Introduction to Bitcoin I 

P Peterlongo[1] A Tomasi[1]

[1]University of Trento
Department of Mathematics

June 10, 2013

UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

Outline

1. Fiat money and online payments
   - Functions of money
   - Online payments and cost of clearing
2. Bitcoin
   - What is it?
   - (Cryptographical Hash Functions)
   - How it works
   - Security aspects
3. Conclusions
   - Some reflections
   - (We have not covered a lot of stuff)

fiat and digital money

- the currency we use today is fiat money: its value is entirely determined by government policy and law
- it is not a commodity (like gold) or representative of commodities (since 1971)

3 functions of money:

- medium of exchange
- unit of account
- store of value

digital currencies and online payments

How are online payments made?

- you ask for a payment to be done giving some credentials
- the system accepts the payment checking your credential
- in a second moment the payment is cleared passing through a central clearinghouse (which uses a ledger)

this involves a trusted third party and implies some *cost of clearing*.

Note that in this context a digital euro is just a bit of information passed along. The problem is not anymore forgery, but avoid double spending of the money (or spending money you do not have).

bitcoin: native digital

Bitcoin

It is the first decentralized digital currency.

- Digital: it is just a record of transactions (a ledger).
- Decentralized: the ledger is public;
  validation of the ledger is made by a peer-to-peer network.

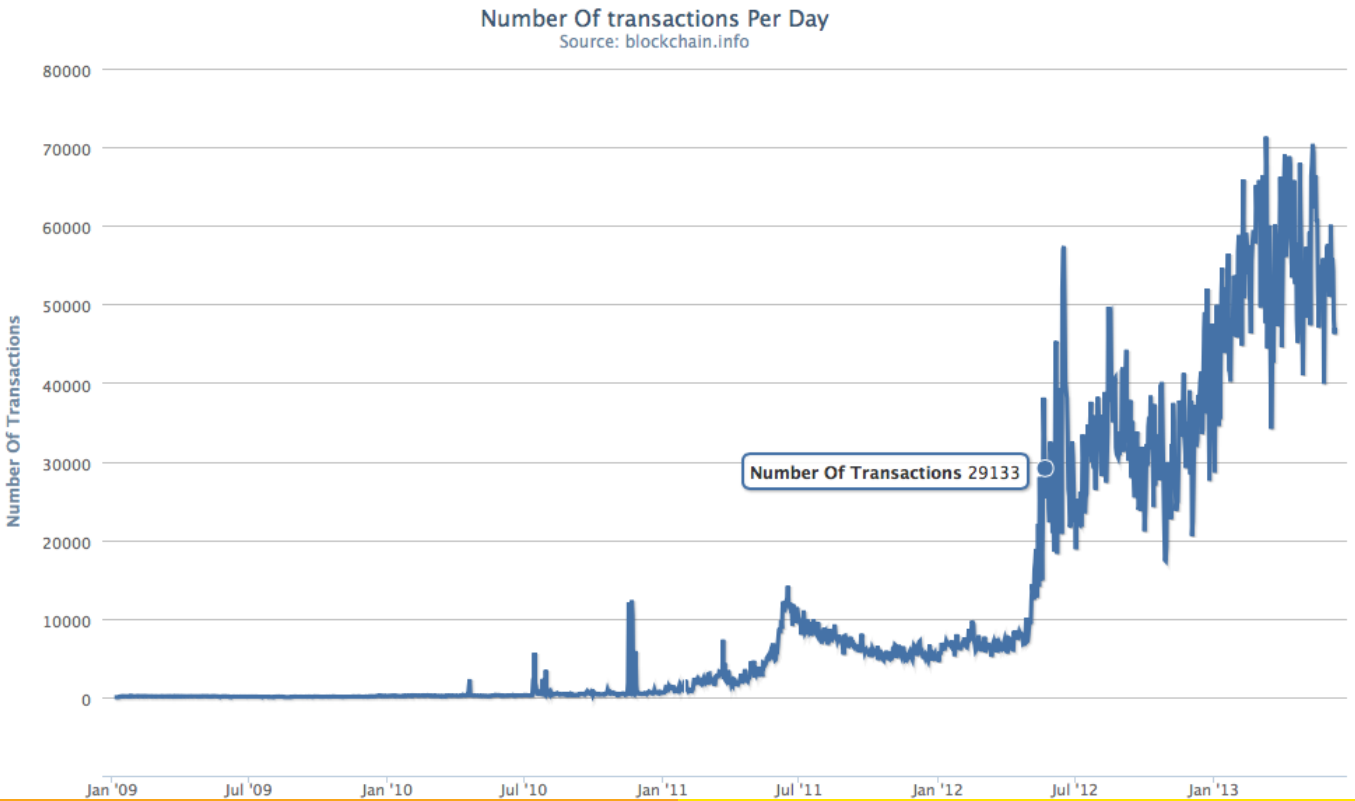
Advantages from an online payment point of view:

