Every ‘bitcoin’ has two sides.

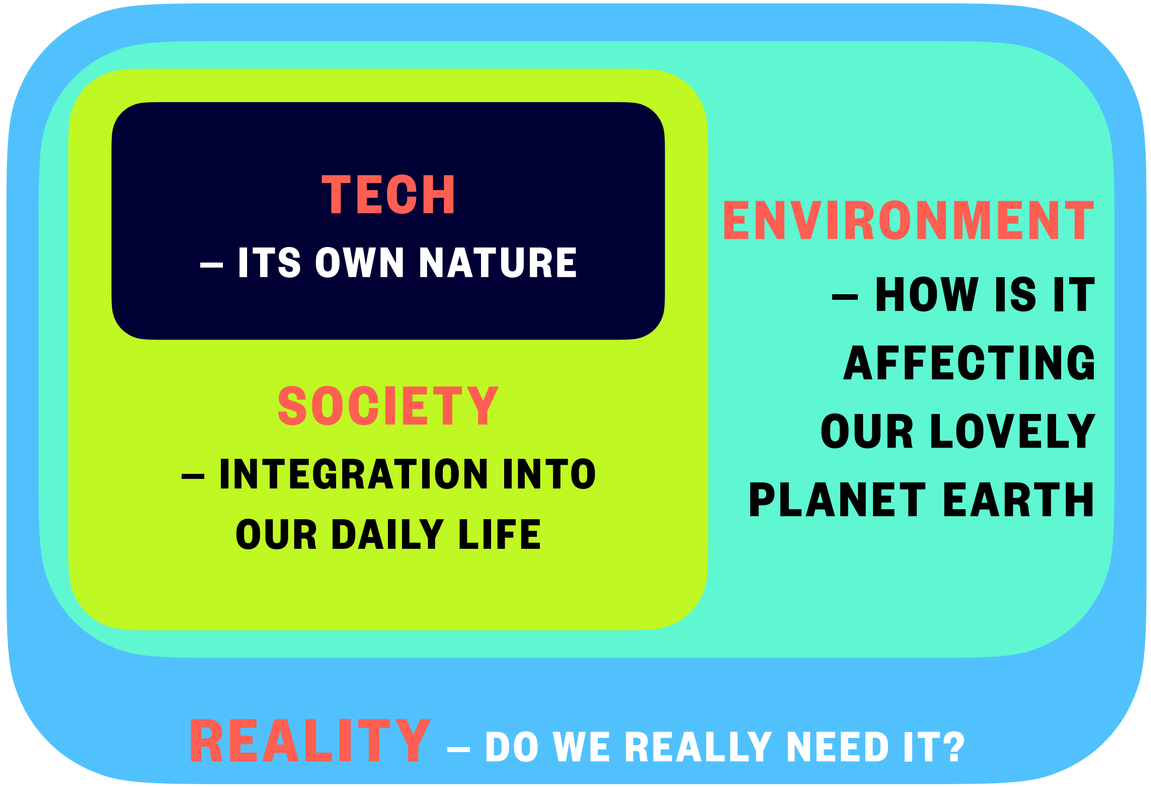
TIBA

Limitations & Vulnerabilities of Blockchain

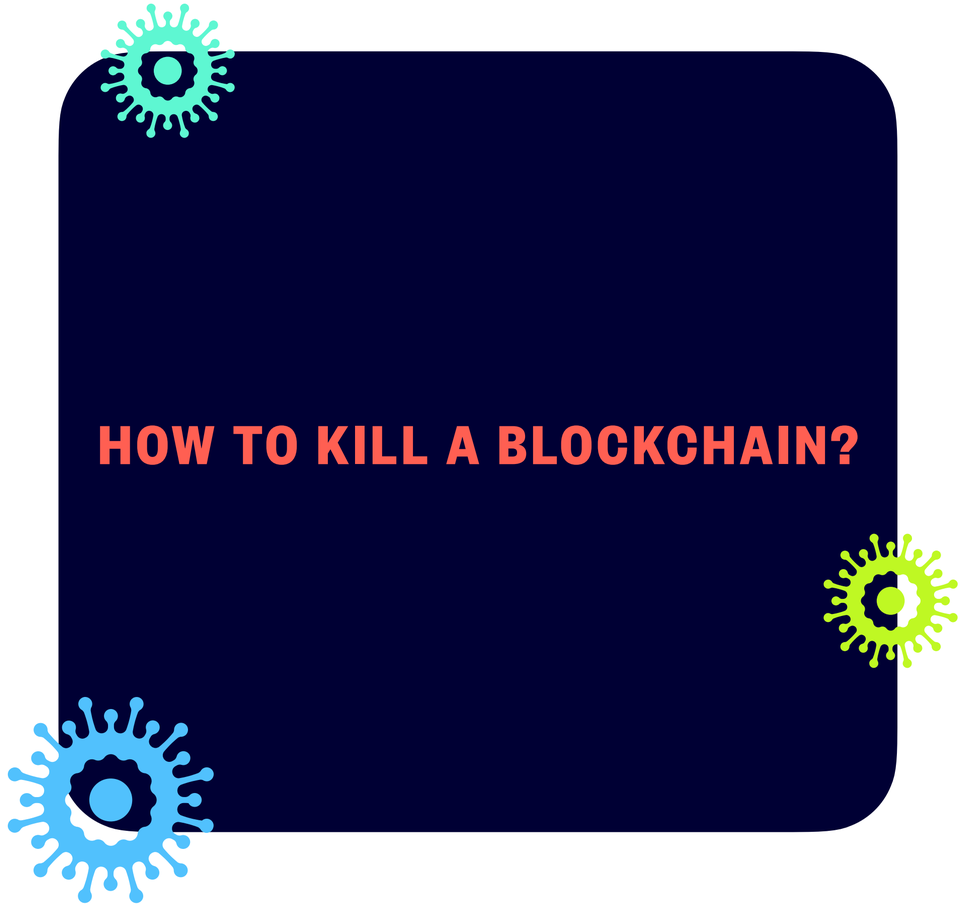
JINWOO SEONG, JUNE 29TH

Topics - How I divided them ?

TIBA



LIMITATIONS

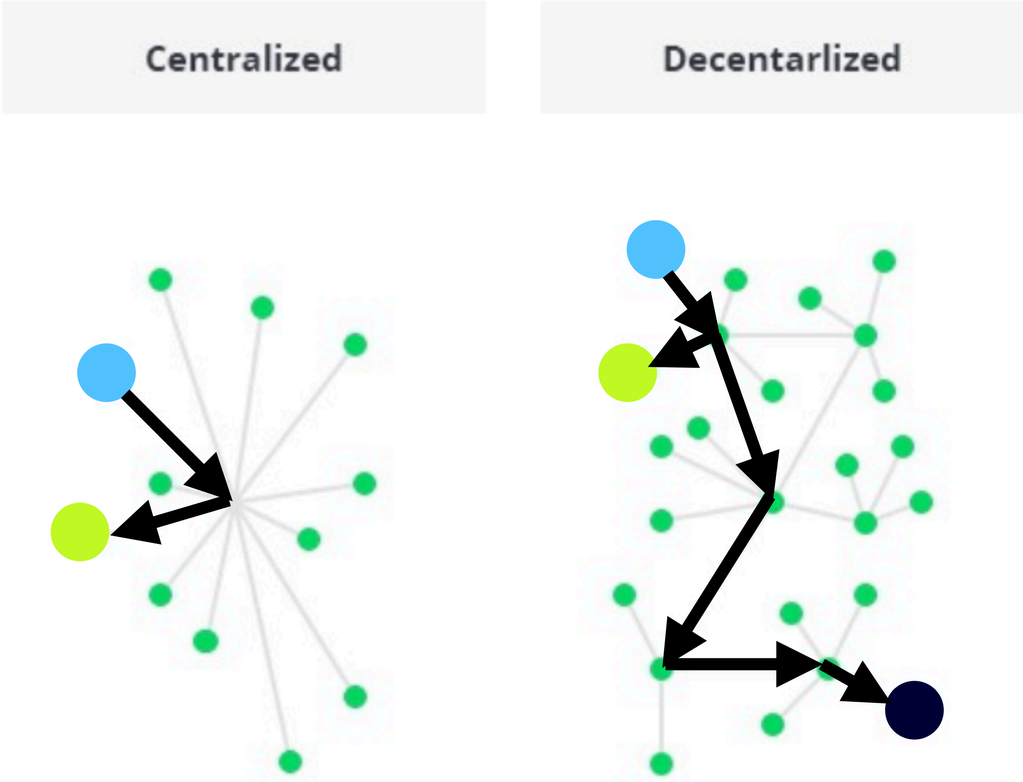


VULNERABILITIES

Limitations - Tech

TECH
– ITS OWN NATURE

- Scalability
- Change of Protocol (hard fork)
- Interoperability



Limitations - Tech

TIBA

TECH
– ITS OWN NATURE

- Scalability
- Change of Protocol (hard fork)
- Interoperability

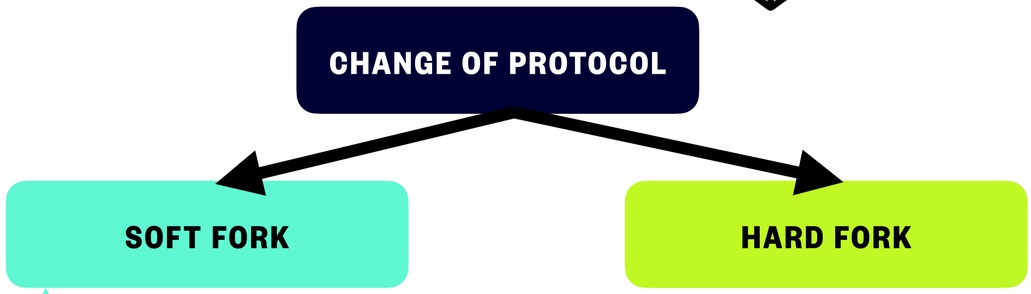
Source: https://howmuch.net/articles/crypto-transaction-speeds-compared

