Bitcoin, Ether, Crypto-currencies and more. Blockchain Technology Explained

TechNovation Talks

Nicolas Engel, OICT - Digital Blue Helmets

Agenda

- Demonstration of a Bitcoin/Ethereum transaction
- Introduction: Economical Landscape of Crypto-currencies
- Crypto-currencies: mechanisms and functioning
  - Structure & principles
  - Mechanisms of a bitcoin transaction
- Bitcoin as a viable money/legal tender?
- Conclusion

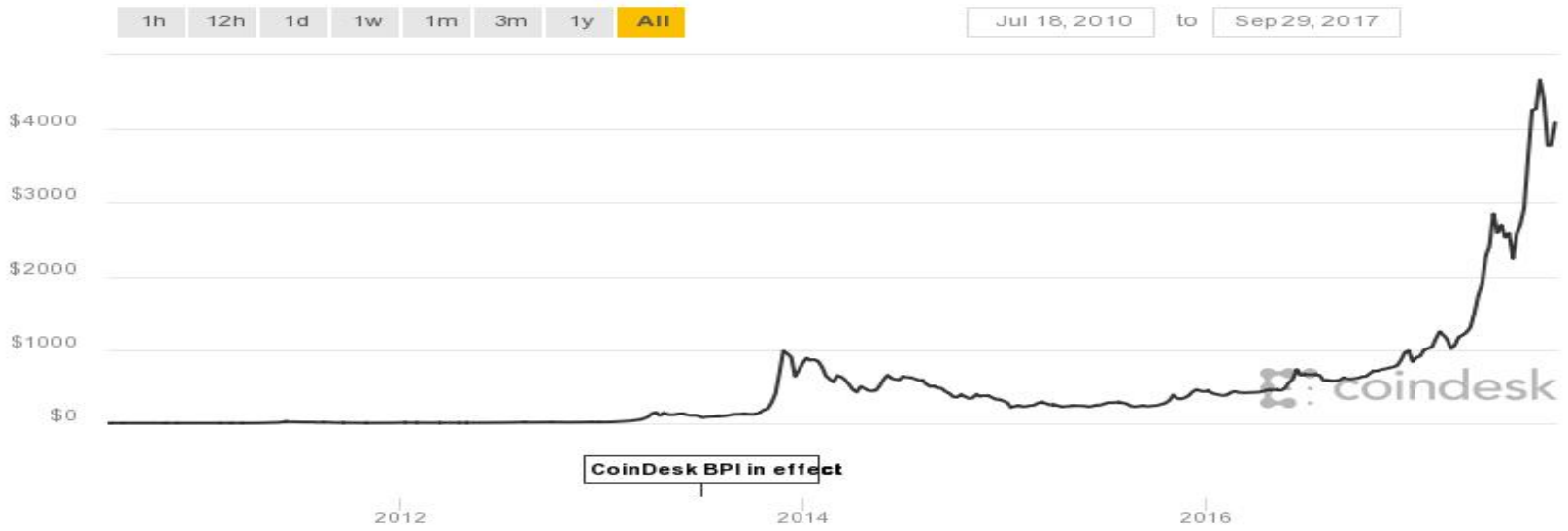
Demo of a Bitcoin or Ethereum transaction

Introduction: Economical Landscape of Crypto-currencies

A few facts and figures:

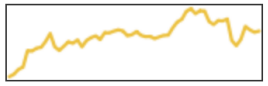
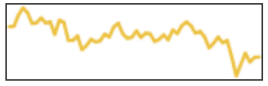
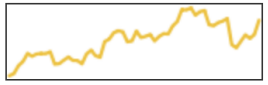
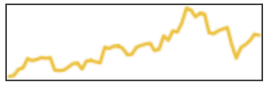
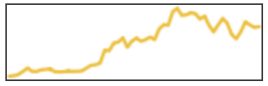
- Bitcoin the first – and most used crypto-currency – exists since 2009.
- Since then we have seen emergence of a huge number of other crypto-currencies – around a 1000.
- The bitcoin network:
  - Around 9600 nodes across the world
  - 477M addresses used
  - Averaging 295 000 transactions per day

