

FC'19 / Financial Cryptography and Data Security 2019
February 18–22, 2019
St. Kitts

Igor Artamonov

Decentralization for public blockchains

Why it's critical for blockchain adoption

About Author

Was a lead of Ethereum Classic development since the fork and made Ethereum Classic happen

Currently doing tech consulting and working on [Emerald Wallet](#)



Ethereum Classic Development

- I was one of the first few people who joined Ethereum Classic, before The DAO fork of ETH
- I believe in blockchain principles such as immutability and decentralization
- Found a ballot fork and transaction reversal in interest of core team as unacceptable act of ruining blockchain ideas
- To show my position I started to contribute to the original code, launched a block explorer, eventually build a team of software engineers to work full time on Ethereum Classic core projects

Since December 2018 I'm not working on
Ethereum Classic protocol or core projects,
i.e. not engaged in Ethereum Classic

All I say is my personal opinion

Blockchain

A globally distributed
Database or **Computer**
without a trusted 3rd party

Is it effective?

- Mastercard/Visa can process 5,000-50,000 operations per second
- Bitcoin is limited to 3-7 operations per second
- Bitcoin is less effective 1,500 times
- Same comparison of Ethereum to AWS gives 1,000,000 times less
- Or, in other words, it cost x1,000,000 times more for the same processing

**Why are we paying
this price?**

We are paying for avoiding a central point

For decentralization of our database,
computation, payments, agreements, etc

**Let's talk about
decentralization**

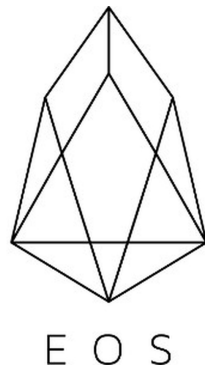
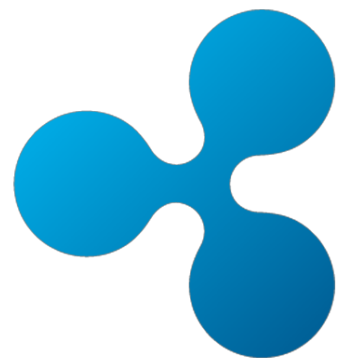
- First of all, blockchain as a physical network seems to be enough decentralized
- But blockchain is more than a peer-to-peer network, it's a whole infrastructure behind it
- This infrastructure has many ways to affect network participants
- Some parts of the infrastructure are centralized or tend to centralization

First check

Which one is centralized, which is decentralized?

- Bitcoin
- Ethereum
- EOS
- Ripple

We will probably all agree that Bitcoin is most decentralized and Ripple is least decentralized, in this set of blockchains



Decentralized →

Factors

that affect decentralization

Internal

- Premine
- Foundation
- Official Team
- Leader
- Development tax
- Official code

External

- Whales
- Mining pools
- Nodes concentration

Premine/Presale

Not a big problem, unless it's big enough to have political weight



Foundation

- Everyone expects the foundation will do development, sponsor research, make decisions, etc. Everything became dependent on foundation
- It concentrates power and decides for everyone what is right path, what is not.
- It decides which fork, in case of community split, is right one. See ETC/ETH split

Leader

- Leader is by definition is a power and also a ~~weak~~ point of failure
- Makes even more problem than foundation, because nobody argue with a leader, it's a disrespect
- Satoshi is the perfect leader btw, he just disappeared at the right time



Core Team/Code

Below is the code from Parity Ethereum unofficial client.
At this particular case the code was forced to comply with the code written for an official client, though if wasn't justified by a specification