Limitations - Tech

TIBA

TECH
– ITS OWN NATURE

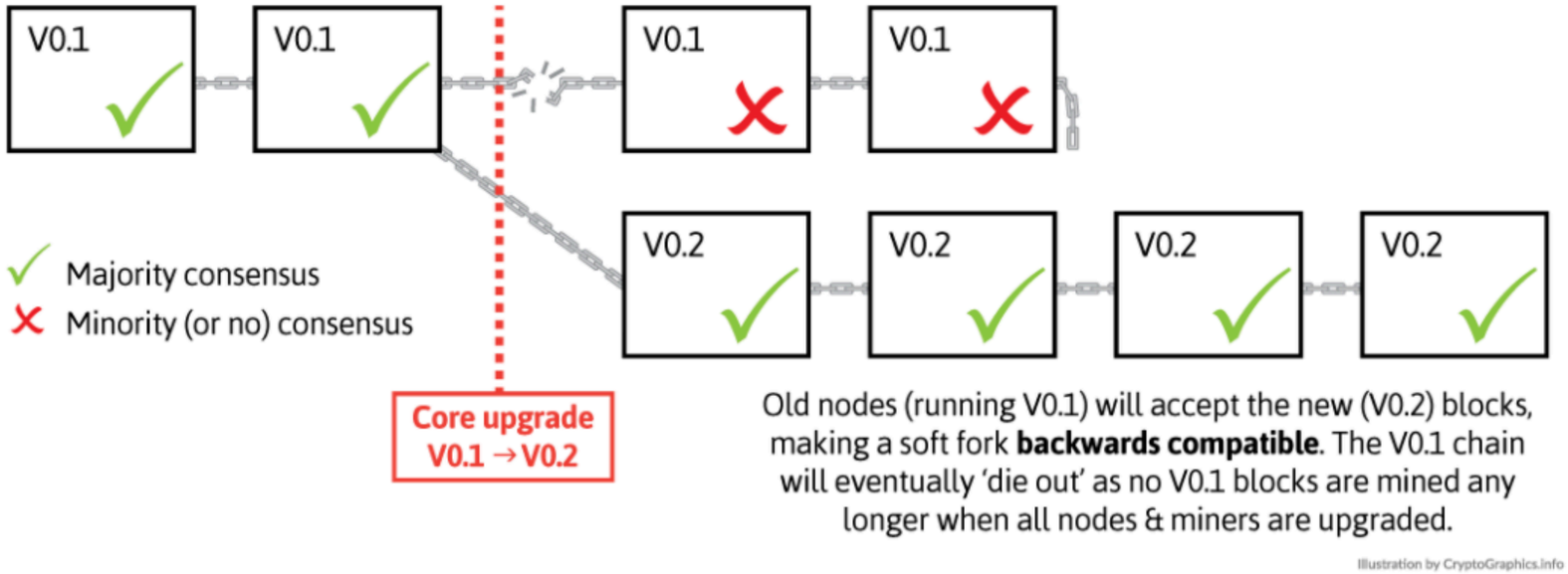
- Scalability
- Change of Protocol (hard fork)
- Interoperability



A SOFT FORK IS A CHANGE IN A CRYPTOCURRENCY PROTOCOL WHICH IS BACKWARD-COMPATIBLE.

THAT MEANS THAT NON-UPDATED NODES ARE STILL ABLE TO PROCESS TRANSACTIONS AND PUSH NEW BLOCKS TO THE BLOCKCHAIN, SO LONG AS THEY DON'T BREAK THE NEW PROTOCOL RULES.

Limitations - Tech



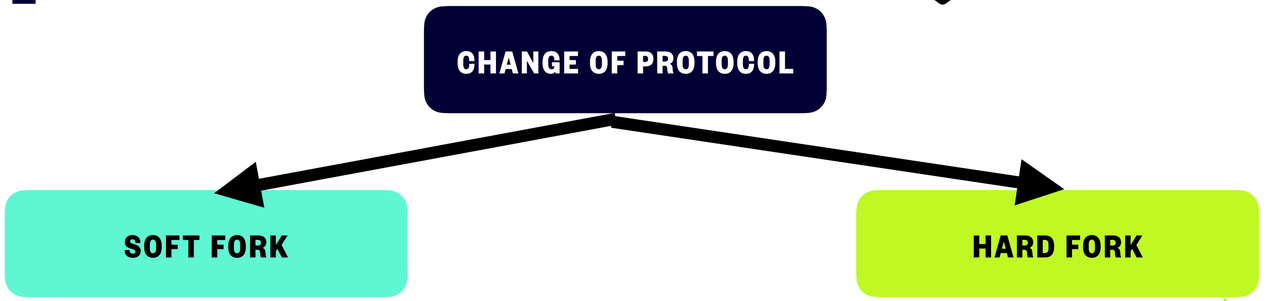
Soft Fork

Limitations - Tech

TIBA

TECH
– ITS OWN NATURE

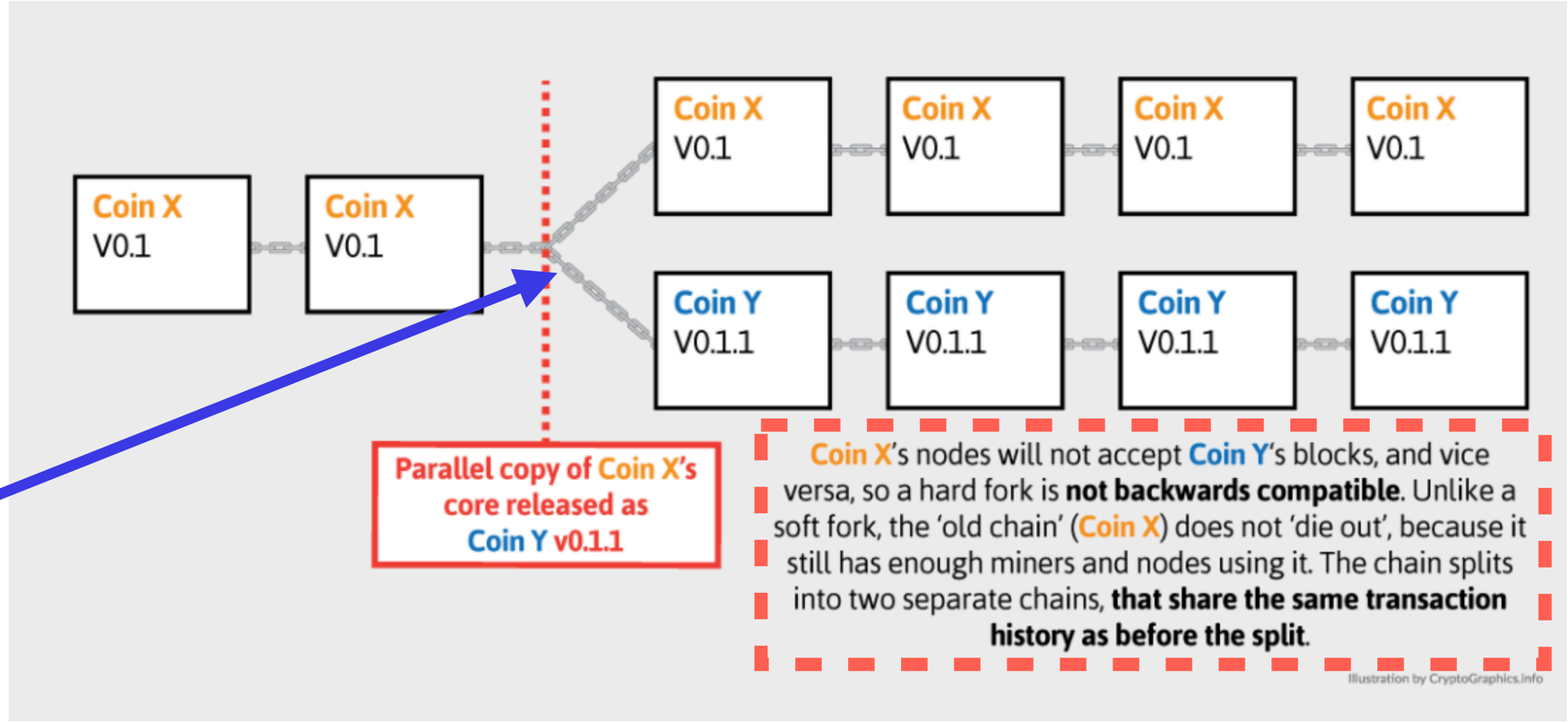
- Scalability
- Change of Protocol (hard fork)
- Interoperability



A HARD FORK IS A CHANGE IN A CRYPTOCURRENCY PROTOCOL WHICH IS **INCOMPATIBLE** WITH THE **PREVIOUS VERSIONS**, MEANING THAT NODES THAT DON'T UPDATE TO THE NEW VERSION **WON'T BE ABLE TO PROCESS TRANSACTIONS OR PUSH NEW BLOCKS TO THE BLOCKCHAIN**.

HARD FORKS CAN BE USED TO CHANGE OR IMPROVE AN EXISTING PROTOCOL, OR EVEN TO CREATE A NEW, INDEPENDENT PROTOCOL AND BLOCKCHAIN.

