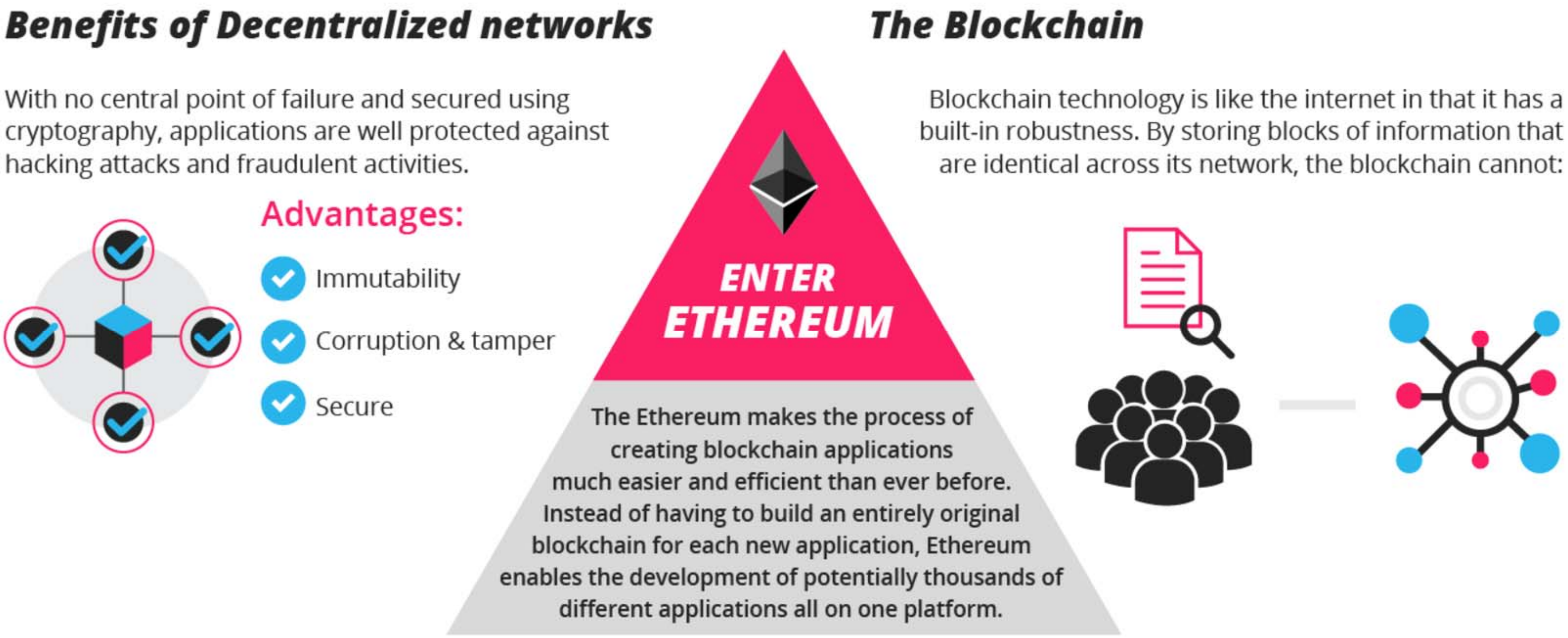
Smart contracts on Ethereum

ETHEREUM

"I thought [those in the Bitcoin community] weren't approaching the problem in the right way. I thought they were going after individual applications; they were trying to kind of explicitly support each [use case] in a sort of Swiss Army knife protocol." Vitalik Buterin, inventor of Ethereum

Ethereum Benefits



Benefits of Decentralized networks

With no central point of failure and secured using cryptography, applications are well protected against hacking attacks and fraudulent activities.

Advantages:

- ✓ Immutability
- ✓ Corruption & tamper
- ✓ Secure

ENTER ETHEREUM

The Ethereum makes the process of creating blockchain applications much easier and efficient than ever before. Instead of having to build an entirely original blockchain for each new application, Ethereum enables the development of potentially thousands of different applications all on one platform.

The Blockchain

Blockchain technology is like the internet in that it has a built-in robustness. By storing blocks of information that are identical across its network, the blockchain cannot:

Smart contracts on Ethereum

- Ethereum provides Solidity
  - A programming language in which to write smart contracts
- Transaction-triggered language
- Cryptographic identities
- Own cryptocurrency (Ether) and thousands of "tokens".
- The user pays the cost of execution on the network.