Bitcoin Focus: Historical Evolution



- A slow but steady evolution over the years
- A sharp acceleration of the growth in the last year
- A certain sensitivity to external factors

Market Capitalization: Bitcoin and other Crypto-Currencies

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$69,413,018,143	$4182.83	16,594,750 BTC	$1,388,010,000	0.40%	
2	Ethereum	$27,747,480,826	$292.45	94,878,103 ETH	$543,405,000	-2.00%	
3	Ripple	$7,478,736,296	$0.195044	38,343,841,883 XRP *	$75,551,700	-0.93%	
4	Bitcoin Cash	$7,299,492,377	$439.09	16,624,175 BCH	$152,457,000	-2.08%	
5	Litecoin	$2,824,962,728	$53.15	53,155,557 LTC	$188,926,000	-1.31%	
6	Dash	$2,503,529,665	$329.97	7,587,189 DASH	$37,802,000	-2.25%	
7	NEM	$2,137,149,000	$0.237461	8,999,999,999 XEM *	$5,075,130	0.14%	
8	IOTA	$1,632,543,214	$0.587345	2,779,530,283 MIOTA *	$17,055,700	-0.92%	
9	Monero	$1,452,901,652	$95.89	15,151,216 XMR	$38,457,300	-1.09%	
10	NEO	$1,451,665,000	$29.03	50,000,000 NEO *	$74,983,200	-4.19%	

Some interesting characteristics of Bitcoin

- The absence of central authority render them immune to centralized manipulation schemes – but not to speculation.
- The cost of transaction remains low – particularly compared to money remittance services (c.a.1% vs 8% in average).
  - Costly verification mechanisms are not necessary anymore
- Transaction are validated in a faster manner (10mn bitcoin even less on other networks)
- Their very structure guarantees integrity, accountability and accessibility of every transaction ever made

CRYPTO-CURRENCIES: PRINCIPLES & FUNCTIONING

Characteristics of Crypto-Currencies

- They rely on a decentralized network of participants
  - There is no central financial establishments.
  - Anyone can become a member and create a crypto wallet
- They allow secure exchanges without the need of a central control authority
  - No settlement entity or external validation is necessary to carry out transactions
- They can be pseudonymous or anonymous:

  Transactions details may be available, but as transactions happen between addresses and are verified using cryptographic and mathematical process, no proof of identity is necessary.

Structure of Crypto-Currencies

- Participants of the network have a copy of the crypto-currency ledger: it contains the list of all accepted transactions in the history of the network.
  - The ledger is usually stored in a blockchain – a tamper-proof distributed structure.
  - **Analogy: record of all banking transactions**
- Each participant can possess bitcoin addresses
  - **Analogy: various accounts where one can receive or send money**

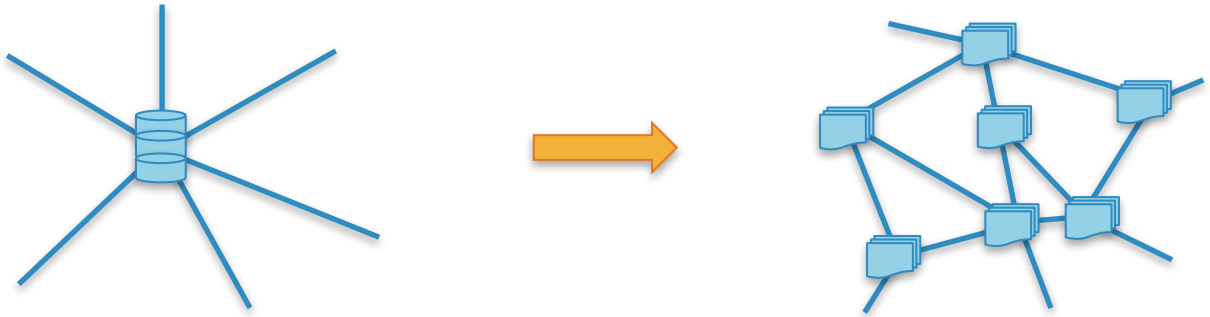
Ex: 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

