What can Bitcoin teach us?

Seminari di Cultura Matematica

Dr. Matteo L. BEDINI

Numerix, Financial Engineering – EMEA

Milano, 11 April 2017

Disclaimer

The opinions expressed in the following slides are solely of the author and do not necessarily represent those of the current (or past) employer(s).

How much do you already know about Bitcoin?

A small quiz for the audience

	True	False
Bitcoin is anonymous	□	□
bitcoins are money	□	□
In Bitcoin protocol, cryptography is used for encrypting transactions	□	□
Bitcoin wallets contain bitcoins	□	□

How much do you already know about Bitcoin?
The “correct” answers are...

	True		False
Bitcoin is anonymous	□		☒
bitcoins are money	□	X	□
In Bitcoin protocol, cryptography is used for encrypting transactions	□		☒
Bitcoin wallets contain bitcoins	□		☒

Main goals and some references

The goals of this presentation are:

- Providing a brief overview of the Mathematics underlying the Bitcoin protocol – [An, S].
- Providing a preliminary, technical understanding of the Bitcoin protocol – [N, Ni].
- Discussing some aspects about the economy sparked by the adoption of bitcoins – [Am].
- Discussing the cultural novelty introduced by Satoshi Nakamoto.

Why this particular choice?

This proposal is limited by the author's knowledge and experience: it's up to you to go and look for what mostly suits your interests. The aim of the author is to spark curiosity in the audience without claiming the ability of satisfying all possible questions.

Outline

1. Mathematical Preliminaries
    - One-way Functions – SHA256
    - Asymmetric Cryptography
    - Hash Functions and Public-Key Cryptography for Signing Documents

2. The Bitcoin Protocol
    - Re-inventing a P2P Payments Protocol Avoiding Double Spending
    - Bitcoin and bitcoins
    - Are bitcoins Money?

3. Conclusions and References
    - Conclusions
    - References

Outline

1. Mathematical Preliminaries
   - One-way Functions – SHA256
   - Asymmetric Cryptography
   - Hash Functions and Public-Key Cryptography for Signing Documents
2. The Bitcoin Protocol
   - Re-inventing a P2P Payments Protocol Avoiding Double Spending
   - Bitcoin and bitcoins
   - Are bitcoins Money?
3. Conclusions and References
   - Conclusions
   - References

Functions that are easy to compute but hard to invert

- Ex: "[...] *It is easy to disassemble a watch into hundreds of minuscule pieces. It is very difficult to put those tiny pieces back together into a working watch* [...]" [S].
- "[...] *If we are being strictly mathematical, we have no proof that one-way functions exist, nor any real evidence that they can be constructed* [...] *Even so, many functions look and smell one-way: We can compute them efficiently and, as of yet, know of no easy way to reverse them*. [...]" [S].
- Trap-door functions: one-way functions that can be easily inverted if you know a secret (the assembly instructions of the watch).
- Hash-functions:
  - Deterministic – The hash function is public and deterministic; there's no secrecy nor randomness in the process.
  - One-way – The output is not dependent on the input in any discernible way.
  - Optional but recommended – Variable-size input, fixed-size output.