Solidity - Hello World

```
pragma solidity ^0.4.21;


contract Coin {
    // The keyword "public" makes those
variables readable from outside.
    address public minter;
    mapping (address => uint) public
balances;
    // Events allow light clients to react on
changes efficiently.
    event Sent(address from, address to, uint
amount);
    // This is the constructor whose code is run
only when the contract is created.
 function Coin() public {
                minter = msg.sender;
```

```
 function mint(address receiver, uint amount)
public {
                if (msg.sender != minter) return;
        balances[receiver] += amount;
    }


    function send(address receiver, uint
amount) public {
                if (balances[msg.sender] <
amount) return;
                balances[msg.sender] -= amount;
        balances[receiver] += amount;
                emit Sent(msg.sender, receiver,
amount);
    }
```

Solidity - Listener

```
Coin.Sent().watch({}, ", function(error, result) {
  if (!error) {
     console.log("Coin transfer: " + result.args.amount +
        " coins were sent from " + result.args.from +
        " to " + result.args.to + ".");
     console.log("Balances now:\n" +
                 "Sender: " +
Coin.balances.call(result.args.from) +
                 "Receiver: " +
Coin.balances.call(result.args.to));
  }
})
```

Examples of applications

- Games of Chance.
- Prediction Markets: Gnosis, Augur
- *Initial Coin Offers* (ICOs)

- Some examples

Smart Contract Platforms

Blockchain	Smart contracts?	Programming languages
Bitcoin	No	
Ethereum	Yes	Solidity
Hyperledger	Yes	GoLang, C++…

Autonomous distributed organizations

Autonomous distributed organizations

- A *Distributed Autonomous Organization* (DAO) is an organization whose rules are established by the code of a smart contract.
- Multiple implications:
  - Autonomous: Independent of the creator
  - Decentralized: Cannot be turned off
  - Self-sufficient: Can obtain the resources it needs

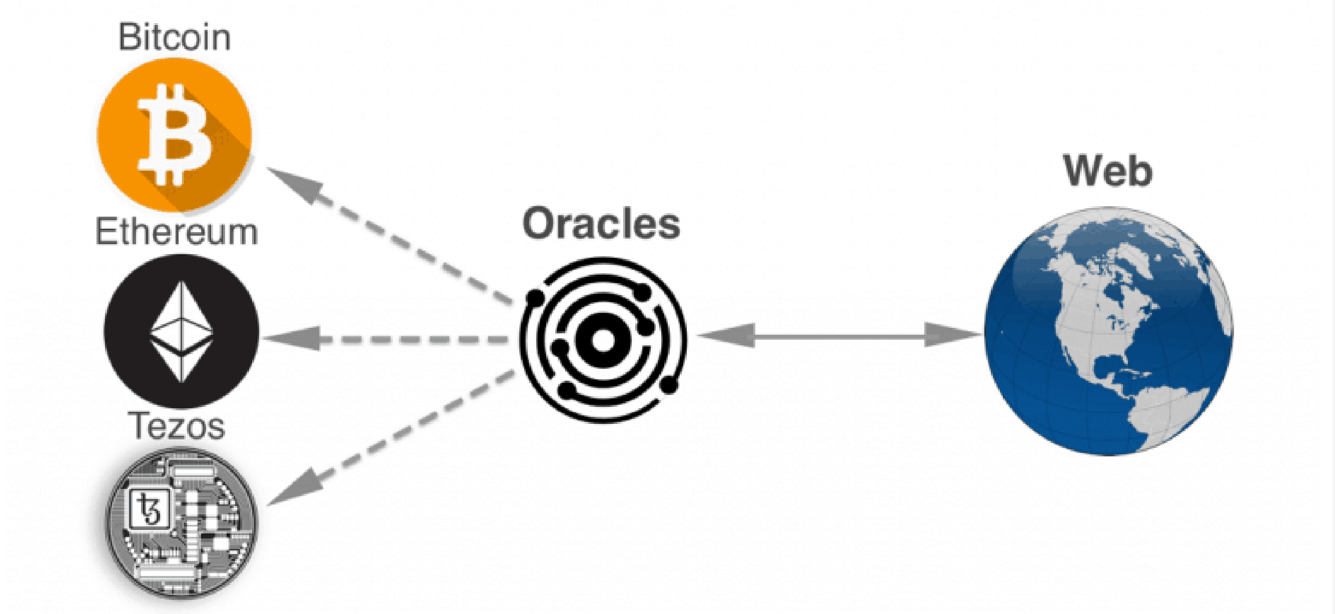
Examples

- □ The DAO
- □ Plantoid (http://www.plantoidproject.eu/)
- □ Cryptokitties (https://cryptokytties.co/)
- □ steemit (https://steem.it/)
- □ Autonomous taxis

Connection to the physical world

Oracles

- Bridge between the real / physical / non-blockchain world and the blockchain system (usually smart contracts).