Limitations - Tech



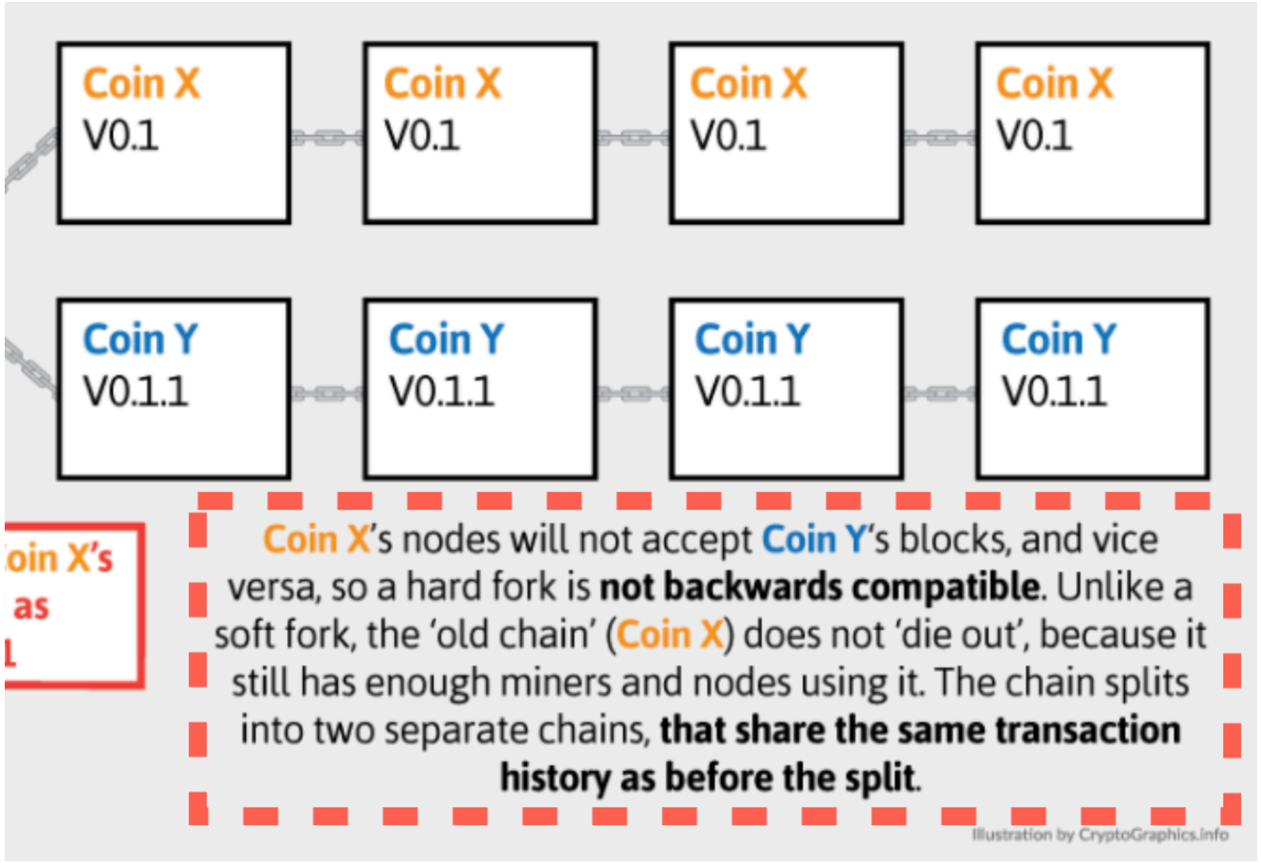
THERE MIGHT BE A PROBLEM HERE !!!

Hard Fork

Limitations - Tech

TIBA

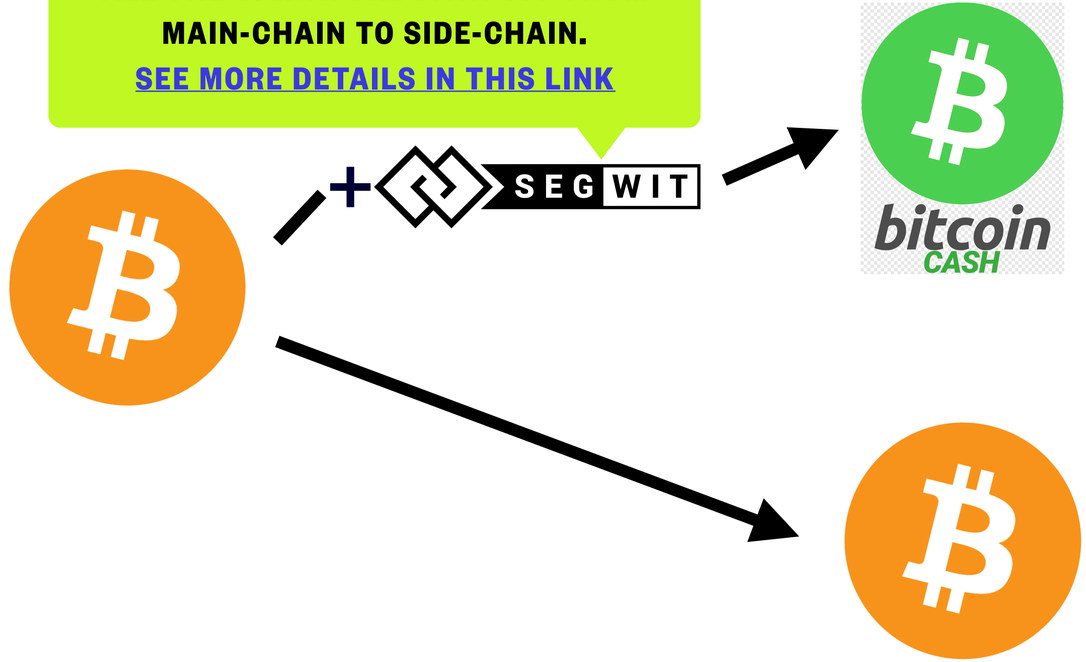
Hard Fork



One Famous Blockchain Hard Fork Case

[The Birth Of Bch: The First Crazy Days Of "Bitcoin Cash"]

A SIDE-CHAIN SOLUTION THAT CAN MOVE ALL THE SIGNATURE DATA OFF FROM MAIN-CHAIN TO SIDE-CHAIN.
SEE MORE DETAILS IN THIS LINK



Limitations - Tech

TIBA

TECH
– ITS OWN NATURE

- Scalability
- Change of Protocol (hard fork)
- Interoperability

THERE ARE MORE THAN 6500 STANDALONE BLOCKCHAIN PROJECTS AVAILABLE, WITH **DIFFERENT PROTOCOLS, CODING LANGUAGES, CONSENSUS MECHANISMS, AND PRIVACY MEASURES**.

IT'S LACKING A **UNIVERSAL STANDARD** THAT WOULD ALLOW DIFFERENT NETWORKS TO COMMUNICATE WITH EACH OTHER.

Polkadot. ← **THEY ARE TRYING TO SOLVE THIS PROBLEM!**

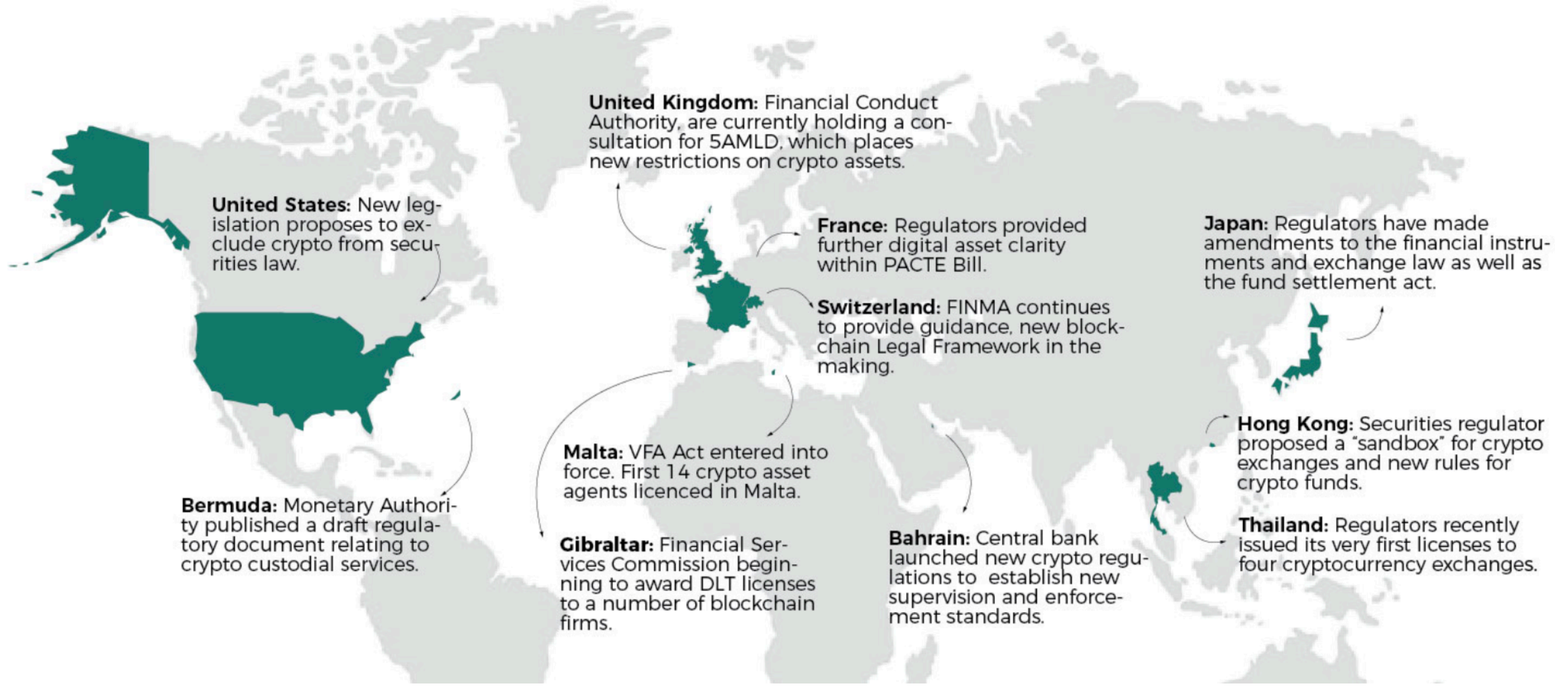
Here is the link to Polkadot.