SHA256 – Nonce

```
SHA256("Hello, world!0") =
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

SHA256("Hello, world!4250") =
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Public-key K for encryption, Private-key k for decryption

"[...] *Encryption is the easy direction. Instructions for encryption are the public key; anyone can encrypt a message. Decryption is the hard direction. It's made hard enough that people with Cray computers and thousands (even millions) of years couldn't decrypt the message without the secret. The secret, or trapdoor, is the private key. With that secret, decryption is as easy as encryption* [...]" – [S].

1) Alice gets Bob's public key from the database → 2) Alice encrypts her message using Bob's public key and sends it to Bob → 3) Bob then decrypts Alice's message using his private key.

The NIST `secp256k1` standard curve used in the Bitcoin protocol is defined by the following function, which produces an elliptic curve:

$$y^2 \mathrm{mod} p = (x^3 + 7) \mathrm{mod} p,$$

where $\mathrm{mod} p$ (modulo prime number p) indicates that this curve is over a finite field of prime order p, where $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$, a very large prime number – [An].

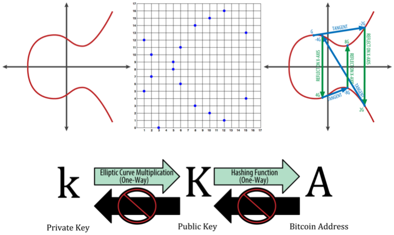


Figure: Elliptic curves and Bitcoin. One-to-one (but not invertible) relation between keys and address [An].

Digital Signature – [S]

The Signing Protocol:

1. Alice produces a one-way hash of a document & timestamp.
2. Alice encrypts the hash with her private key, thereby signing the document.
3. Alice sends the document and the signed hash to Bob.
4. Bob produces a one-way hash of the document that Alice sent. He then, using the digital signature algorithm, decrypts the signed hash with Alice's public key. If the signed hash matches the hash he generated, the signature is valid.

Features:

1. The signature is **authentic**; when Bob verifies the message with Alice's public key, he knows that she signed it.
2. The signature is **unforgeable**; only Alice knows her private key.
3. The signature is **not reusable**; the signature is a function of the document and cannot be transferred to any other document.
4. The signed document is **unalterable**; if there is any alteration to the document, the signature can no longer be verified with Alice's public key.
5. The signature **cannot be repudiated**. Bob doesn't need Alice's help to verify her signature.

Outline

1. Mathematical Preliminaries
   - One-way Functions – SHA256
   - Asymmetric Cryptography
   - Hash Functions and Public-Key Cryptography for Signing Documents
2. The Bitcoin Protocol
   - Re-inventing a P2P Payments Protocol Avoiding Double Spending
   - Bitcoin and bitcoins
   - Are bitcoins Money?
3. Conclusions and References
   - Conclusions
   - References

How to Use Digital Signature

> "[...] *Digital signatures provide part of the solution* [...]" [N]

Basic information	"I, Alice, am giving Bob one bitcoin"	
Better	"I, Alice, am giving Bob one bitcoin"	+ Alice's digital signature
Even Better	"I, Alice, am giving Bob the bitcoin # 123654"	+ Alice's digital signature
The Best	"I, Alice, am giving Bob the bitcoin # 123654" 20180411T112043Z	+ Alice's digital signature

Who's printing serial the serial number 123654? A bank certifying that:

1. bitcoin #123654 actually belongs to Alice
2. Alice hasn't yet spent the bitcoin #123564

hence guaranteeing and authorizing the transaction from Alice to Bob?

Why Using a Public Ledger

> "[...] *the main benefits are lost if a trusted third party is required to prevent double spending* [...]" [N]

Idea: everybody is a bank thanks to a public ledger called **blockchain**.

Bob, before accepting a payment from Alice, has to

1. check his own copy of the blockchain
2. broadcast the transaction on the Bitcoin network.

When *enough users* (50? 50%?) will have *confirmed* (?) the transaction, this will be actually registered on Bob's account.

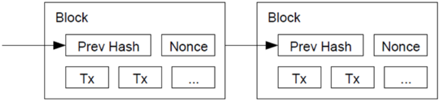
Two problems remain to be solved:

1. Who's printing serial numbers on bitcoins?
2. Double-spending cannot be difficult, it must be practically impossible.

The Role of Seignorage