Oracles

- Software
  - E.g. software that communicates who has won the election.
- Hardware
  - E.g. IoT device that communicates the temperature that it is doing
- How can we trust an uncontrolled third party?
  - Oracle problem in the blockchain

Consensus protocols for oracles

- Consensus-based oracles
  - E.g. Augur is a decentralized prediction market with bets on future events.

- They are already being worked on in several networks
  - E.g. Delphi, Oraclize, Chainlink, Augur

Smart Property

- *Smart* property
  - Managed through smart contracts
  - React/query the status of a Blockchain.
  - E.g. car that works with cryptographic keys.
  - E.g. http://kointoken.org/

Blockchain + IoT

Advantages and opportunities

- Interoperability
  - Communication between IoT devices in **open ecosystem**
- Security
  - No reliance on third parties (distributed)
- Identity
  - Asymmetric Key Infrastructure
- Immutable record
  - Transactions and traceability
- …

Challenges and drawbacks

- Costs
  - Transaction, execution, storage)
- Privacy
  - Full transparency of transaction history
- Scale
  - Limited transactions per second
  - Storage Size
- Security
  - Unstoppable software (bugs, undesirable features...)
  - e.g. The DAO: $50M hack
  - Ex. Parity (multi-signature wallets): $32M hack, 8x more money saved by white hat hackers
- Legality
- Ethics
- …

Standardization

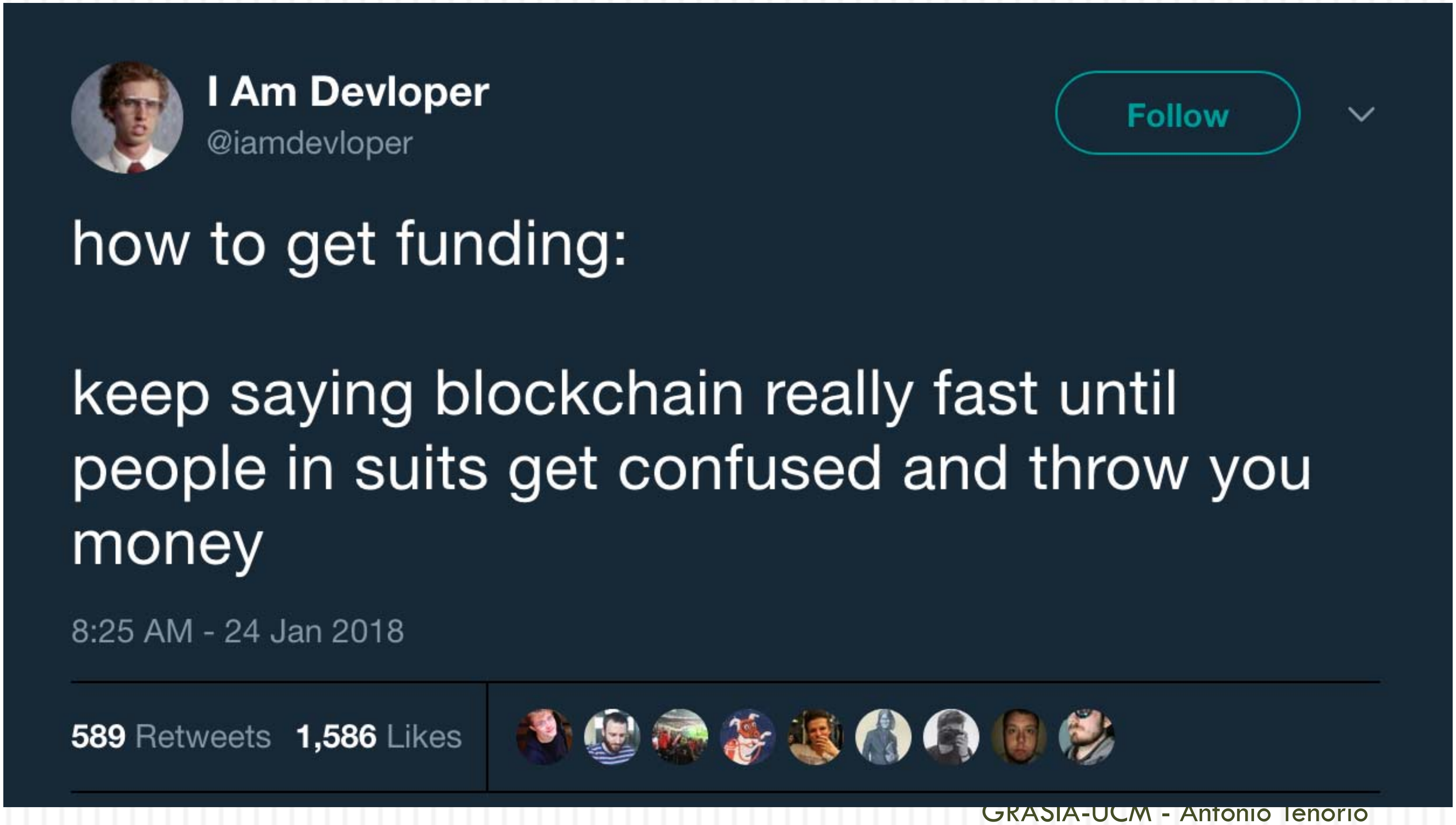
- *Trusted IoT Alliance*
  - Partnership for the development of secure IoT ecosystem on blockchain
- Hyperledger Project
  - Open Source Standard for Private Blockchains