Limitations - Society

TECH
– ITS OWN NATURE

SOCIETY
– INTEGRATION INTO OUR DAILY LIFE

- Regulations/Politics
- Inefficiency
- Cost of Implementation



Source: https://www.e-zigurat.com/innovation-school/blog/blockchain-regulations-recent-key-developments/

Limitations - Society

TIBA

TECH
– ITS OWN NATURE

SOCIETY
– INTEGRATION INTO OUR DAILY LIFE

- Regulations/Politics
- Inefficiency
- Cost of Implementation

REGULATIONS IN CHINA

DEC.5TH, 2013
ON 5 DECEMBER 2013, PEOPLE'S BANK OF CHINA (PBOC) MADE ITS FIRST STEP IN REGULATING BITCOIN BY PROHIBITING FINANCIAL INSTITUTIONS FROM HANDLING BITCOIN TRANSACTIONS.

APR.1ST, 2014
ON 1 APRIL 2014 PBOC ORDERED COMMERCIAL BANKS AND PAYMENT COMPANIES TO CLOSE BITCOIN TRADING ACCOUNTS IN TWO WEEKS.

SEP.4TH, 2017
SEVEN CENTRAL GOVERNMENT REGULATORS JOINTLY ISSUED THE ANNOUNCEMENT ON PREVENTING FINANCIAL RISKS FROM INITIAL COIN OFFERINGS, WHICH BANNED INITIAL COIN OFFERINGS (ICOS) IN CHINA.

2018
CRYPTOCURRENCY EXCHANGES OR TRADING PLATFORMS WERE EFFECTIVELY BANNED BY REGULATION IN SEPTEMBER 2017 WITH 173 PLATFORMS CLOSED DOWN BY JULY 2018.

FEB, 2019
IN FEBRUARY 2019, THE CYBERSECURITY ADMINISTRATION OF **CHINA** IMPLEMENTED THE **BLOCKCHAIN** INFORMATION SERVICE MANAGEMENT **REGULATIONS** (“BISMR”) WHICH ESTABLISHED THE LEGAL FRAMEWORK FOR THE OPERATION OF A **BLOCKCHAIN**-BASED BUSINESS WITHIN THE PRC.

Limitations - Society

TIBA

TECH
– ITS OWN NATURE

SOCIETY
– INTEGRATION INTO OUR DAILY LIFE

- Regulations/Politics
- Inefficiency
- Cost of Implementation

1. Multiple Copies of the same huge chunk of data(ledger).
2. The more transactions are made and nodes are created, the bigger the blockchain size, therefore the slower the network.

That's how big the bitcoin ledger is!

Limitations - Society

TIBA

TECH
– ITS OWN NATURE

SOCIETY
– INTEGRATION INTO OUR DAILY LIFE

- Regulations/Politics
- Inefficiency
- Cost of Implementation

1. Learning Curve: Not very welcome to beginners, and the resources are scattered all over.
2. Maintenance: will takes up about 15%~20% of the overall project cost
3. Time Consumption: Implementation takes up a lot of time (as everybody knows how long it took for ETH 2.0 to develop and it's still developing.)
4. Financial Aspect: if your blockchain service can be done easily via smart contracts, and it shouldn't be much. It is estimated that the cost of implementing blockchain solution will vary from 5000 dollars to 200,000 dollars depends on the projects complexity.

Limitations - Environment

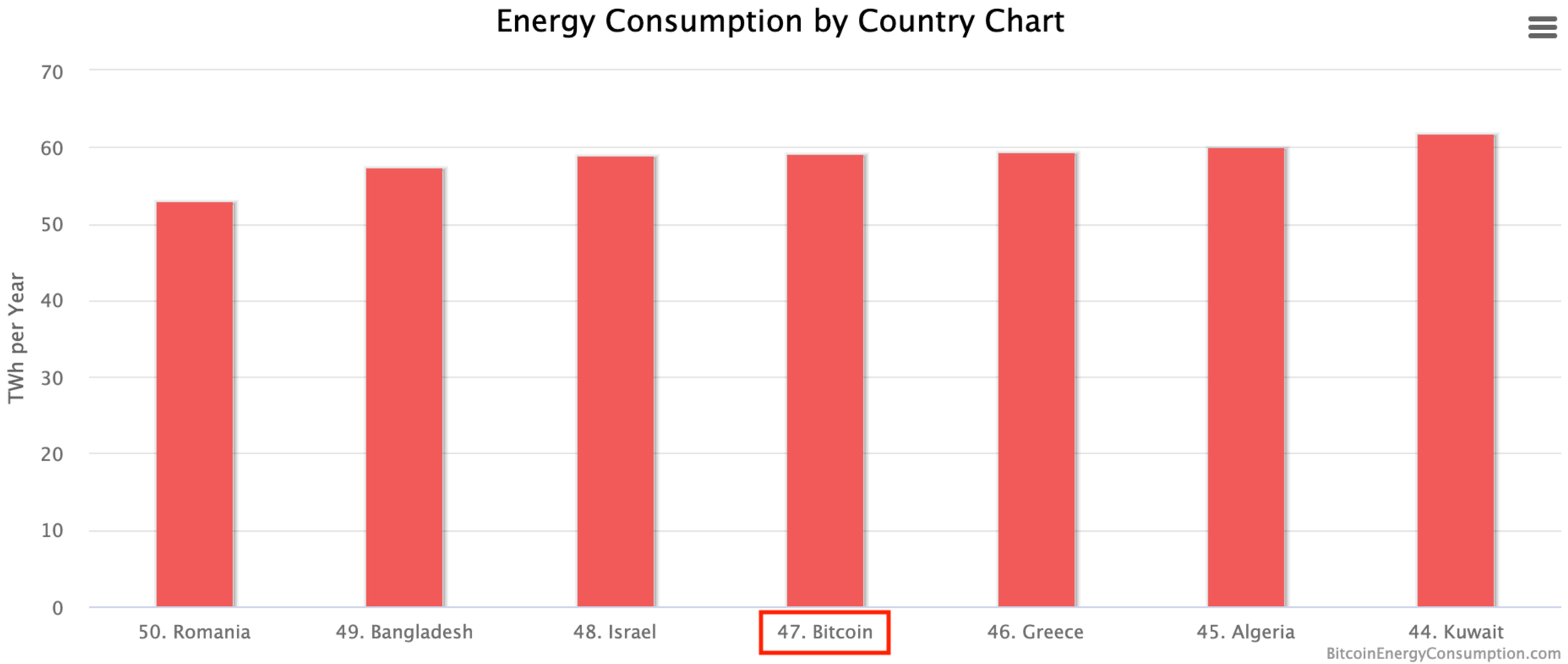
TIBA

"The problem with mining cryptocurrencies is that it only works well when done at scale: an individual server is worthless. As a result, mining Bitcoin alone uses the same amount of energy as used by the entire island of Ireland in a single year."

source: https://emagazine.com/environmental-effects-of-blockchain/#:~:text=Even%20outside%20the%20context%20of,are%20very%20reliant%20on%20energy.