- Those addresses are not tied to identities but to a private key, that can unlock the funds
  - To perform an operation one uses this key to prove possession of the address

Structure of Crypto-Currencies: blockchains

- It is a chain-of-blocks each of the block containing data
- Interesting properties for Data Storage:
  1. It is **tamper-proof**

  2. It can be use in **decentralized** networks



  3. It can be **trusted without** a **central authority**

A BITCOIN FUND TRANSFER

A bitcoin fund transfer – Initial State

- Initial situation:
  - A sender (Jorge) wants to transfer 10 bitcoins to a receiver (Nicolas)

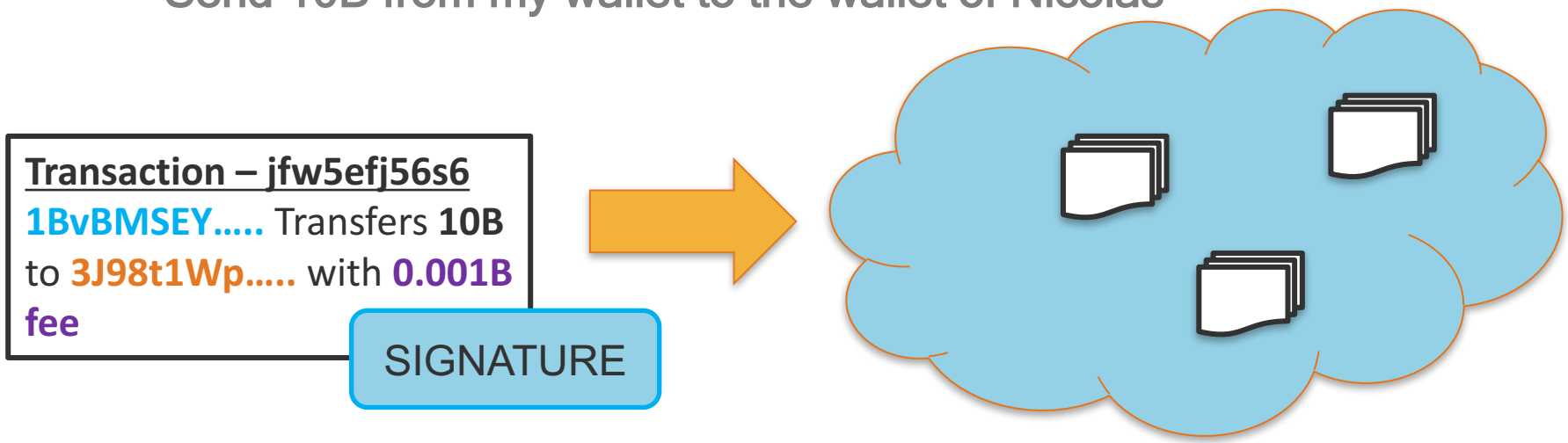
Sender - 1BvBMSEY…..
- 100B

Receiver - 3J98t1Wp…..
- 100B

Transaction – jfw5efj56s6
1BvBMSEY….. Transfers **10B** to **3J98t1Wp…..**

How do they work – I: Initiating a transaction

- What will actually happen
  1. Jorge signs and publishes the transaction to the network stating: **Send 10B from my wallet to the wallet of Nicolas**

