Why do we study Bitcoin?

Mainly interested in underlying blockchain technology

Bitcoin first & most popular blockchain application

What is our impression?

Sometimes, an inaccurate perception is created
7 Myths About Bitcoin

1. Bitcoin is money
Legal Status in European Union

Ad hoc definition ECB
“A virtual currency is a digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money.”

Medium of exchange (Ruilmiddel)
- Money
- Legal tender (Wettig betaalmiddel)
- Electronic money
## EU - Electronic Money?

<p>| European directive 2009/110/EC (Electronic money). Art.2.2  |</p>
<table>
<thead>
<tr>
<th>Definition “electronic money”</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) electronically, including magnetically, stored monetary value as represented by a claim on the issuer</td>
</tr>
<tr>
<td>b) <strong>issued on receipt of funds</strong> for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC</td>
</tr>
<tr>
<td>c) which is accepted by a natural or legal person other than the electronic money issuer</td>
</tr>
</tbody>
</table>

According to report of ECB (10/2012)  b) not applicable on virtual money such as Bitcoin. Hence, virtual money is not a form of electronic money. Followed by FSMA & NBB (Press release 14/01/2014)

### 2009/110/EC, article 11: Issuance and redeemability

“Member States shall ensure that, upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held.”

→ **No guarantee that you can get back the original value** when obtaining the virtual money (*Exchange rate fluctuations*).
Legal Status in European Union

Medium of exchange (Ruilmiddel)

→ Money

→ Legal tender (Wettig betaalmiddel)

→ Electronic money
Money

Legally
Anything widely used to exchange value in transactions

⇒ Degree of acceptance of virtual money is very low

Economically
Should hold 3 properties
1) Medium of exchange
2) Stable store of value
3) Unit of account (rekeneenheid)

⇒ No virtual currency fullfils today these criteria

Bitcoin is not money

Bron: Briefing European Parliament (March 2016): Virtual currencies – Challenges following their introductions
Legal Status in European Union

Medium of exchange (Ruilmiddel)

Money

Legal tender (Wettig betaalmiddel)

Electronic money

No legal tender
No one obliged to accept payment with virtual currencies

No deposit protection
↔ bank account, term accounts, ... (e.g. Legal protection up to € 100 000 by Guarantee Fund)

Not electronic money
No legal guarantee that you will get back the original value (Exchange rate fluctuations)
2 Bitcoin is efficient
Bitcoin Blockchain

- **Blockchain = concatenation of blocks, which contain transactions**
- **At predetermined frequency new block appended with most recent transactions**
- **blockchain contains ALL transactions**
- **Transaction in blockchain unremovable & unchangeable**
- **Many entities possess the same copy of the blockchain**

Transaction examples:
- Block 51: 5.10 BTC →
- Block 52: 0.70 BTC →
- Block 53: 0.40 BTC →
Bitcoin Mining

Winner gets reward
- New bitcoins
- Transaction fees

Disclaimer: in reality, only the header is hashed & also random value in coinbase
Miners compete with each other to solve the cryptographic puzzle of the next block.
Ecological Impact

Electricity consumption per country

> 70% in China
Weak environmental laws
Electricity subsidized

Max. capacity
4 transactions / sec.

“That’s just an inaccurate, unscientific estimate!”

https://digiconomist.net/bitcoin-energy-consumption
Difficulty adjusted every 2 weeks (2016 blocks)

Higher prices → more mining power → higher difficulty
Theoretical Minimum

Antminer S9
- "Currently the most energy-efficient miner"
- 14TH/s
- 1323W

26 335 883 TH/s
⇒ 1 881 134 Antminers S9
⇒ 2 488 740 282 Watt
⇒ 21,8 TWh / year
(Excl. cooling)

Belgium
Electricity generation 2016:
82 TWh / year
Electricity consumption 2014:
82 TWh / year

± 11 transactions per Belgian citizen per year

https://www.iea.org/media/countries/Belgium.pdf
Elimination of trusted authorities (banks) ⇞ More efficient
3. Bitcoin has perfect security
A Sophism...