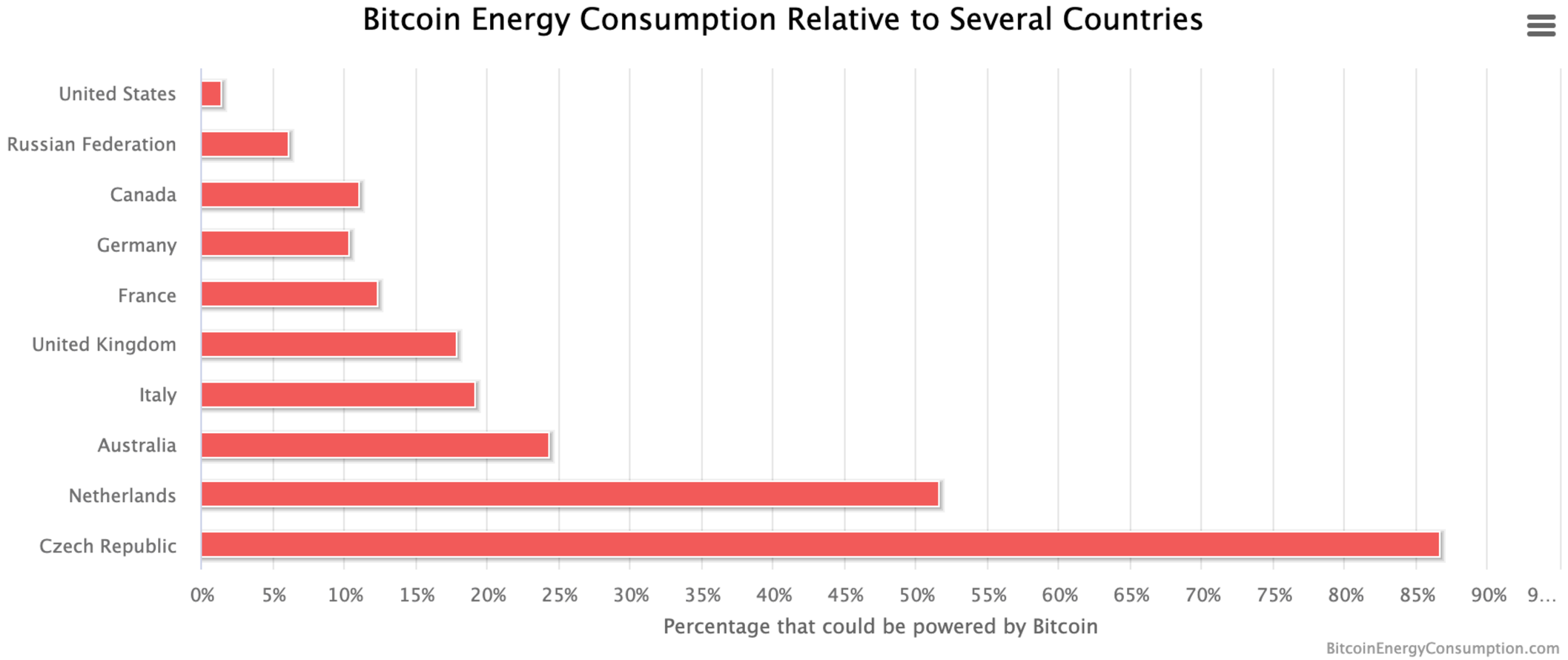
- Energy Consumption

Limitations - Environment

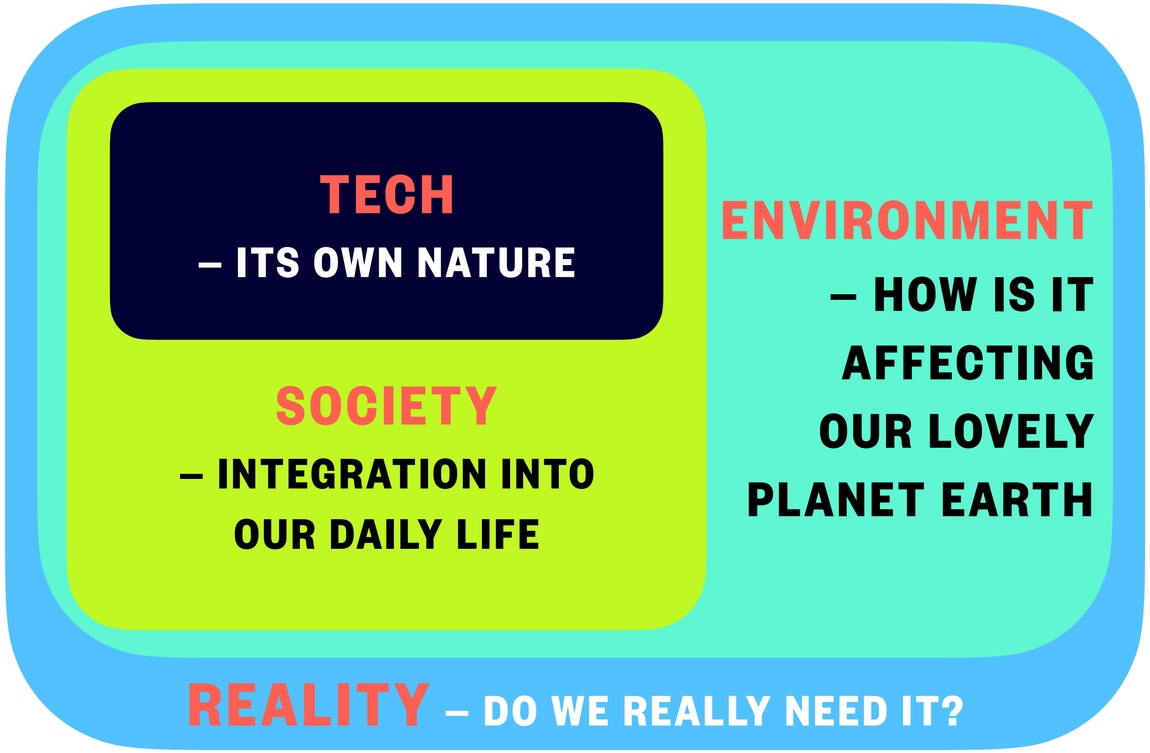


Limitations - Environment

TIBA



Limitations - Reality



- Integration with Legacy System

  Why would corporations spend tons of money on something that benefits them by little while they could just use their old xp software as it is?

- Lack of Blockchain Developers

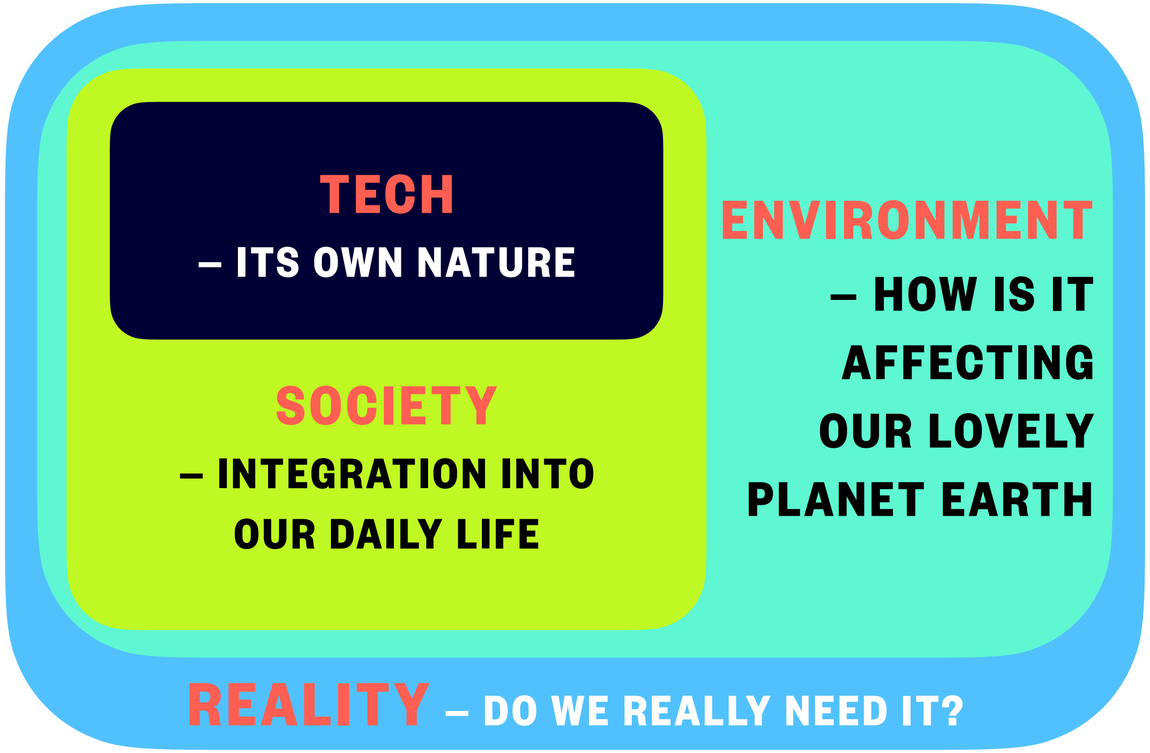
> **Blockchain developers** have become very valuable in the job market, with jobs ranging from $150,000 to $250,000. According to job search platform, Hired, there has been a 517% increase in **demand** for software engineers having knowledge in **blockchain development**, in the past year. Nov 27, 2019
>
> www.blockchain-council.org › blockchain › why-the-d...
>
> Why the Demand for Blockchain Developers is 'through the ...

- Blockchain in some cases can be slow and cumbersome

  Takes 60 minutes to send A BTC while I could just use WeChat Pay instead…

Limitations

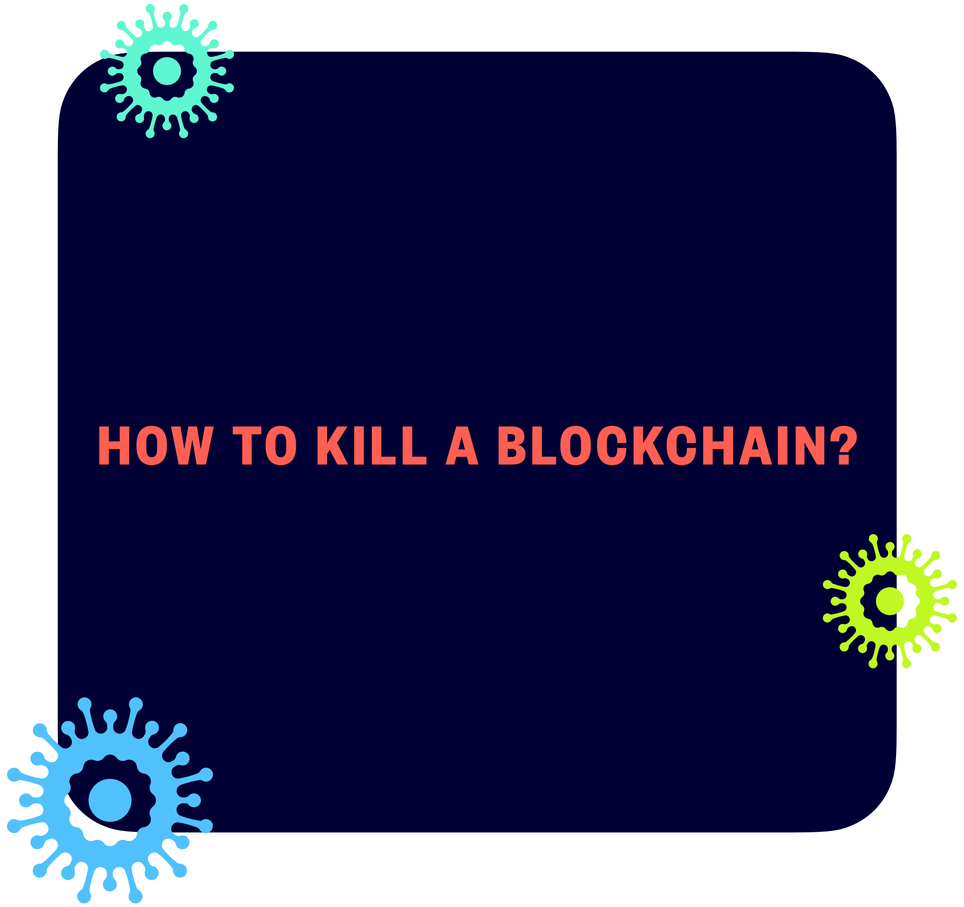
TIBA



LIMITATIONS

Vulnerabilities

TIBA



VULNERABILITIES

Vulnerabilities

TIBA

51% ATTACK	SYBIL ATTACK	ECLIPSE ATTACK	SELFISH MINING ATTACK	MINING MALWARE	TIMEJACK ATTACK	MEMPOOL ATTACK
CENTRALIZED MINING	CRYPTOGRAPHIC TRACKING	HUMAN ERROR	DDOS ATTACK	FINNEY ATTACK	RACE ATTACK	CONSENSUS DELAY
THE DAO ATTACK	PARITY MULTISIG WALLET ATTACK	EXCHANGE HACKS	SOCIAL ENGINEERING	SOFTWARE FLAWS	CENTRALIZED WALLET KEEPING	DOUBLE SPENDING ATTACK

Vulnerabilities

TIBA

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK

If one wants to know what 51% attack is,

One should understand how blockchain works first…..