- a native digital (modelled on the internet)
- low (even zero) transaction fees and easy to set up

the Blockchain

Bitcoin's public ledger is called the Blockchain:

- it contains all transactions of bitcoins
- it is validated every 10 minutes with new transactions
- during validation process new bitcoins are created



bitcoin is a cryptocurrency

Bitcoin is based on cryptography. Two main ingredients are:

- Cryptographical Hash Functions
- ECDSA: Elliptic Curve Digital Signature Algorthm

jgarzik
Staff
Hero Member

Posts: 2750

Ignore

Re: i want to understand
December 28, 2010, 12:36:28 AM

#3

The entire system is not based on encryption, but public/private keypairs, and cryptographic signatures.

Each time you spend bitcoins, you are creating a cryptographically-signed transaction that says "transfer 1234.56 bitcoins to public key ABCD."

Only the person with the private key ABCD can then spend those 1234.56 BTC.

Jeff Garzik, bitcoin core dev team

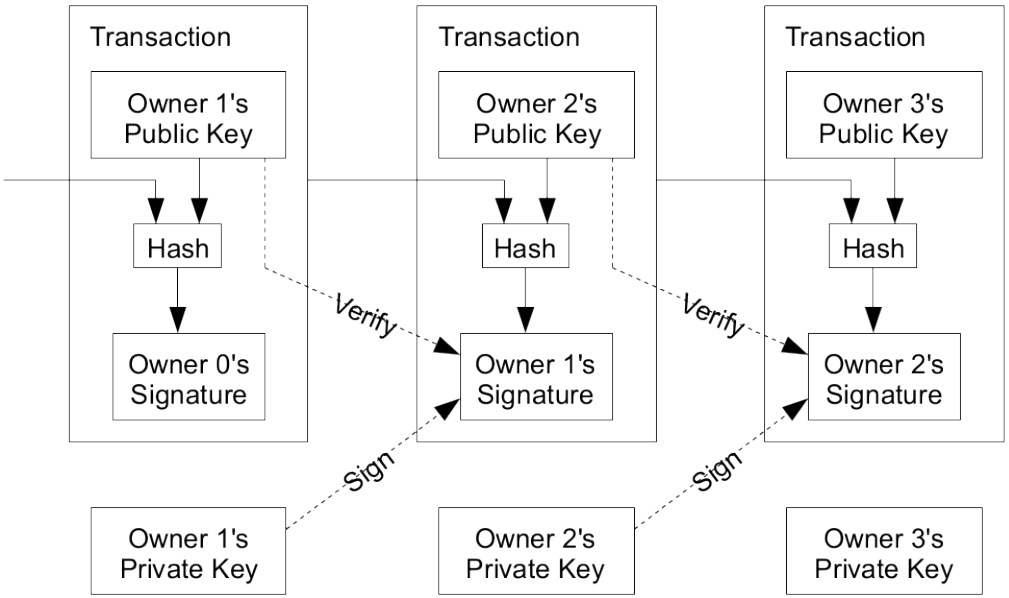
Donations / tip jar: 1BrufViLKnSWtuWGkryPsKsxonV2NQ7Tcj

taken from `bitcointalk.org`

what is a digital coin?

Satoshi Nakamato, 1998:
"We define a digital coin as a chain of digital signatures"

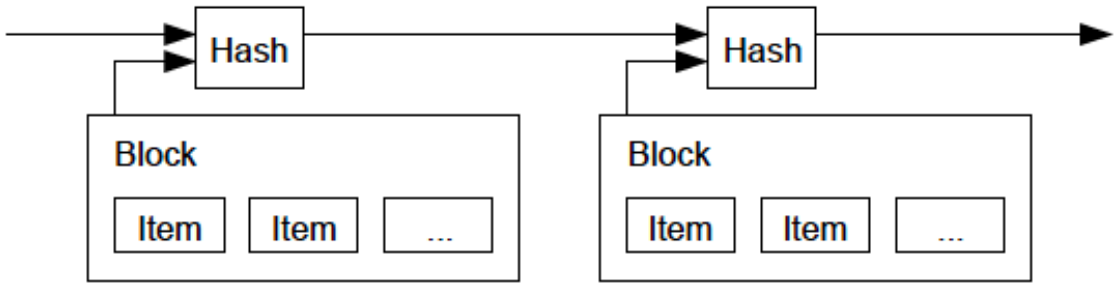
- a coin is defined by the list of its transactions up to know (change of ownership)
- proof of ownership is (usually) given by digital signature of transaction by last owner



we will see what a digital signature is in next presentation.