“Bitcoin already exists 9 years, which proves that it is secure”

Counterexample
WPA2 available since 2004
Proven to be secure
Broken in October 2017
by KU Leuven researchers (KRACK)
Security

Bitcoin is conceptually secure as long as some assumptions are met

Applicative assumptions
E.g. No miner > 50% mining power

Cryptographic assumptions
E.g. SHA-2 & RIPEMD

Mathematical assumptions
E.g. ECDSA

In crypto
- We trust that the assumptions are (and stay) correct
- Weaker assumptions → stronger solutions
- Heavier assumptions → weaker solutions
The Bitcoin protocol is secure as long as not participant has over 50% of total mining power (*).

(*) According to Decker and Wattenhofer 49.1% suffices due to stale blocks.
There is more than the Blockchain

James Howells, who works in IT, lost in 2013 7500 bitcoins by throwing away by accident an old hard disk, which contained his secret key.

Nearly 4M Bitcoins Lost Forever
Source: chainalysis.com
Risk

Central entity → individual user

Withdraw limit ✓
Card stop ✓
Refund ✓
Deal with loss ✓

→ Sometimes, we are happy that there is a central party...
Don’t forget your PIN / Password!

https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/?mbid=nl_102917_daily_list1_p1
Online Wallets

Some hacked online wallets...

Customers lost money

Manages your bitcoins
Full trust required
Bitcoin: $64m in cryptocurrency stolen in 'sophisticated' hack, exchange says

Mining marketplace NiceHash suspends operations while it co-operates with authorities over ‘professional attack’, urging users to change passwords.

Nearly $64m in bitcoin has been stolen by hackers who broke into Slovenian-based bitcoin mining marketplace NiceHash.

The marketplace suspended operations on Thursday while it investigated the breach, saying it was working with law enforcement as “a matter of urgency” while urging users to change their passwords.

The hack was “a highly professional attack with sophisticated social engineering” that resulted in approximately 4,700 bitcoin being stolen, worth about $63.92m at current prices, said NiceHash head of marketing Andrej P Škraba.
4 Bitcoin is a scarce asset, like gold
Total Amount of Bitcoins

Total amount of bitcoins created

Max. 21M bitcoins by 2040
- Not cryptographically enforced
- Just a common rule
- Rules can change
Forks

March '17

Oct. '17

Aug. '17

bitcoin

bitcoin unlimited

BITCOINGOLD

Bitcoin Cash
<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Symbol</th>
<th>Market Cap</th>
<th>Price</th>
<th>Circulating Supply</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>BTC</td>
<td>$181,214,836,784</td>
<td>$10,729,70</td>
<td>16,889,087</td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>ETH</td>
<td>$87,551,820,315</td>
<td>$894,56</td>
<td>97,871,925</td>
</tr>
<tr>
<td>3</td>
<td>Ripple</td>
<td>XRP</td>
<td>$37,735,632,299</td>
<td>$0,965234</td>
<td>39,094,802,192 *</td>
</tr>
<tr>
<td>4</td>
<td>Bitcoin Cash</td>
<td>BCH</td>
<td>$22,011,418,650</td>
<td>$1,295,56</td>
<td>16,989,888</td>
</tr>
<tr>
<td>5</td>
<td>Litecoin</td>
<td>LTC</td>
<td>$12,341,360,446</td>
<td>$222,77</td>
<td>55,400,308</td>
</tr>
<tr>
<td>6</td>
<td>NEO</td>
<td>NEO</td>
<td>$9,371,440,000</td>
<td>$144,18</td>
<td>65,000,000 *</td>
</tr>
<tr>
<td>7</td>
<td>Cardano</td>
<td>ADA</td>
<td>$8,790,262,141</td>
<td>$0,339038</td>
<td>25,927,070,538 *</td>
</tr>
<tr>
<td>8</td>
<td>Stellar</td>
<td>XLM</td>
<td>$6,810,062,729</td>
<td>$0,368748</td>
<td>18,468,066,889 *</td>
</tr>
<tr>
<td>9</td>
<td>IOTA</td>
<td>MIOTA</td>
<td>$5,308,430,320</td>
<td>$1,91</td>
<td>2,779,530,283 *</td>
</tr>
<tr>
<td>10</td>
<td>Dash</td>
<td>DASH</td>
<td>$5,078,204,941</td>
<td>$642,08</td>
<td>7,908,954</td>
</tr>
<tr>
<td>11</td>
<td>Monero</td>
<td>XMR</td>
<td>$4,834,894,443</td>
<td>$306,63</td>
<td>15,767,794</td>
</tr>
</tbody>
</table>
Each creation of a successful crypto currency ~ creation of new, rare, element on the periodic table (but with different properties)
Supply of crypto currencies theoretically unlimited
5. Bitcoin has low transaction fees
Average Transaction Fee in $

