Blockchain: Cybersecurity and Accountability for the Next Decade

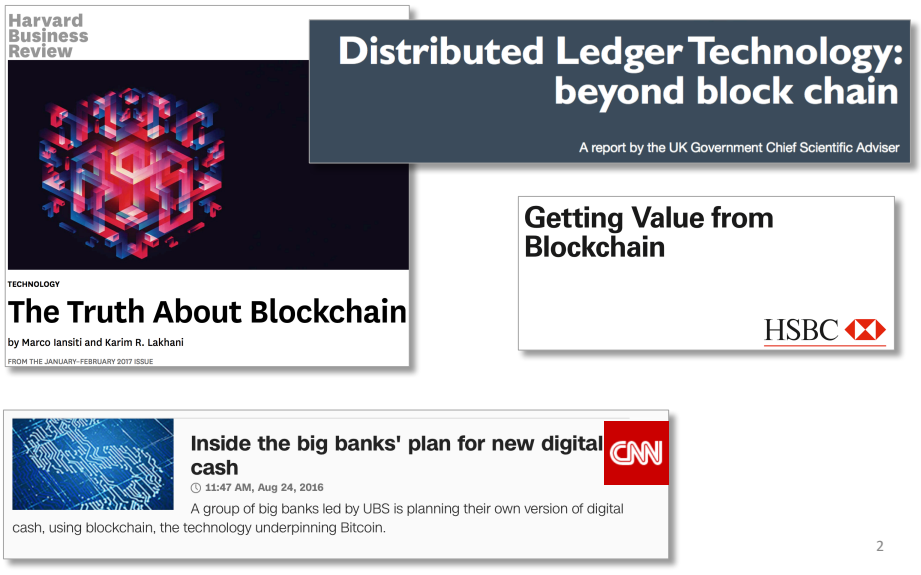
Miguel Pupo Correia

IPAI – Fórum de Auditoria Interna 2017

Jun. 2017

U LISBOA | UNIVERSIDADE DE LISBOA
TÉCNICO LISBOA
FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR
inesc id lisboa

Motivation: vast interest world-wide



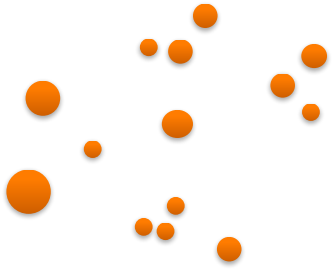
2

Motivation: vast interesting in Portugal

Blockchain or distributed ledger

- Ordered, append-only, database of transactions

- Distributed: in servers connected by the Internet
  - Each one keeps a copy of the chain/database



4

Cybersecurity properties

- Byzantine fault-tolerant
  - Even if some nodes are compromised, availability and integrity are ensured
  - How? By running a consensus algorithm between servers
- Auditable because the ledger is visible to "all"

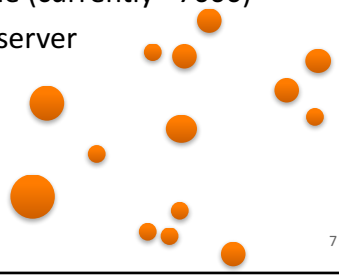
5

FROM BITCOIN TO BLOCKCHAIN

6

Bitcoin

- Bitcoin is a cryptocurrency
  - A currency like Euro or Dollar
  - That is not issued by a country of a central bank
  - Based on cryptographic mechanisms
- Who issues the coin?
  - A federation of servers world-wide (currently ~7000)
  - Anyone can enter by providing a server



7

Bitcoin – payments

- These server run a blockchain that stores all transactions of bitcoins (money changing of hands)
  - Solves the double payment problem, i.e., avoid that the same owner uses the same coin in two transactions
  - Anonymity is guaranteed using a cryptographic scheme
  - Bitcoin rather slow today ☹ : ~1h to have the transaction inserted in the chain + 1h to be certain it stays there

8

Bitcoin – coin creation

- New coins are created through mining, i.e., providing proof-of-work
  - Requires minutes in high-performance servers
  - Mining is needed for consensus; coins are a compensation

9

Why trusting Bitcoin?