Timestamping transactions

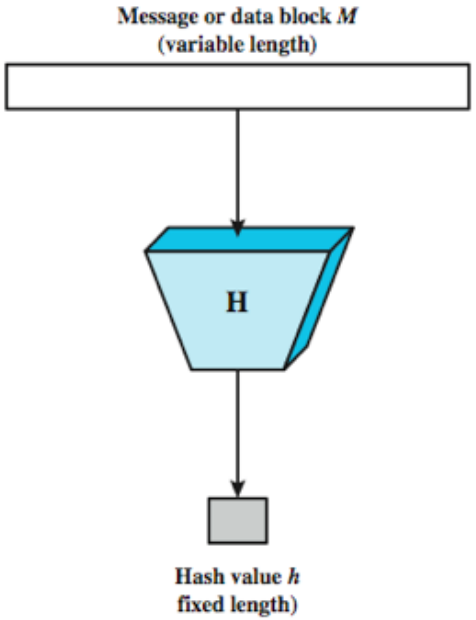
A timestamp server takes a hash of a block of items to be timestamped and widely publishing the hash. The timestamp proves that the data must have existed at the time in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a *chain*, with each additional timestamp reinforcing the ones before it.



This shared public transaction log is called the *block chain*.

Cryptographical Hash Functions

A hash function takes as input an arbitrary length string and outputs a fixed length digest.



cryptographical hash functions

- are very difficult to 'invert' (difficulty is measured in computation time)
- their output looks randomly generated

Bitcoin protocol uses SHA-256 hash function to provide proof-of-work concept used to validate transactions.

Output example of SHA-256

SHA-256 outputs a 256-bit strings

input: "Edward Snowden is PRISM whistleblower"

output:

48FCB0286DFF720812402010EFCA0A3121BBCE61BA0A121B591756D3B487B8B3

input: "Edward Snowden is PRISM whistleblower [00]"

output:

7C8AC6BFA2315E7AC4D11F8986B677F29173BA86955DE37341FE311761D93E24

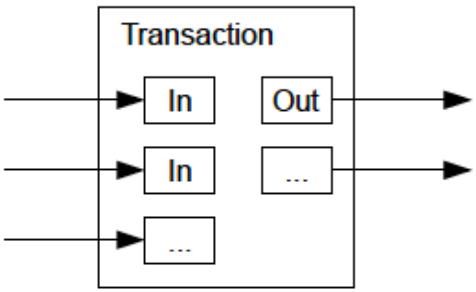
input: "Edward Snowden is PRISM whistleblower [12]"

output:

0D97B5BE09152D3610F5D5F0079A46957E3951CAD8077F495D1AB150C107ED9D

more on SHA-256 later. [nonce,proof-of-work]

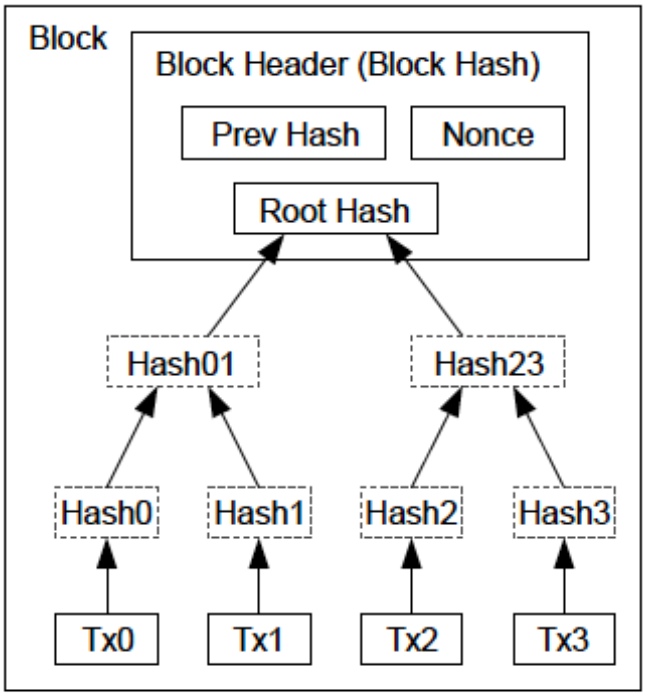
Transactions



A transaction is a record of where is money coming from, where it is going and how much is being transferred. It may have multiple inputs or outputs.