Volatile & unpredictable
Based on supply & demand
Based on size (in bytes) of transaction, not on amount
Payed by the entity sending money

https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#1y
You send

1,000

Show fee breakdown

- 14.78 EUR  Total fees

7.86009  Exchange rate (Not guaranteed)

Recipient gets approximately

7,743.92

Should arrive in 27 minutes
Bitcoin is not always the cheapest option
6 Bitcoin is anonymous
One-Time Pseudonyms

Physical world

- Bob
- Alice
- Charlie

Bitcoin network

Transaction
0.8 BC →
0.4 BC →

Better privacy
Bitcoin & Privacy

Degree of privacy on Bitcoin network, but far from perfect

“We show that, if the user pays using a cryptocurrency, trackers typically possess enough information about the purchase to uniquely identify the transaction on the blockchain, link it to the user’s cookie, and further to the user’s real identity.

“Identified” persons linked to

PRINCETON UNIVERSITY

MIT Massachusetts Institute of Technology

WikiLeaks

Silk Road

identified persons linked to


Legislation EU
3/2017: Amendment proposal on directive (EU) 2015/849

“Member States shall ensure that providers of exchanging services between virtual currencies and fiat currencies, custodian wallet providers, currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered”

Maart 2017: European Parliament proposes amendment:
“The Commission therefore proposes to make virtual currency exchange platforms and custodian wallet providers subject to some of the same reporting obligations as traditional financial service providers. In this framework, national FIUs (Financial Intelligence Units) should be able to associate virtual currency addresses with the identity of the owner of virtual money.”

December 2017: Agreement EP & EC

Regulation can be bypassed, but becomes harder and less attractive
Bitcoin is pseudonymous
Identification attacks possible
Exchange platforms will identify you
7 Myths About Bitcoin

7 Bitcoin is trustless
We trust...

1. The correctness of the assumptions
2. The unhackability of our blockchain client
3. The unhackability of websites & trade platforms
4. Our infallibility (onfeilbaarheid)
5. Miners not to rewrite the blockchain collectively
6. That the value of Bitcoin will not collapse
7. That rules will not be changed against our interests
8. That the transaction fees will be acceptable
1. Bitcoin is money
2. Bitcoin is efficient
3. Bitcoin has perfect security
4. Bitcoin is a scarce asset, like gold
5. Bitcoin has low transaction costs
6. Bitcoin is anonymous
7. Bitcoin is trustless
Conclusion

Bitcoin is a 1\textsuperscript{st} experiment with blockchain
We cannot expect that a 1\textsuperscript{st} experiment is perfect
Hijacked by speculators

Future evolutions
- Legislation
- Technology (e.g. lightning network)
Dr. Kristof Verslype
Researcher, advisor & speaker in crypto, privacy & blockchain tech

Smals Research
@SmalsResearch
www.smalsresearch.be

Smals ICT for society
@Smals_ICT
www.smals.be

Personal
www.cryptov.net
@KristofVerslype
kristof.verslype@smals.be
be.linkedin.com/in/verslype