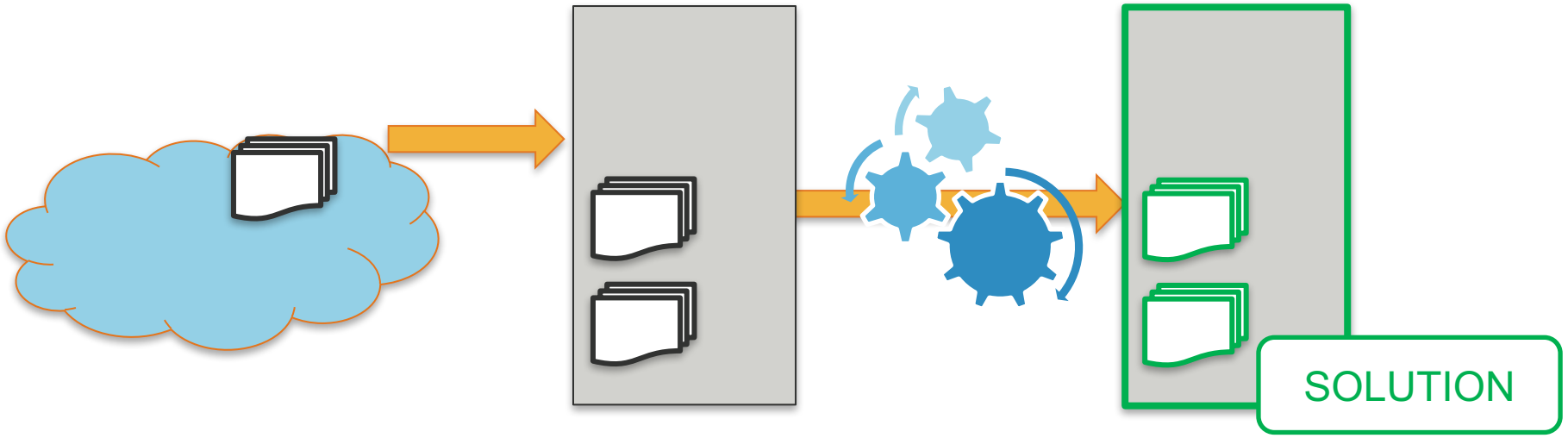


  2. The network receives and broadcast the transaction: each participant forward the transaction

How do they work – II: Validating a transaction

A miner – or a validator - will pick-up the transaction – along with many others - and will do two things:

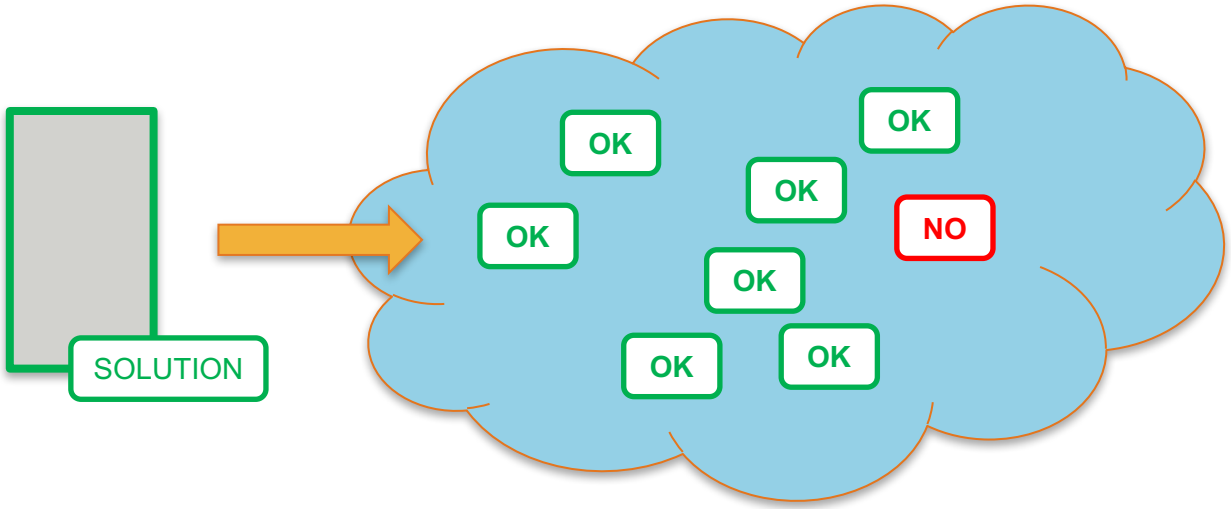
1. He checks if the **signature** and the **transaction** are **valid**
2. If they are, he adds the transaction to his block. Once he has enough…
3. …. he **solves** a **difficult** and unique **puzzle** – specific to the block.