Vulnerabilities

TIBA

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK

PROOF-OF-WORK, OR POW,

IS THE ORIGINAL CONSENSUS ALGORITHM IN A BLOCKCHAIN NETWORK.

IN BLOCKCHAIN, THIS ALGORITHM IS USED TO **CONFIRM TRANSACTIONS** AND **PRODUCE NEW BLOCKS TO THE CHAIN**. WITH POW, MINERS COMPETE AGAINST EACH OTHER TO COMPLETE TRANSACTIONS ON THE NETWORK AND GET REWARDED.

IT FOLLOWS THE RULE OF “DECISION WILL BE MADE BY THE MAJORITY”

So what if I am the majority???

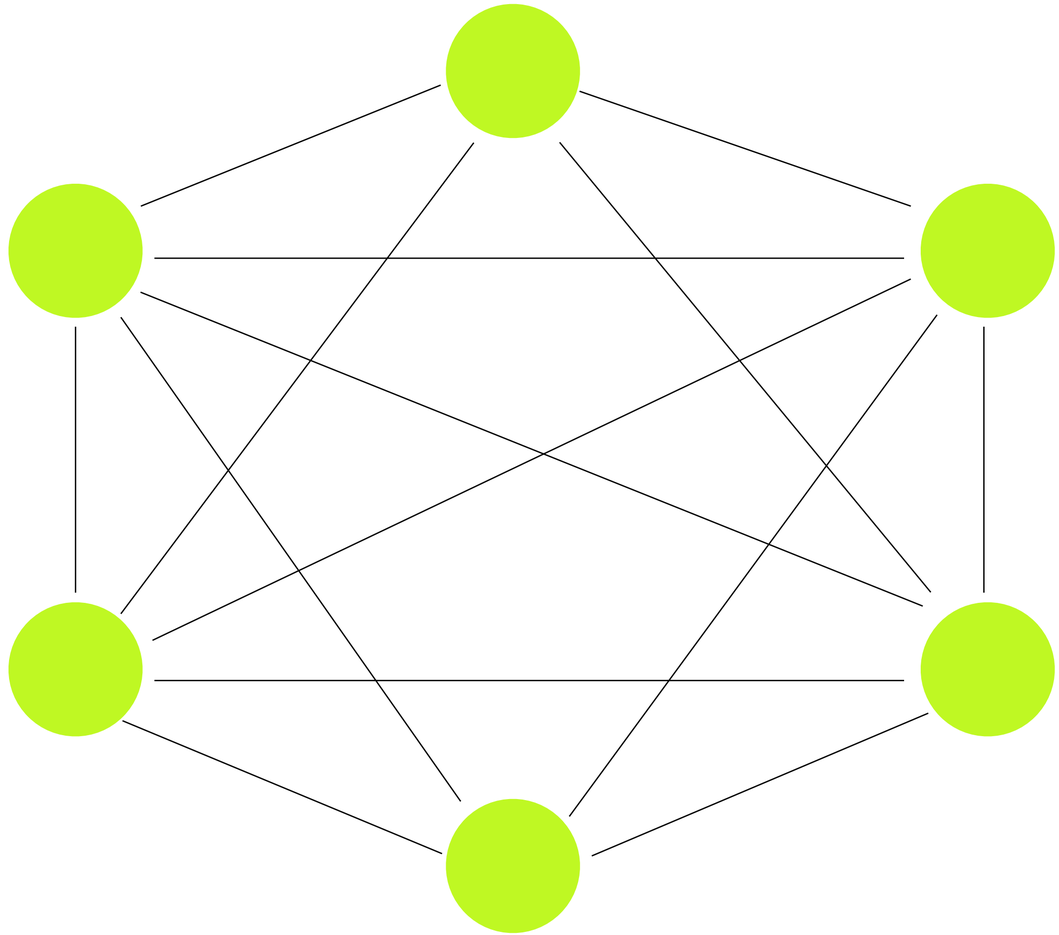
Vulnerabilities

TIBA

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK



HEALTHY STATE

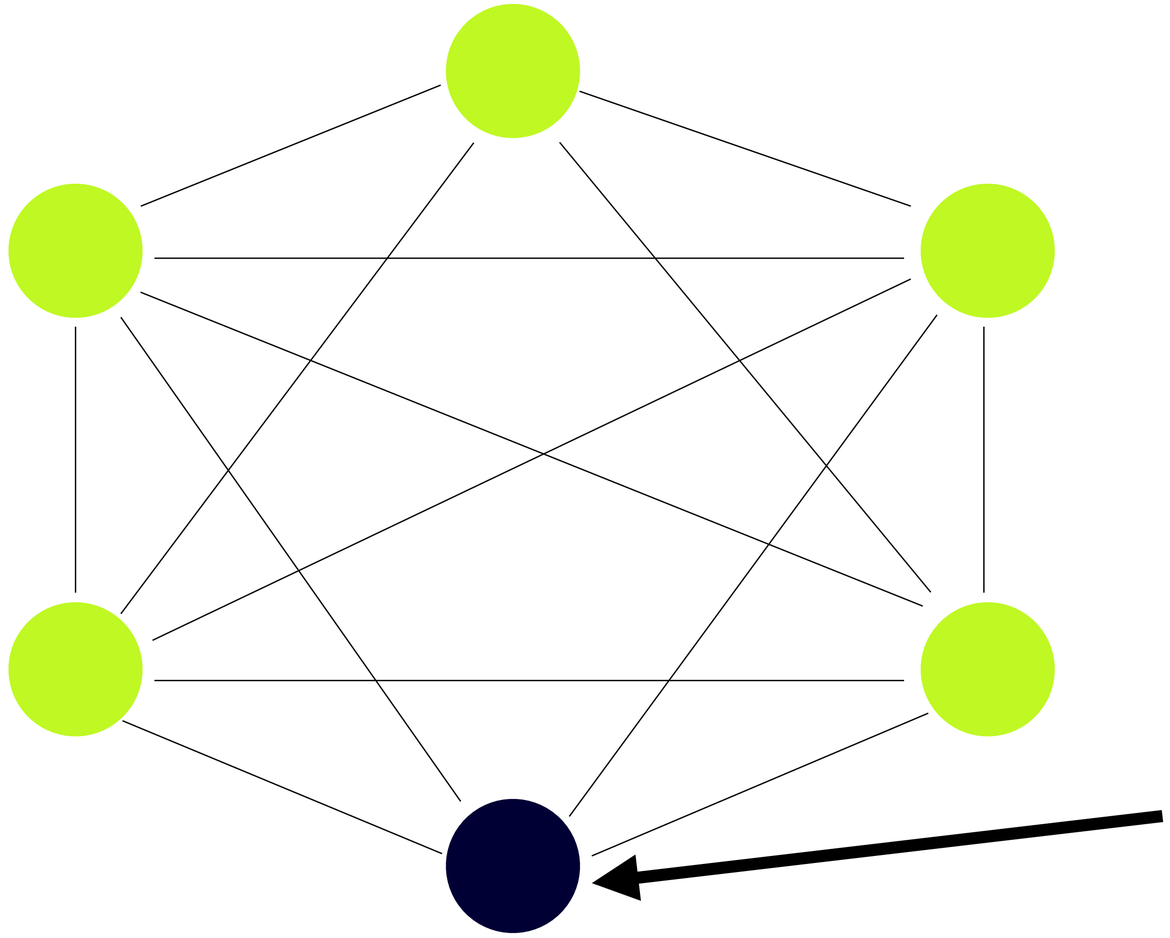
Vulnerabilities

TIBA

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK



If a node is being hacked or destroyed,

the other 5 nodes can use their own ledger to indicate the this node is a ‘fault node’.