IoT Applications

- Supply chain tracking
  - E.g. Chronicled (https://www.chronicled.org/) , OriginTrail (https://origintrail.io/)
- Identity and authorization
  - E.g. Uport (https://www.uport.me/)
- Secure Device to Blockchain connectivity
  - E.g. Filament (https://filament.com/technology/)
- Smart Property
  - Ex. Slock.it (https://slock.it/)
- Blockchain Infrastructure for IoT
  - E.g. IoTeX (https://iotex.io/), IOTA (https://iota.org/)
- Connection with sensors
  - e.g. Pylon (https://pylon-network.org/) decentralized ecological energy exchange
- …

Conclusions

When to use Blockchain?



I Am Devloper
@iamdevloper

how to get funding:

keep saying blockchain really fast until people in suits get confused and throw you money

8:25 AM - 24 Jan 2018

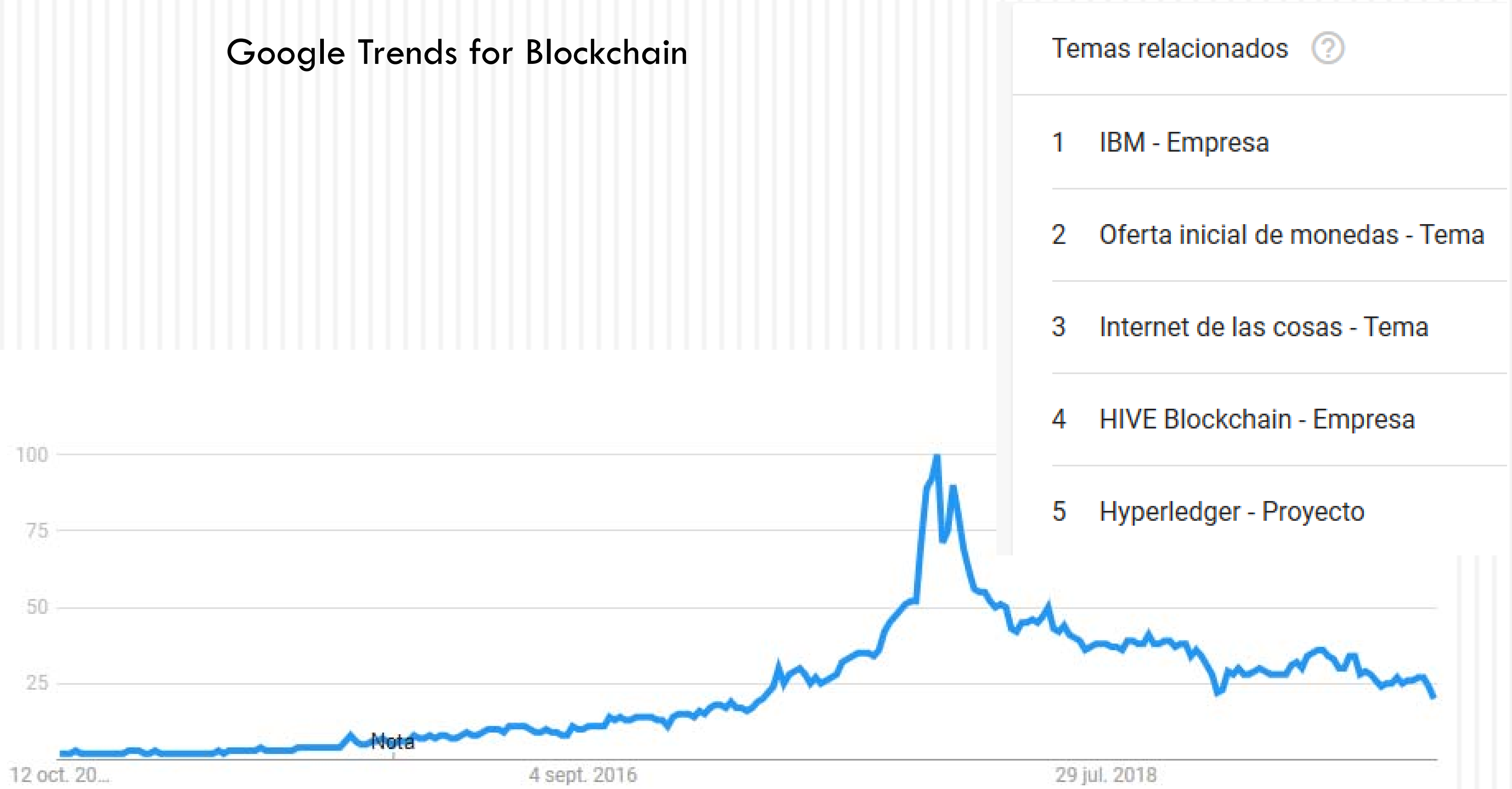
589 Retweets 1,586 Likes

When to use Blockchain?

WHERE SHOULD WE FOCUS THIS YEAR?
"BLOCKCHAIN"
IT WILL CHANGE EVERYTHING.
EVERYBODY IS TALKING ABOUT IT.
THE POTENTIAL APPLICATIONS ARE ENDLESS.
WE DON'T WANT TO BE LEFT BEHIND.
WHAT EXACTLY IS BLOCKCHAIN?
ALSO, "ARTIFICIAL INTELLIGENCE"
TOM FISHBURNE
© marketoonist.com

When to use Blockchain?