hash:
`9c809ffd57fe160b7a5504f0ff9ec2beb3f491fd3eb88d548d56399b7b8bd4db`
inputs (1):
amount: 100 from (address): `1PgMst4c11hPpuYQeqRPTCjMv9Z8CmLus4`
scriptSig:
`3045022100804 4adfa98b5bd83f2ec0852e8c5aa7b5e226924b475be32...`
outputs (1):
amount: 100 to (address): `16MgZaATWXrAgDB3Q9evULCHATWrmbxmUt`
scriptPubKey: `...3ac1f8f5cb7ab8ed6d2d5dc1d295ec3e1d00dbd6 ...`

Blocks



Transactions Hashed in a Merkle Tree

A block contains a list of transactions (with their hashes) and a block header which contains:

Prev Hash:
000000000001978...
Merkle Root:
e39d3f5dea...
Nonce:
1277352253

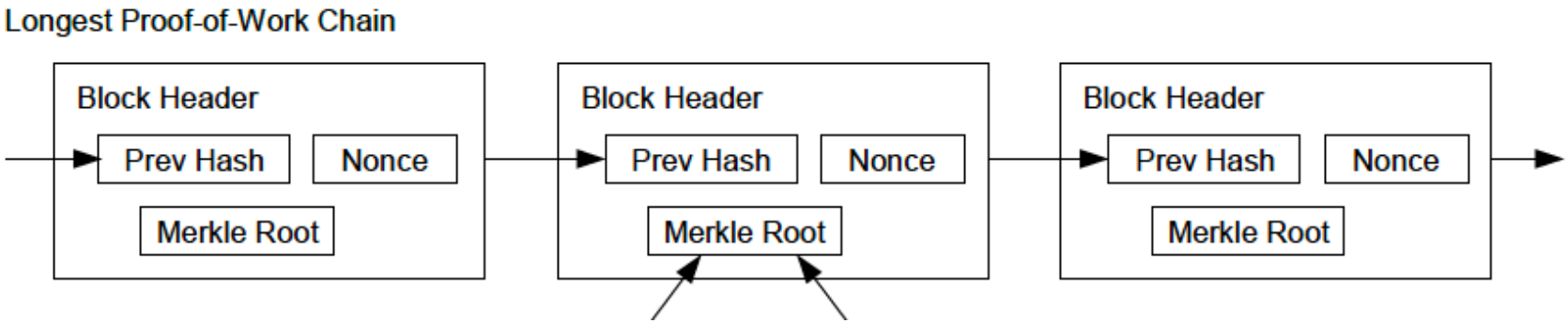
Hash of Block header:

000000000000003f522c0efba7648a8940055555b8738a2820b26d9a1603d5577

Proof-of-work

The proof-of-work system:
we increment a nonce in the block until a value is found that gives the block's $(\texttt{SHA-256})^2$ a specified number of zero bits at the beginning.

The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.



Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work

The Bitcoin Network

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Bitcoins are successfully collected by the receiving node which found the proof-of-work. This includes "mining" and voluntary transaction fees.
6. Nodes accept the block only if all transactions in it are valid and not already spent.
7. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Honesty of the Network

A majority of honest nodes is essential to prevent an attack based on the control of the majority of computing power.
It would enable to:

- reverse transactions that the attacker does while in control.
- prevent some or all transaction to get confirmed
- prevent some or all miners to mine valid blocks

It would *not* enable to:

- reverse/modify other people's transactions
- prevent transaction from being sent
- create/steal coins

SHA-256 security

Breaking SHA-256 means that it will take less time to validate a block, thus making easier to control majority of CPU power.

SHA-256: Security Hash Algorithm is approved by NIST, belongs to the family SHA-2.
Complexity (measured in bits of security) of finding a collision, i.e. two strings that HASH to the same value (brute force, best attack):

SHA1	$k = 80$	$k = 58$
SHA256	$k = 128$	$k = 128$
SHA3	$k = 128$	$k = 128$

The structure of SHA-2 is quite similar to SHA-1, so we expect similar vulnerabilities to be found; SHA-3 on the other hand is entirely different and expected to be much more robust.

Some reflections

Bitcoin is

- a fascinating experiment
- a concrete example of a (possible) future online payment protocol
- a seed for innovation

We have not covered

3 aspects we have not treated but which contributed essentially to adoption of bitcoin.

- Mining
- Payment protocols
- Privacy
- Regulations