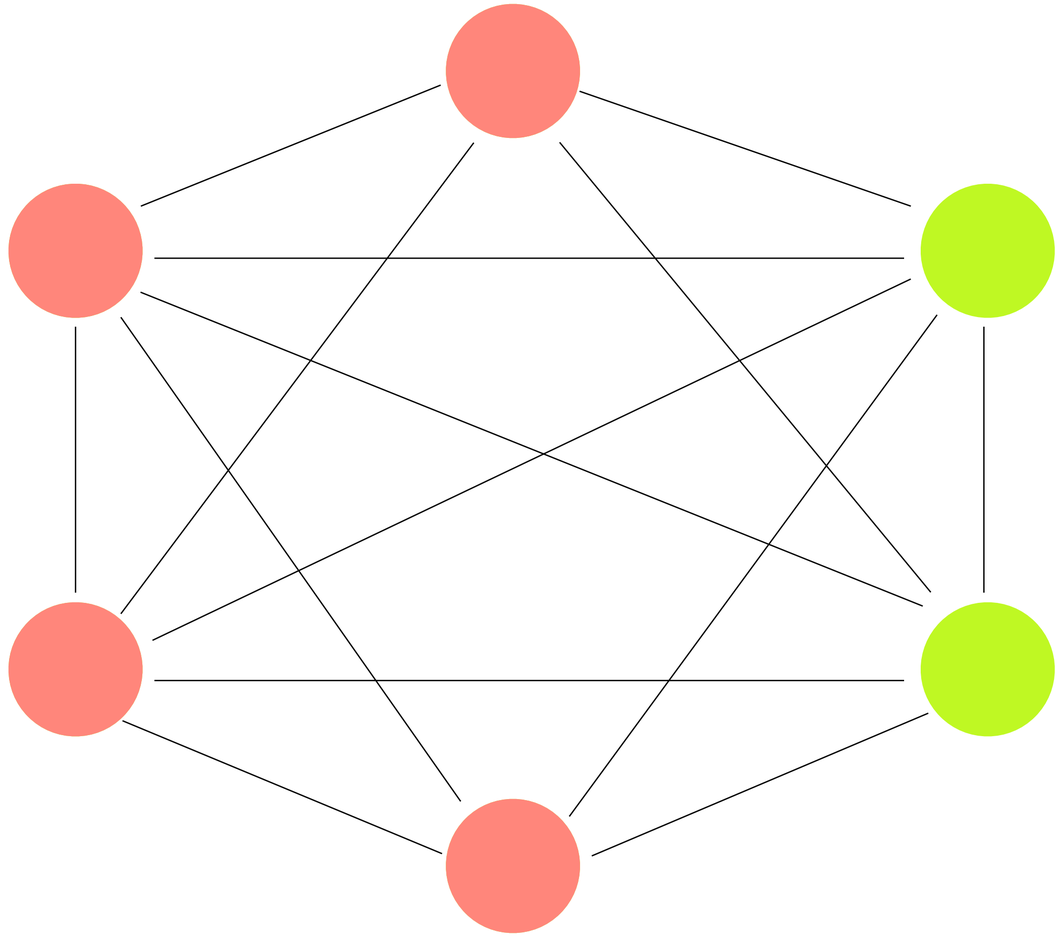
therefore the node will be erased from the network

Vulnerabilities

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK



I AM RICH AND POWERFUL, I HAVE THE MOST COMPUTING POWER IN THE WORLD.

I OWN 4 NODES IN THIS NETWORK!

THEREFORE IF I MAKE MY NODES TELL THE NETWORK I OWN EVERY COIN IN THIS NETWORK,

THEN THE OTHER TWO NODES CAN BE ELIMINATED AND ALL THE COINS WILL BECOME MINE

Vulnerabilities

TIBA

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK

WHAT IS A 51% ATTACK?

A 51% ATTACK REFERS TO AN ATTACK ON A BLOCKCHAIN—MOST COMMONLY BITCOINS, FOR WHICH SUCH AN ATTACK IS STILL HYPOTHETICAL—BY A GROUP OF MINERS CONTROLLING MORE THAN 50% OF THE NETWORK'S MINING HASH RATE OR COMPUTING POWER.

THE ATTACKERS WOULD BE ABLE TO PREVENT NEW TRANSACTIONS FROM GAINING CONFIRMATIONS, ALLOWING THEM TO HALT PAYMENTS BETWEEN SOME OR ALL USERS. THEY WOULD ALSO BE ABLE TO REVERSE TRANSACTIONS THAT WERE COMPLETED WHILE THEY WERE IN CONTROL OF THE NETWORK, MEANING THEY COULD DOUBLE-SPEND COINS.

Vulnerabilities

TIBA

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK

A Beijing Based Company who design ASIC chipped mining machines for blockchain minings.

ASICS(APPLICATION SPECIFIC INTEGRATED CIRCUITS)

ASICS ARE SO POWERFUL THAT ONCE A COIN-SPECIFIC ASIC IS RELEASED, IT IS USUALLY UNPROFITABLE TO MINE WITHOUT ONE, ACCORDING TO A REPORT BY LOKI NETWORK.

THE IDEA OF THE CENTRALIZED MINING

BASICALLY A PERSON OR A COMPANY OWNS A LOT OF HASHING POWER THAT THIS OWNER HAS A REALLY HIGH CHANCE OF MINING THE NEXT BLOCKS.

EX. IF A PERSON HAS 10% OF THE GLOBAL HASHING POWER, THEN IT IS LIKELY THAT WHEN EVERY 10 BLOCKS ARE MINED, THERE IS ONE BLOCK THAT BELONGS TO THEM.

This might cause **51% ATTACK**

For more info: https://www.investopedia.com/investing/why-centralized-crypto-mining-growing-problem/

JINWOO SEONG, JUNE 29TH

Vulnerabilities

TIBA

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK

In 2016, there is a smart contract called DAO, and it possibly had one of the largest crowd fund, which was 120 million dollars.

Everybody was hyped about the beginning of Fintech, but the truth is, an attacker drained 70 million dollars from the crowd fund by using a contract bug.

So

What's Smart contract?

What's the DAO?

How did he hack?

Vulnerabilities

TIBA

What's Smart contract?

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK

```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

  /* Initializes contract with initial supply tokens to the creator of the contract */
  function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

  /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```

It's just codes!

BUT, ITS BLOCKCHAIN CODE, THEREFORE: IT'S IMMUTABLE AND PERPETUAL

Vulnerabilities

TIBA

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK

What's the DAO?

```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

  /* Initializes contract with initial supply tokens to the creator of the contract */
  function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

  /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```

x1000

Vulnerabilities

TIBA

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK

What's the DAO?

A DAO IS A DECENTRALIZED AUTONOMOUS ORGANIZATION.

ITS GOAL IS TO CODIFY THE RULES AND DECISION MAKING APPARATUS OF AN ORGANIZATION, ELIMINATING THE NEED FOR DOCUMENTS AND PEOPLE IN GOVERNING, CREATING A STRUCTURE WITH DECENTRALIZED CONTROL.

How does it work?

A GROUP OF PEOPLE WRITES THE SMART CONTRACTS THAT WILL BE RUNNING THE ORGANIZATIONS → GO THROUGH ICO, AND THE TOKENS WILL REPRESENT THE OWNERSHIP OF THE ORGANIZATIONS. → AFTER FUNDING PERIOD, THE ORGANIZATION WILL START TO OPERATE. → PEOPLE THEN CAN MAKE PROPOSALS TO THE DAO ON HOW TO SPEND THE MONEY, AND THE MEMBERS WHO HAVE BOUGHT IN CAN VOTE TO APPROVE THESE PROPOSALS.

Vulnerabilities

TIBA

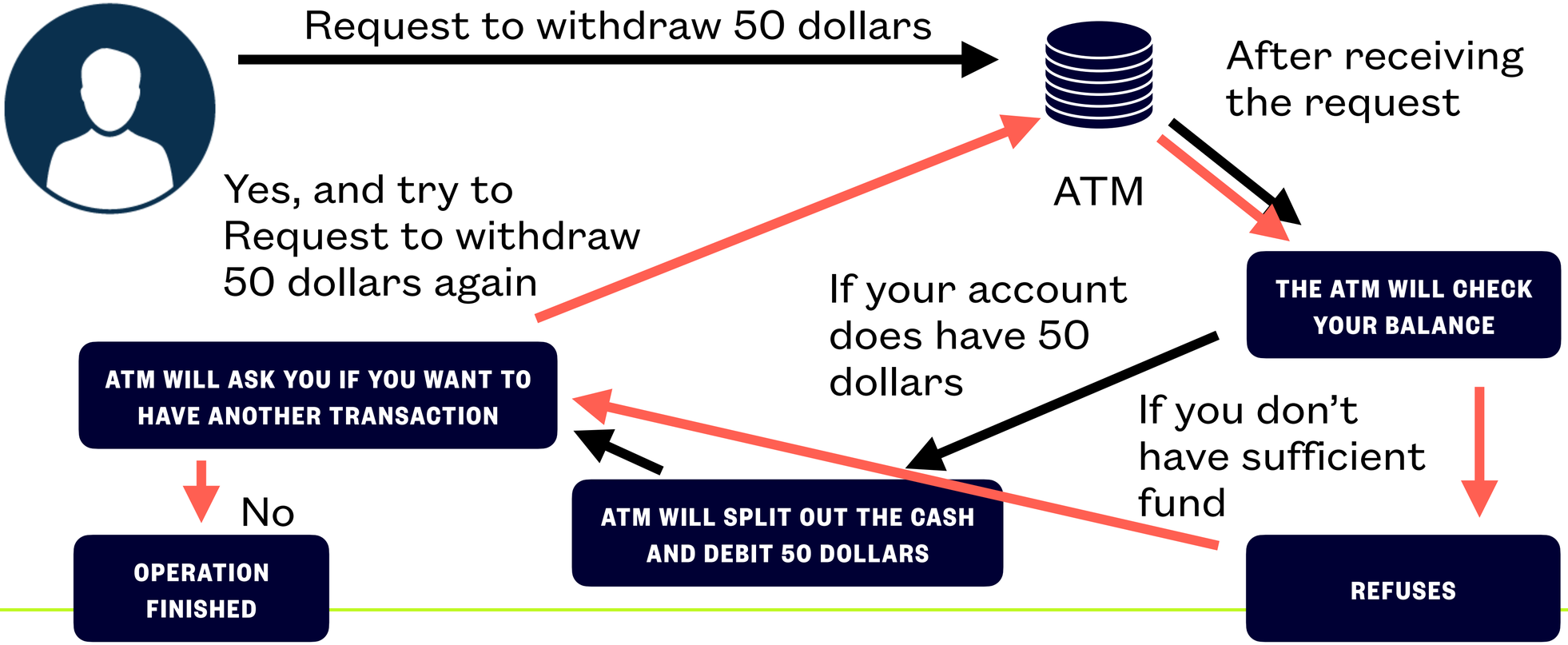
How did he hack?

Ex. You have 50 dollars in your account, and trying to withdraw from ATM

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK



Vulnerabilities

WHAT IF THE ATM ONLY CHECK YOUR BALANCE WHEN YOU FIRST REQUEST, AND DOESN'T CHECK IT AFTER THAT?