Google Trends for Blockchain



Temas relacionados

1 IBM - Empresa

2 Oferta inicial de monedas - Tema

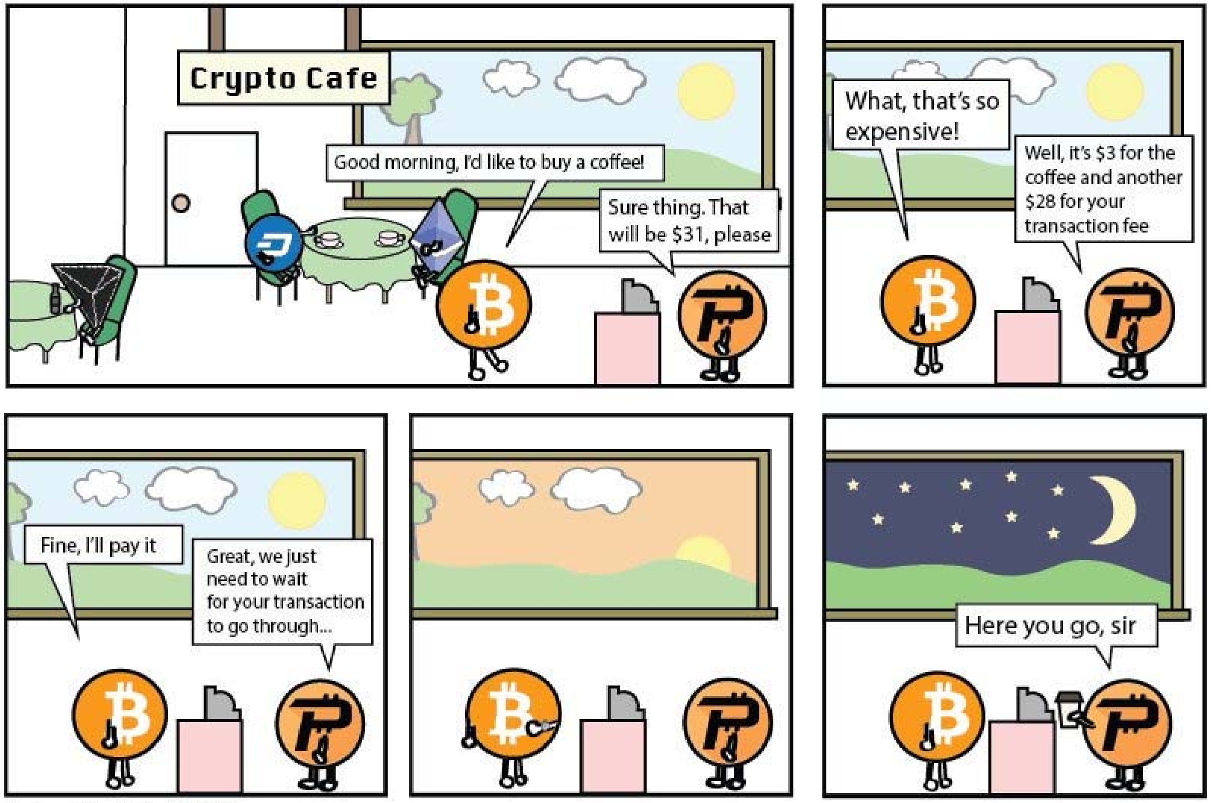
3 Internet de las cosas - Tema

4 HIVE Blockchain - Empresa

5 Hyperledger - Proyecto

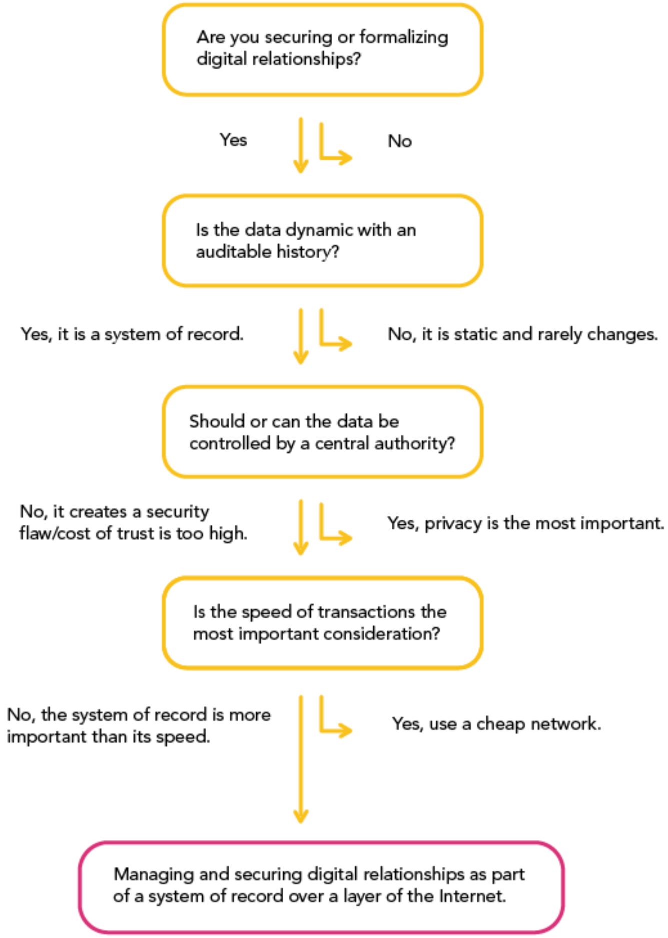
When to use Blockchain?

The Cryptos #16


Crypto Cafe
Good morning, I'd like to buy a coffee!
Sure thing. That will be $31, please
What, that's so expensive!
Well, it's $3 for the coffee and another $28 for your transaction fee
Fine, I'll pay it
Great, we just need to wait for your transaction to go through...
Here you go, sir

First published: Jan 10, 2018

When to use Blockchain?



Are you securing or formalizing digital relationships?

Yes

No

Is the data dynamic with an auditable history?

Yes, it is a system of record.

No, it is static and rarely changes.

Should or can the data be controlled by a central authority?

No, it creates a security flaw/cost of trust is too high.

Yes, privacy is the most important.

Is the speed of transactions the most important consideration?

No, the system of record is more important than its speed.

Yes, use a cheap network.