- Trust is put on:
  - Distribution: many servers involved, unlikely to collude
  - Consensus algorithm: now well analyzed and it works
  - Money: mutual benefit of having it running
  - "I don't know, but people are using it and it works"

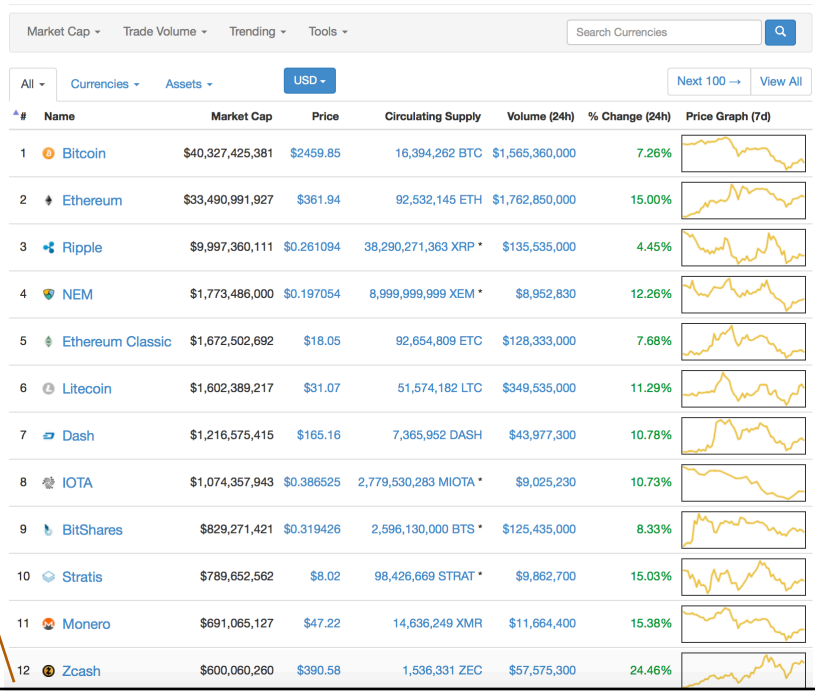
10

CryptoCurrency Market Capitalizations

Bitcoin is the first of many

https://coinmarketcap.com/all/views/all/

868 on June 16, 2017



Market Cap | Trade Volume | Trending | Tools | Search Currencies

All | Currencies | Assets | USD | Next 100 → | View All

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$40,327,425,381	$2459.85	16,394,262 BTC	$1,565,360,000	7.26%	
2	Ethereum	$33,490,991,927	$361.94	92,532,145 ETH	$1,762,850,000	15.00%	
3	Ripple	$9,997,360,111	$0.261094	38,290,271,363 XRP *	$135,535,000	4.45%	
4	NEM	$1,773,486,000	$0.197054	8,999,999,999 XEM *	$8,952,830	12.26%	
5	Ethereum Classic	$1,672,502,692	$18.05	92,654,809 ETC	$128,333,000	7.68%	
6	Litecoin	$1,602,389,217	$31.07	51,574,182 LTC	$349,535,000	11.29%	
7	Dash	$1,216,575,415	$165.16	7,365,952 DASH	$43,977,300	10.78%	
8	IOTA	$1,074,357,943	$0.386525	2,779,530,283 MIOTA *	$9,025,230	10.73%	
9	BitShares	$829,271,421	$0.319426	2,596,130,000 BTS *	$125,435,000	8.33%	
10	Stratis	$789,652,562	$8.02	98,426,669 STRAT *	$9,862,700	15.03%	
11	Monero	$691,065,127	$47.22	14,636,249 XMR	$11,664,400	15.38%	
12	Zcash	$600,060,260	$390.58	1,536,331 ZEC	$57,575,300	24.46%	

