- @10 cent per KWh: 1 block costs 3000$ electricity (25 BTC = 6700$)

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

Bitcoin Crypto

Hash functions:
- SHA-256:
  - Computing ID of block (double hash)
  - Hashing transaction before it is digitally signed (double hash)
  - Computing address given public key or script
- RIPEMD-160:
  - Computing address after SHA-256 to get 20-byte result

Digital signature algorithm:
- ECDSA-SHA256 using curve $y^2 = x^3 + 7$ modulo $p$ where $p = 2^{256} - 2^{224} - 2^{192} - 2^{96} + 1$
- Private key: 256-bit scalar $k$, Public key: point $[k]G$ on the curve $E$, with $G$ base point
- Signature consists of two scalars $(r,s)$ each having max 256 bits
- Can be verified using public key $[k]G$ and the message $m$ that was signed
Bitcoin Address (P2PKH)

The simplest form of Bitcoin address is Pay-to-Public-Key-Hash (P2PKH)

- Public key is point \( Q = (x_Q, y_Q) \) on the elliptic curve \( E \)
- Can be represented as:
  - Uncompressed form \( 04 \ ) || \( x_Q \) || \( y_Q \)
  - Compressed form \( 02 \ ) || \( x_Q \) if \( y_Q \) is even or \( 03 \ ) || \( x_Q \) if \( y_Q \) is odd
- Bitcoin address is derived as RIPEMD160(SHA256(public key representation))

Example:
- point \( P = 02 \ c1f66af6f1aee1b1d28d3bb36039453269fa7bdcd5c5a3bd473212c85acdfcd \)
- Gives RIPEMD160(SHA256(P)) = eb21d8090ba7b3323aaa001d55a3c86b1199277

20-byte result is then encoded using Base58Check encoded (version byte 00 for mainnet)

Example: bitcoin address 1NSGLbVWJW1b2hMGQ3oHwpq2jut7N7XfV0

Bitcoin Script

Script is simple scripting system that is stack-based

- List of instructions that has to be satisfied when claiming an output of a transaction

Occurs in two places in a transaction:
- In an output: called the pubKeyScript, has to be satisfied to claim the value
- In an input: called the scriptSig, a proof that satisfies the pubKeyScript

Simplest example: pay to Pay-to-Public-Key-Hash

- pubKeyScript is of form OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
- scriptSig is of form <sig> <pubKey>
  - Sig is a signature computed using the private key (corresponding to the public key)
Bitcoin Script

The value in an output can be claimed if the input that refers to it leads to a valid script

- Consisting of the concatenation of the scriptSig and pubKeyScript
  
  \[
  \langle \text{sig} \rangle \langle \text{pubKey} \rangle \text{ OP\_DUP OP\_HASH160 } \langle \text{pubKeyHash} \rangle \text{ OP\_EQUALVERIFY OP\_CHECKSIG}
  \]

- \( \langle \text{sig} \rangle \langle \text{pubKey} \rangle \): The signature and pubKey are pushed onto stack
- \text{OP\_DUP}: The pubKey is duplicated
- \text{OP\_HASH160}: The copy of the pubKey is hashed using RIPEMD160(SHA256()) and put onto the stack
- \( \langle \text{pubKeyHash} \rangle \): The pubKeyHash is pushed onto the stack
- \text{OP\_EQUALVERIFY}: the top two items are the stack are popped and compared; if not equal, script is not valid
- \text{OP\_CHECKSIG}: the signature is verified using the pubKey
  - The signature was computed using ECDSA-SHA256 on the SHA256 hash of a serialized form of the transaction

Bitcoin Transaction

List of Transaction Inputs:

- Hash of block where this input occurred as output
- Index of this output
- scriptSig: a proof that you can claim the value contained in the output

List of Transaction Outputs:

- Value
- pubKeyScript: describes the conditions that have to be fulfilled to claim the bitcoins (when it is used as an input for a new transaction)
Number of Transactions Per Day