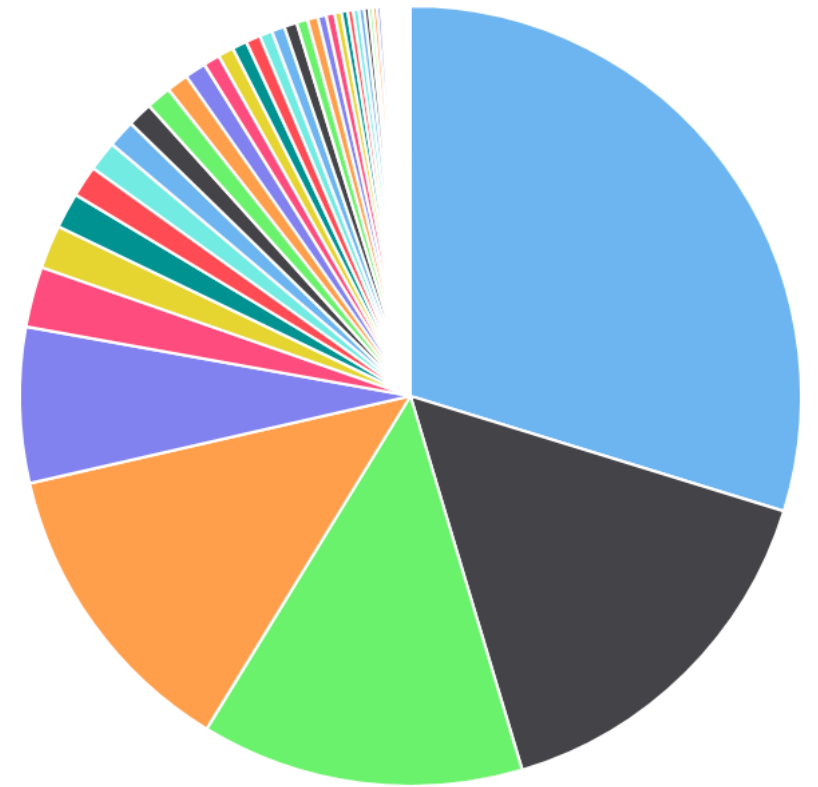
```
646
647     #[test]
648     fn should_agree_with_vitalik() {
649         use rustc_hex::FromHex;
650
651         let test_vector = |tx_data: &str, address: &'static str| {
652             let signed = rlp::decode(&FromHex::from_hex(tx_data).unwrap()).expect("decode");
653             let signed = SignedTransaction::new(signed).unwrap();
654             assert_eq!(signed.sender(), address.into());
655             println!("chainid: {:?}", signed.chain_id());
656         };
657
```

Whales

- Just price manipulation is toy wars, but whales can also drastically change development path
- See BCH/BTC/BSV. Groups of whales had disagreement with “core team” and made a fork, with enough capital it became more or less successful

Mining Pools

- 51% attack. ETC is a an example where it happened in practice
- At some point pools will realize that they can make money on providing a service to penalize specific transactions
- Pools can also sabotage or spam network, and charge for that as well
- We saw examples when it has political weight in BCH/BTC split























Nodes concentration

- In an ideal world every user will have own full node
- Unfortunately it doesn't work yet because a full node requires advanced knowledge and is a resource intensive software
- Even businesses depend on central providers like Infura
- Central provider decides which fork is right, which transaction is acceptable, and so on

**Every blockchain
seems to be centralized**

If we'll come to decentralization metric from 0 to 1, where 1 is fully decentralized blockchains, I believe than average value for the top 10 blockchains will be even less than 0.5, likely less than 0.25

1	 Bitcoin	\$63,777,505,257	\$3,636.08	\$6,199,524,369	17,540,187 BTC	0.23%	
2	 Ethereum	\$12,877,720,824	\$122.79	\$3,013,012,633	104,876,843 ETH	0.40%	
3	 XRP	\$12,449,212,485	\$0.302106	\$431,766,250	41,208,093,050 XRP *	-0.17%	
4	 Litecoin	\$2,603,175,191	\$43.04	\$1,053,461,017	60,487,825 LTC	1.91%	
5	 EOS	\$2,549,621,686	\$2.81	\$825,981,401	906,245,118 EOS *	0.92%	
6	 Bitcoin Cash	\$2,156,743,088	\$122.37	\$196,342,742	17,624,225 BCH	-0.07%	
7	 Tether	\$2,030,247,961	\$1.00	\$5,034,685,920	2,021,459,017 USDT *	-0.01%	
8	 TRON	\$1,605,815,156	\$0.024082	\$122,081,802	66,682,072,191 TRX	-0.10%	
9	 Stellar	\$1,514,909,985	\$0.079005	\$170,409,952	19,174,868,660 XLM *	1.85%	
10	 Binance Coin	\$1,301,635,956	\$9.22	\$80,368,717	141,175,490 BNB *	1.15%	