Managing and securing digital relationships as part of a system of record over a layer of the Internet.

When to use Blockchain?

- When **YES**
  - Digital relationship management and assurance
  - Maintenance of a shared and decentralized record-keeping system
  - Any place where an intermediary or *gatekeeper* is expensive in time or resources
  - When you need to securely store complex transactions between multiple parties
  - When there is data in constant flow but you want to keep a history of actions

When to use Blockchain?

- When **NOT**
  - High throughput in number of transactions per second required
  - Small organizations
    - No business networks
  - BD Substitute
  - Messaging Solution Substitute
  - Transaction Processing System Substitute

Some discussion

When to use Blockchain?

- Easy, isn't it?
  - So, when?
  - Workshop

Questions?

Conclusions

- What have we learned?

Questions?

KEEP
CALM
AND
ASK
QUESTIONS

References

References

- [EdX, 2019] EdX: Introduction to Hyperledger Blockchain Technologies. 2019. Available at https://www.edx.org/course/blockchain-for-business-an-introduction-to-hyperledger-technologies on 1/10/2019
- [Ethereum, 2019] Ethereum: Ethereum White Paper. 2019. Available at https://github.com/ethereum/wiki/wiki/White-Paper on 1/10/2019.
- [Linux Foundation, 2019] The Linux Foundation: Hyperledger. 2019 Available from https://www.hyperledger.org/ on 1/10/2019.
- [Nakamoto, 2008] Nakamoto, S.: Bitcoin - A peer-to-peer electronic cash system. 2008. Available at https://bitcoin.org/bitcoin.pdf on 1/10/2019
- [Wood, 2014] Wood, G.: Ethereum - A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151. 2014. Available at https://ethereum.github.io/yellowpaper/paper.pdf on 1/10/2018
- [Filippi & Hassan, 2016] Filippi, P., Hassan, S.: Blockchain technology as a regulatory technology - From code is law to law is code. First Monday, 21(12). Available at http://dx.doi.org/10.5210/fm.v21i12.7113 on 1/10/2019