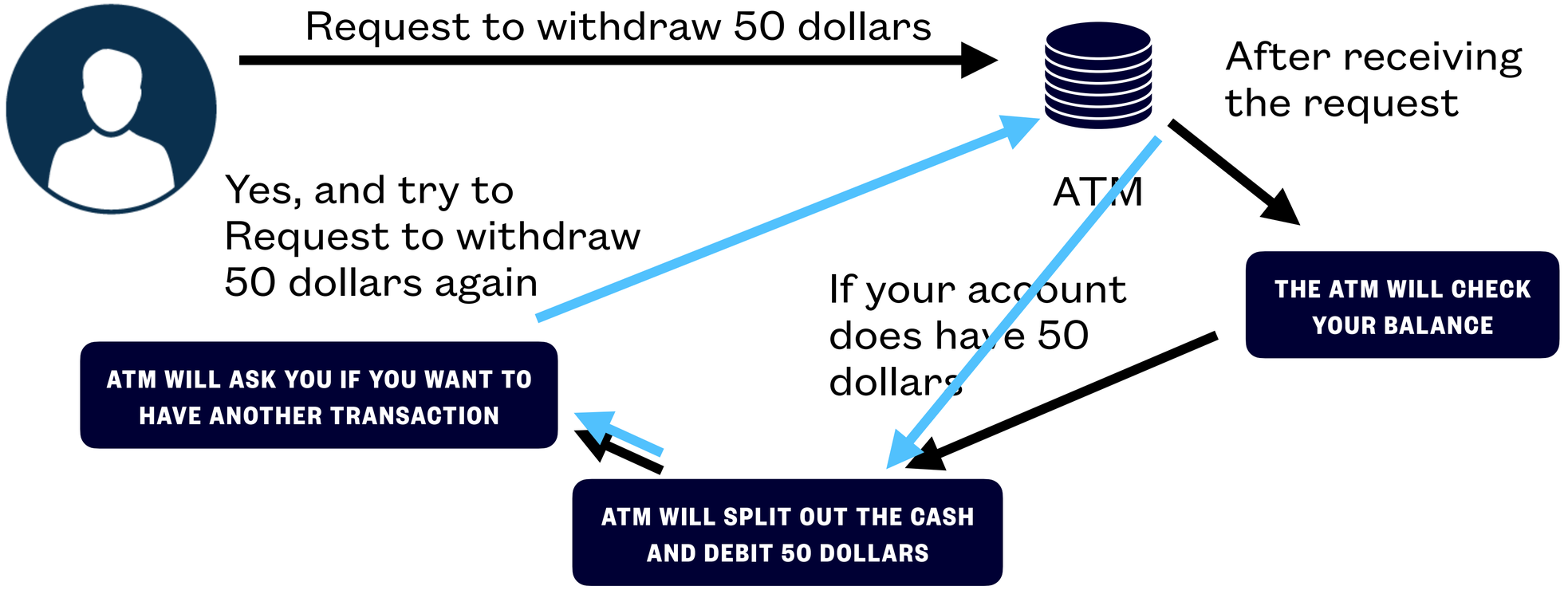
How did he hack?

Ex. You have 50 dollars in your account, and trying to withdraw from ATM

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK



Vulnerabilities

TIBA

51% ATTACK

CENTRALIZED MINING

THE DAO ATTACK

ABOUT DAO ATTACK

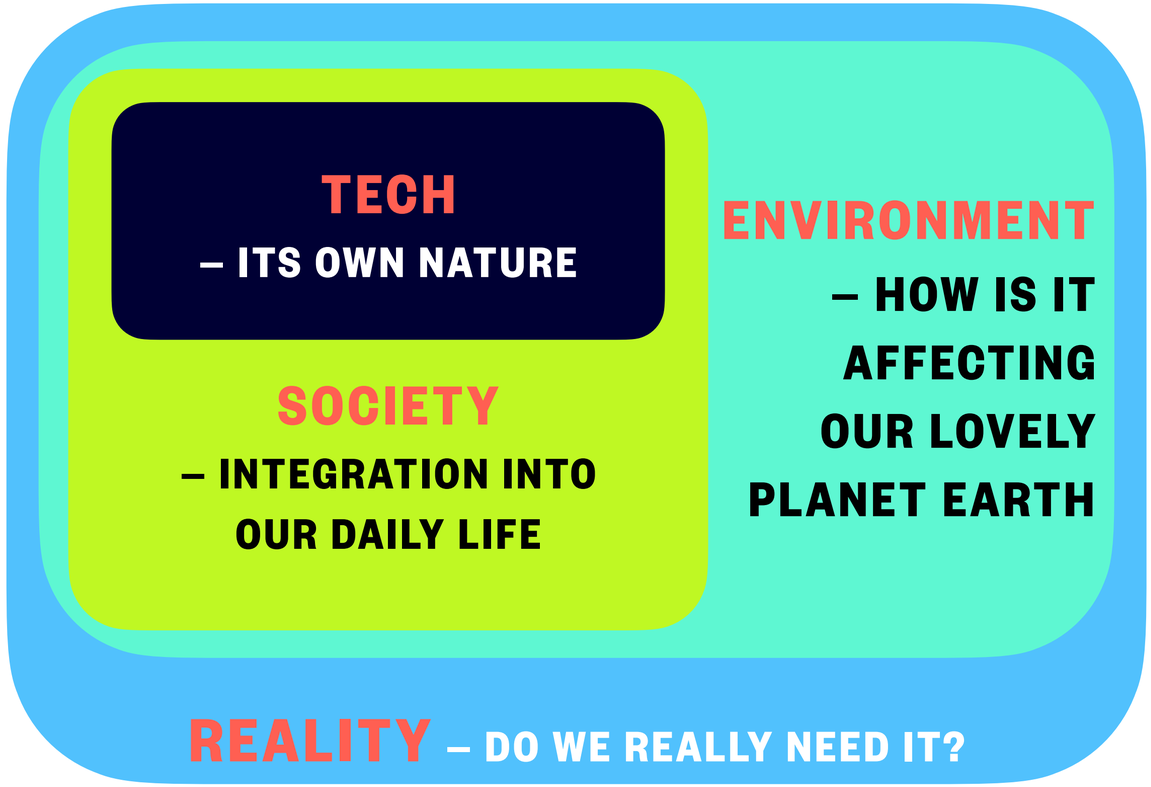
IT IS AN ATTACK THAT WAS POSSIBLE NOT BECAUSE OF THE PROBLEM OF ETHEREUM BUT THE CONTRACT THAT IS BUILT ON TOP OF IT.

AND THE ORGANIZATION WAS NOT ABLE TO FIX THE PROBLEM IN TIME DUE TO THE REASON THAT IT WAS NOT ABLE TO GET ENOUGH VOTES FOR SUCH AMENDMENT.

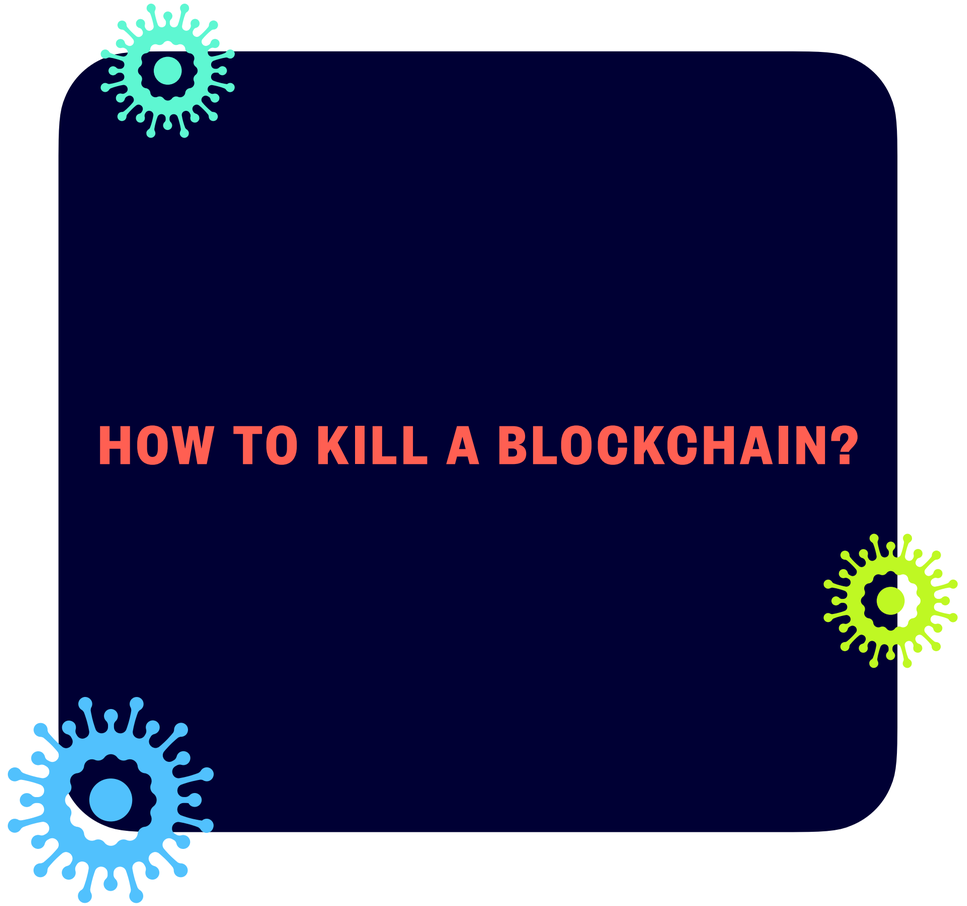
More resources: https://www.coindesk.com/understanding-dao-hack-journalists

Topics - Conclusion

TIBA



LIMITATIONS



VULNERABILITIES

Topics - Conclusion

TIBA

Blockchain is still an immature technology,

But it’s the bright side of it that brought us all here today,

Despises all the Limitations and Vulnerabilities I mentioned before,

There is still so much of blockchain’s potentials that we haven’t discovered…

Thank you all for listening !