Large share goes to a few addresses

1041 per 10 minutes or 1.7 per second

Guestimate for card payments: a few 10,000 per second?
Bitcoin Address (P2SH)

The Script language can be used to express more complicated conditions than simple P2PKH

- The pubKeyScript looks like OP_HASH160 <scriptHash> OP_EQUAL
- scriptHash is the RIPEMD160(SHA256()) hash of a whole Script program
- that has to be satisfied to claim the value of the output
- The scriptSig is of the form “signatures” <serialized script>
  - “signatures” is a script containing digital signatures such that the combined scriptSig || pubKeyScript is a valid script

  “signatures” <serialized script> OP_HASH160 <scriptHash> OP_EQUAL

- Note: the output only contains the hash of the serialized script
  - Serialized script has to be given in the scriptSig
  - A P2SH is the BaseCheck58 encoding of the hash (version byte 05)
  - Example: 35Y8rz2wTPHvk4cJB5hWHDi5Aqi9gm3csV

Multi-signatures

Expresses that value can be claimed when M-out-of-N signatures are provided in the scriptSig

Public key is derived from the following script using RIPEMD160(SHA256()):

OP_m <pubKey1> ... <pubKeyn> OP_n OP_CHECKMULTISIG

The scriptSig then is of the following form:

OP_0 <signature1> ... <signaturem> OP_m <pubKey1> ... <pubKeyn> OP_n OP_CHECKMULTISIG

Use case: 2-out-of-3

- Escrow and dispute mediation
- Buyer and seller do not trust each other, so involve a 3rd party called mediator
- Buyer pays to a 2-out-of-3 address using public keys of the 3 parties involved
- If buyer is happy, provides one signature, and seller can claim bitcoins
- Otherwise mediator decides who gets bitcoins (or which part of it)
Bitcoin Wallet

Payment associated to key pair (pay with digital signature)

Loss of signing key means loss of BTC

**Secure key storage**
- Software: if hacked, loss of BTC
- Exchange and wallet service: can also be hacked or corrupt insider risk
- Hardware: growing interest

Bitcoin Wallet

Public ledger allows to trace back any transaction to a coinbase transaction
- Anonymity of transactions is not guaranteed

Avoid re-use of addresses (and thus public keys)

BIP32 + BIP44 proposal: hierarchical deterministic wallet
- Use each address only once
- Construct tree like structure of public keys derived from single master secret
- Private and public keys are “extended” with a chain code
- “Normal” child public key can be derived from parent **public** key, index and chain code
- “Hardened” child can only be derived from parent **private** key, index and chain code
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.

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 (Oct’15: 45 Gbyte!)
- Authoritative one is the longest – race for aggregate CPU power

Who has it to start with? (Does it matter?)
- Satoshi Nakamoto

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)

Today: 716 currencies derived from Bitcoin (see http://mapofcoins.com/bitcoin)
Alt Coins

Monetary policy:
- Litecoin: block every 2.5 minutes, 84 million coins by 2140, scrypt as proof-of-work
- Dogecoin: block every 60 sec, $10^{11}$ coins by 2015, scrypt as proof-of-work
- Freicoin: negative interest rate to encourage spending, block every 10 minutes, SHA256 proof-of-work

Consensus mechanism:
- scrypt, scrypt-N, Skein, Groestl, SHA3, X11, Blake, or a combination of these
- Proof-of-stake: stake currency to generate interest
- Peercoin, Myriad, Blackcoin, VeriCoin, NXT (not Bitcoin derivative)

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

Anonymity:
- Zerocoin/Zerocash: use zk-SNARKS; CryptoNote: using traceable ring signatures
- Darkcoin: re-mixing + multi-algorithm POW (X11)

Further Topics

Bitcoin contracts (e.g. trading digital art)

Security of Bitcoin network:
- 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?