How do they work – III: Accepting a transaction

The validated block is broadcasted to the network – i.e. each participant

1. They check that the **transactions** & **signatures** are **valid**
2. They check that the **puzzle solution** is **correct**



How do they work – III: Accepting a transaction

Each participant can find two answers:

The block is valid – this set of transaction is sound and correct

The participant accepts those transactions and updates his version of the ledger

OK

The block is not valid – this set of transaction is not correct

One of the transaction is not correct OR the puzzle solution is not correct

The participant does not add these transactions and wait for another block

NO

A bitcoin fund transfer – Final State

- Final situation:
  - After a few minutes, if the transaction is validated:

Sender - 1BvBMSEY…..
- 100B – 10.01B = 89,09B

Transaction – jfw5efj56s6
1BvBMSEY….. Transfers **10B** to **3J98t1Wp….. with 0.001B fee**

Receiver - 3J98t1Wp…..
- 100B + 10B = 110B

Miner - 1B5Au4m4……
+ 0.01B

  - Each participants has updated its record with the new transaction **jfw5efj56s6** and has an updated ledger.

Crypto-Currencies as a Money

Characteristics of Money

- A money must fulfill three main purposes:
  - **Medium of exchange**
  - **Measure of value**
  - **Store of value**

- And have specific characteristics:
  - Durability
  - Portability
  - Divisibility
  - Uniformity / fungibility
  - Limited Supply / Scarcity
  - Acceptability
  - Difficulty to counterfeit
  - **Stability**

Characteristics of Money

Properties	Fiat Currency	BTC
Medium of exchange	YES	YES
Measure of Value	YES	Evolving
Store of Value	YES	Evolving
Durability	YES	YES
Portability	YES	YES
Divisibility	YES	YES
Uniformity/Fungibility	YES	Evolving
Limited Supply/Scarcity	YES	YES
Acceptability	YES	Evolving
Difficulty to Counterfeit	YES	YES

Bitcoin as a money?

- Bitcoin as money faces some challenges due mainly to:
  - Its high volatility
  - Its limited acceptability
  - Its disputable fungibility

If we can consider there is an economy **around bitcoin** (Exchanges, Wallets, Initial Coin Offerings(ICO), the **absence** of an **economy based** on **bitcoin** as an underlying explains some of the **properties it lacks**.

Legal & Regulatory status of Bitcoin

- There is no world-wide consensus on how to define bitcoin and per extensions crypto-currencies, it can be either:
  - Forbidden
  - A property
  - An asset, a commodity, a security, …
  - A legal tender
- Generally speaking, the high monetary risks associated to a **highly volatile** currency combined to the **difficult traceability of transaction** and **identification of actors** limit its acceptance as a legal tender.
  - The price of bitcoin and some other cryptocurrencies is heavily impacted by speculation or political/economical announcements of real world economies
  - There is no regulation that is easily achievable

Looking ahead

1. Recently we have seen a strong increase in Initial Coin Offerings (ICO) – somewhat similar concept to IPOs using cryptocurrencies – with level actually higher than traditional early stage venture capital for internet companies.
2. Smart contracts – that leverage distributed ledger technologies – to achieve more complex operations on virtual currencies networks also have seen an increase in interest from a broad range of stakeholders

- These recent phenomenon could lead to the **emergence of a virtual-currency based economy** – which would use cryptocurrencies as **underlying currencies** hence allowing to achieve a certain **stability** and assert virtual-currencies as an **alternative money**

QUESTIONS & REMARKS