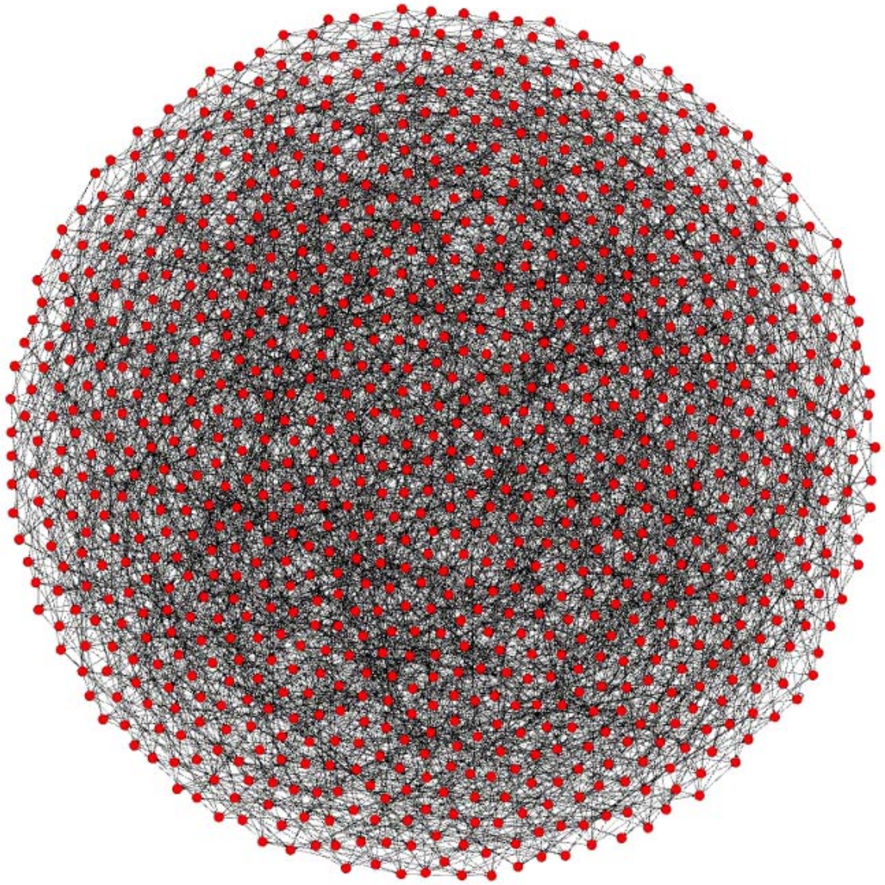
Glossary

Glossary

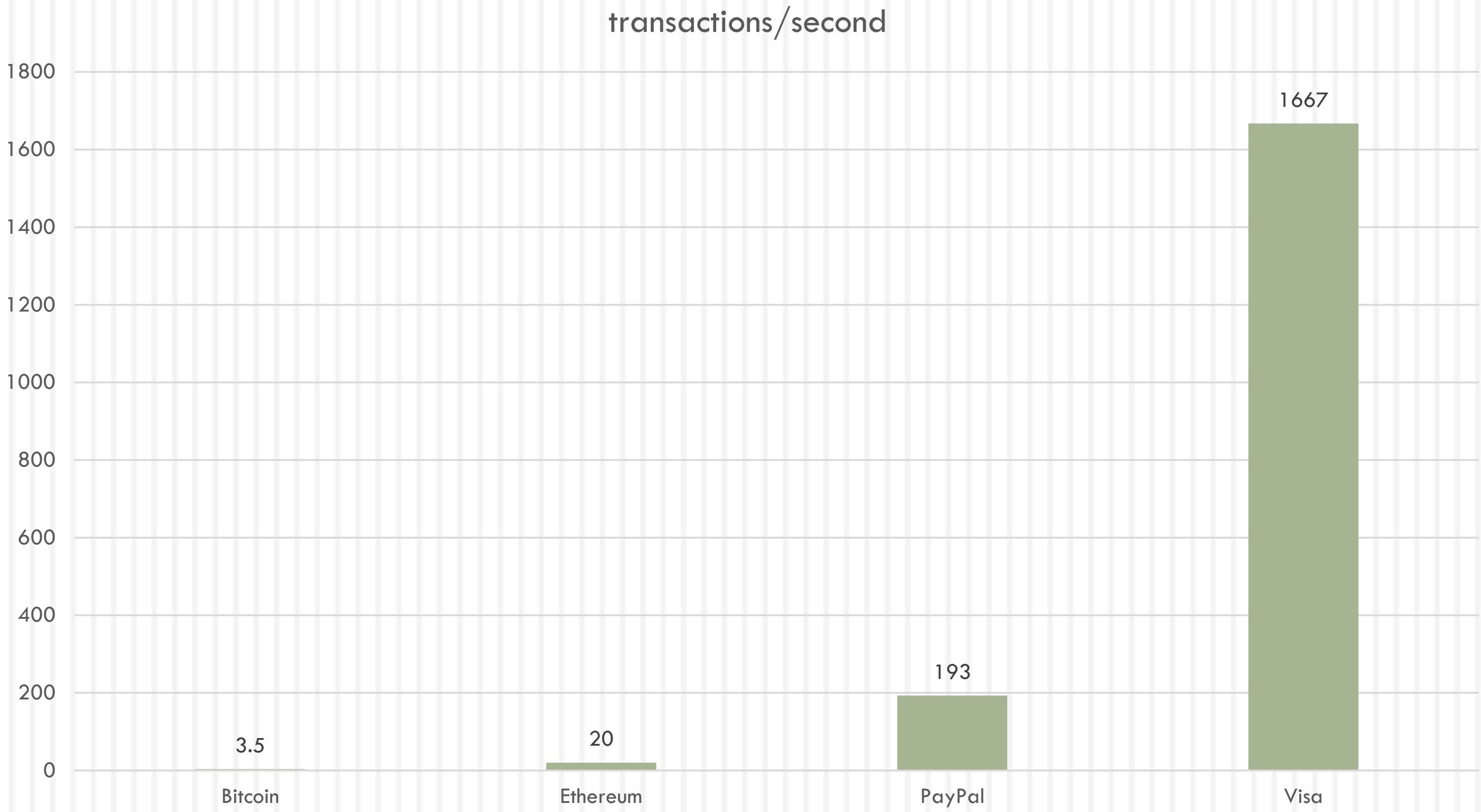
- DB = Database
- BYOE = *Bring Your Own Encryption*
- DAO = *Distributed Autonomous Organization*
- P2P = *Peer to Peer*
- PoS = *Proof of Stake*
- PoW = *Proof of Work*

Extras

Bitcoin today



Speed of transactions


transactions/second
Bitcoin
Ethereum
PayPal
Visa