BLOCKCHAIN FOR GENERIC APPLICATIONS

12

Smart contracts

- The notion was introduced in Ethereum, another blockchain, with a cryptocurrency (Ether)
- A smart contract is:
  - A computer program (software), which is a formal and executable version of a contract
  - Stored in a blockchain
  - Executed in the same blockchain
  - That may result in updates to the blockchain, e.g., transactions of a cryptocurrency (e.g., Ether)

13

Blockchain variants

- Permissionless (i.e., no permission needed):
  - any server can enter, but to participate actively must provide proof-of-work (slow and expensive)
  - examples: Bitcoin and Ethereum
  - for public use
- Permissioned (i.e., permission needed):
  - servers must have permission; no proof-of-work needed
  - example: Hyperledger Fabric
  - for consortium or private (!) use

14

Permissionless blockchains applications

- Cryptocurrencies
- Smart contracts

15

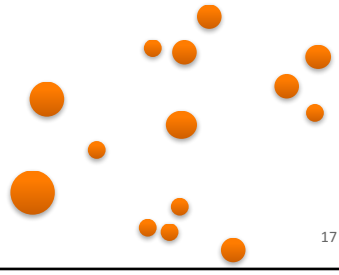
Permissioned blockchains applications

- Permissioned blockchains are the future imho
  - As most applications are supposed to be managed by a consortium or a single entity, not open for anyone to enter
- Examples
  - Selling fund participations (APFIPP prototype)
  - Public administration registry of X
  - Public key infrastructure (i.e., to store personal and organizations' public keys for verifying digital signatures)

16

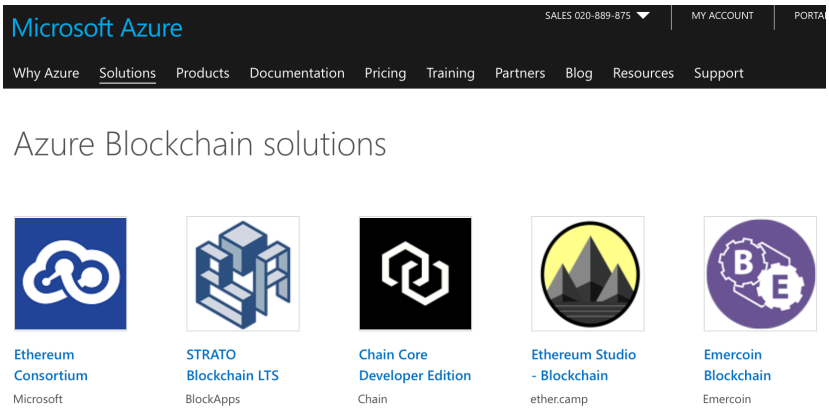
Accountability / auditing

- Blockchains provide accountability in the sense that data may available for a set of entities to audit:
  - Everyone in public blockchains
  - All consortium members in consortium blockchains, plus entities to which access is given
- Note: not mandatory, as data may be encrypted
- Examples:
  - Selling funds
  - Public administration registry



17

Not rocket science, use the cloud



18

WHY PORTUGAL?

19

Expertise in Portugal

- Bitcoin born ~2009 but the techniques it uses are older
- Several PhDs in Byzantine fault tolerance at ULisboa, MIT
- Technology
  - PBFT, a popular algorithm, was designed by Miguel Castro
  - BFT-Smart, the only open stable BFT algorithm, designed by Alysson Bessani
- Research at INESC-ID and FCUL
- Companies interested, startups appearing

20

CONCLUSION

21

Conclusion

- Blockchain: a distributed, ordered, append-only, database of transactions
  - Originally part of Bitcoin, now many available
- Applications
  - Crypto-currencies
  - Smart contracts
  - Other based on permissioned blockchains
- Cybersecurity: availability&integrity with bad nodes
- Accountability / auditing

22

Thank you

Miguel Pupo Correia

http://www.gsd.inesc-id.pt/~mpc/

U LISBOA | UNIVERSIDADE DE LISBOA

TÉCNICO LISBOA

FCT Fundação para a Ciência e a Tecnologia

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

inesc id lisboa