> “[...] *The network timestamps transactions by hashing them into an ongoing chain of hash-based* **proof-of-work**, *forming a record that cannot be changed without redoing the proof-of-work* [...]” [N]

- Validating transaction is computationally costly (find the Nonce).
- Reward (today 12.5 BTC) for the user validating a block.



Mining: 1 CPU = 1 vote

1. Check block's transaction integrity.
2. Find the nonce satisfying a given target (number of leading 0s).
3. Broadcast on Bitcoin block + nonce.

Consensus for the Most Powerful

> "[...] **The longest chain** *not only serves as a proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU available* [...]" [N]

- Every block points to the previous one (from which then name: blockchain).
- Forks may occur whenever two blocks are simultaneously validated.
- Keep track of the forks, but always work on the longest chain.
- A transaction is confirmed when 5 other blocks are validated after its block on the longest chain.

A Self-Enforcing Mechanism

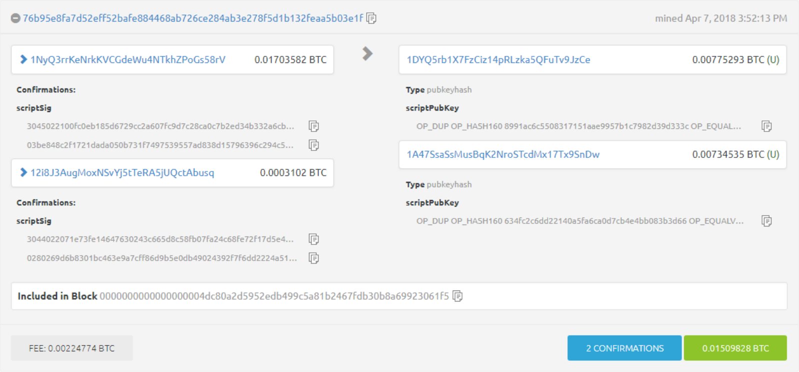
> "[...] *As long as a* **majority of CPU power** *is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace the attackers* [...]" [N]

Problem of Double-Spending: how to do it?

1. Two transactions TxB and TxC in the same block B? NO. Even if Alice validates B, other network users will not.
2. Transaction TxB in block B1 and transaction TxC in block B2? NO. Even if Alice validates and broadcast the two blocks, only one of the two blocks will be part of the blockchain (i.e., the one reaching the pool of miners with greater computing power).
3. Alice waits for Charlie accepting the transaction, goes back of 6 blocks, forks the blockchain and try to outpace it with her new branch. **OK only if Alice (alone) has at least the 51% of computing power of the whole network**.

Addresses, Transactions, bitcoins and Wallets

The transfer of bitcoins from some addresses to some others is enabled by the solution of a puzzle involving the related keys. A wallet is a container of the private keys associated to the input addresses.



76b95e8fa7d52eff52bafe884468ab726ce284ab3e278f5d1b132feaa5b03e1f

mined Apr 7, 2018 3:52:13 PM

1NyQ3rrKeNrkKVCGdeWu4NTkhZPoGs58rV 0.01703582 BTC

Confirmations:

scriptSig

3045022100fc0eb185d6729cc2a607fc9d7c28ca0c7b2ed34b332a6cb...

03be848c2f1721dada050b731f7497539557ad838d15796396c294c5...

12i8J3AugMoxNSvYj5tTeRA5jUQctAbusq 0.0003102 BTC

Confirmations:

scriptSig

3044022071e73fe14647630243c665d8c58fb07fa24c68fe72f17d5e4...

0280269d6b8301bc463e9a7cff86d9b5e0db49024392f7f6dd2224a51...

1DYQ5rb1X7FzCiz14pRLzka5QFuTv9JzCe 0.00775293 BTC (U)

Type pubkeyhash

scriptPubKey

OP_DUP OP_HASH160 8991ac6c5508317151aae9957b1c7982d39d333c OP_EQUAL...

1A47SsaSsMusBqK2NroSTcdMx17Tx9SnDw 0.00734535 BTC (U)

Type pubkeyhash

scriptPubKey

OP_DUP OP_HASH160 634fc2c6dd22140a5fa6ca0d7cb4e4bb083b3d66 OP_EQUALV...

Included in Block 0000000000000000004dc80a2d5952edb499c5a81b2467fdb30b8a69923061f5

FEE: 0.00224774 BTC

2 CONFIRMATIONS

0.01509828 BTC

Figure: A transaction as a double-entry bookkeeping with optional input (https://blockexplorer.com/tx/76b95e8fa7d52eff52bafe884468ab726ce284ab3e278f5d1b132feaa5b03e1f).

The result is an online system that does not need trusted third party for transferring a scarce asset

- **Bitcoin** is a peer-to-peer protocol enabling transaction in **bitcoins**.
- The **blockchain** is a resilient WORM[1] data-structure implementing a **distributed ledger**, the ledger of transactions.
- **Mining** bitcoins:
  - Starting from 2009, 50 BTC are generated and given to those who validate a block.
  - This amount halves every four years (today: 12.5 BTC).
  - This is the only way of creating new bitcoins.
  - In 2140 there will be 21 mln of bitcoins and the total supply of bitcoins will cease to grow.
- **Computing power** can either support or destroy Bitcoin, but the **self-enforcing mechanism design of the protocol** revenues CPU support to the project with **seignorage fee**.

[1] Write Once Ready Many

Value, Coin, Money, Commodities

How to asses the value of a “medium of exchange”?

LVDOVICVS·XIII·D·G·FR·ET·NAV·REX
SIT·NOMEN·DOMINI·BENEDICTVM·1643

Figure: AR Douzième d’Écu (21mm, 2.26 g). Paris mint, dated 1643. Formally 967/1000 of silver, 1/12th of ecu, Turkish women in 1660-1670 settled a bid price at twice its face value. See [C, La truffa del secolo (XVII), pp. 51-62].

What is “Money”?

Goals of using money:

- Medium of exchange
- Unit of account
- Way to settle a debt (standard or deferred payment – legal tender)
- Store of value

	Cows	Silver Coins	Diamonds	USD	ZWL	BTC
Interchangeability	☹☹	☺	☺☺	☺☺☺	☺☺☺	☺☺☺
Durability	☹☹	☺	☺☺☺☺	☺☺☺	☺	☺☺☺
Portability	☹	☺	☺	☺☺	☺☺	☺☺☺☺☺
Cognizability	☹☹	☺	☺☺	☺☺☺☺	☺	☺☺
“Stability” of Value	☹☹	☺	☺☺	☺☺	☹☹☹	☺?

Table: A brief overview of different system of payments.

Are bitcoins money? And if so, which one?

Money in history:

- **Commodity Money**: finite and chaotic supply of the metal. Difficult assessment of the alloy quality.
- **Representative Money**: more controllable supply of the precious metal, easier rebasement. 15 August 1971: end of gold-USD conversion.
- **Fiat Money** (see, e.g. ECB monetary aggregates):
  - M1: monetary base (is the sum of currency in circulation and overnight deposits).
  - M2, M3: everything else.

  Roughly speaking, M1 is a little bit less than 10% of the total[2].

What about bitcoins? Two, possibly equivalent, considerations

bitcoins might be considered:

- internet-based M1 with finite, inelastic, deterministic supply.
- digital gold (see [Am]).

[2] Author's personal estimate

Outline

1. Mathematical Preliminaries
   - One-way Functions – SHA256
   - Asymmetric Cryptography
   - Hash Functions and Public-Key Cryptography for Signing Documents

2. The Bitcoin Protocol
   - Re-inventing a P2P Payments Protocol Avoiding Double Spending
   - Bitcoin and bitcoins
   - Are bitcoins Money?

3. Conclusions and References
   - Conclusions
   - References

Why Bitcoin is a great cultural achievement

- Solution of the Byzantine Generals Problem:

  Generals of the Byzantine Army need to coordinate for attacking a city or retreating, but some of them are traitors...

- Implementation of a resilient transaction system:
  - almost real-time execution (though other systems are better)
  - almost real-time clearing and settlement!
- Bitcoin protocols underpins the first natively-digital scarce asset:
  - bitcoins are transferable but not duplicable
  - total amount of bitcoins is capped at 21000000

  See [Am, e.g. 1]
- Notarization services (see [Am, e.g. 4]): `https://opentimestamps.org/`.
- First cases of smart-contracts (scripting language Turing-incomplete by design).

Misunderstandings

The dark-side of the hype:

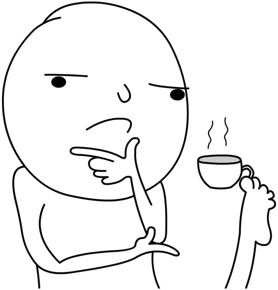
- The blockchain is a data-structure/database with cryptographic steroids. Useful in very special circumstances (mea-culpa).
- Most of other cryptocurrencies are rarely able to improve some aspects of Bitcoin. Some purpose-limited exceptions:
  - Ethereum
  - Ripple
  - Monero/Zcash
- **I**nitial **C**oin **O**ffering: are you sure you understand what you are talking about?
- Lot of frauds behind the hype: Cryptocurrencies: Last Week Tonight with John Oliver (HBO).

Not so true:

- Bitcoin is anonymous and is good for criminal activities.
- No trusted third-party is required for using bitcoins.

GRAZIE!

Everything's clear now... right?



[Am] F. Ametrano. https://speakerdeck.com/nando1970. URLs last retrieved 4 April 2018.

1. *Bitcoin as Digital Gold*. 1 February 2018.
2. *Bitcoin: The Digital Rush*. 19 January 2018.
3. *Bitcoin, Blockchain, and Distributed Ledger Technology: Hype or Reality?* 19 June 2017.
4. *Bitcoin and Blockchain Technology: Hayek Money*. 12 June 2017.
5. *Bitcoin and Blockchain Technology: An Introduction*. 27 March 2017.
6. *About Bitcoin, Blockchain, and the DLT Chimera*. 22 November 2016.
7. *Response to ESMA on DLT Applied to Securities Markets*. 1 November 2016 (jointly with E. Barucci, S. Marazzina, S. Zanero).
8. ...

[An] A. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain* – Second Edition, Second Print. 20 July 2017. URL last retrieved 4 April 2018.

[C] C. M. Cipolla. *Tre storie extra vaganti*. Bologna, Il Mulino, 2011.

[N] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 24 May 2009. URL last retrieved 4 April 2018.

[Ni] M. Nielsen. *How the Bitcoin protocol actually works*. 6 December 2013. URL last retrieved 4 April 2018.

[S] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. 2nd ed. New York: Wiley, 1996.