Bitcoin

- Premine - kind of
- Foundation - no
- Team - not very centralized, but people think it has some issues with centralization
- Leader - no
- Development tax - no
- Core code - yes
- Whales - yes, not a big control, but we saw them in BCH/BTC split
- Mining pools - not so much centralized (4 pools ~ 50%)
- Nodes centralization - no

Ethereum

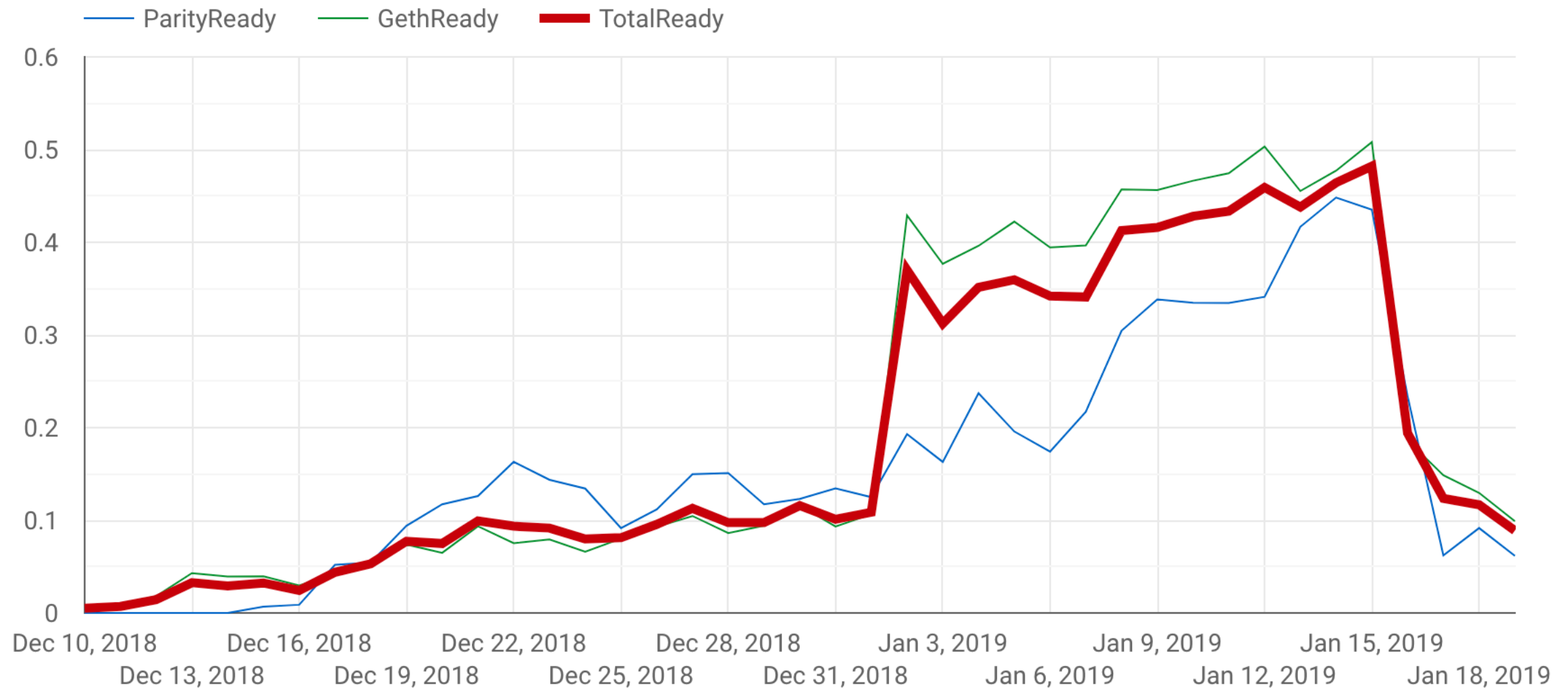
- Premine - **yes, 70%** of current supply
- Foundation - **yes**
- Team - formally no, but **in fact one group**
- Leader - **yes**
- Development tax - **no**
- Core code - yes, though they are trying to change it
- Whales - **yes**
- Mining pools - more or less centralized (3 pools > 50%)
- Nodes centralization - **yes**

**Maybe centralization
is good?**

Network preparations for Ethereum Constantinople hard fork.

Jan 1 - unnatural spike

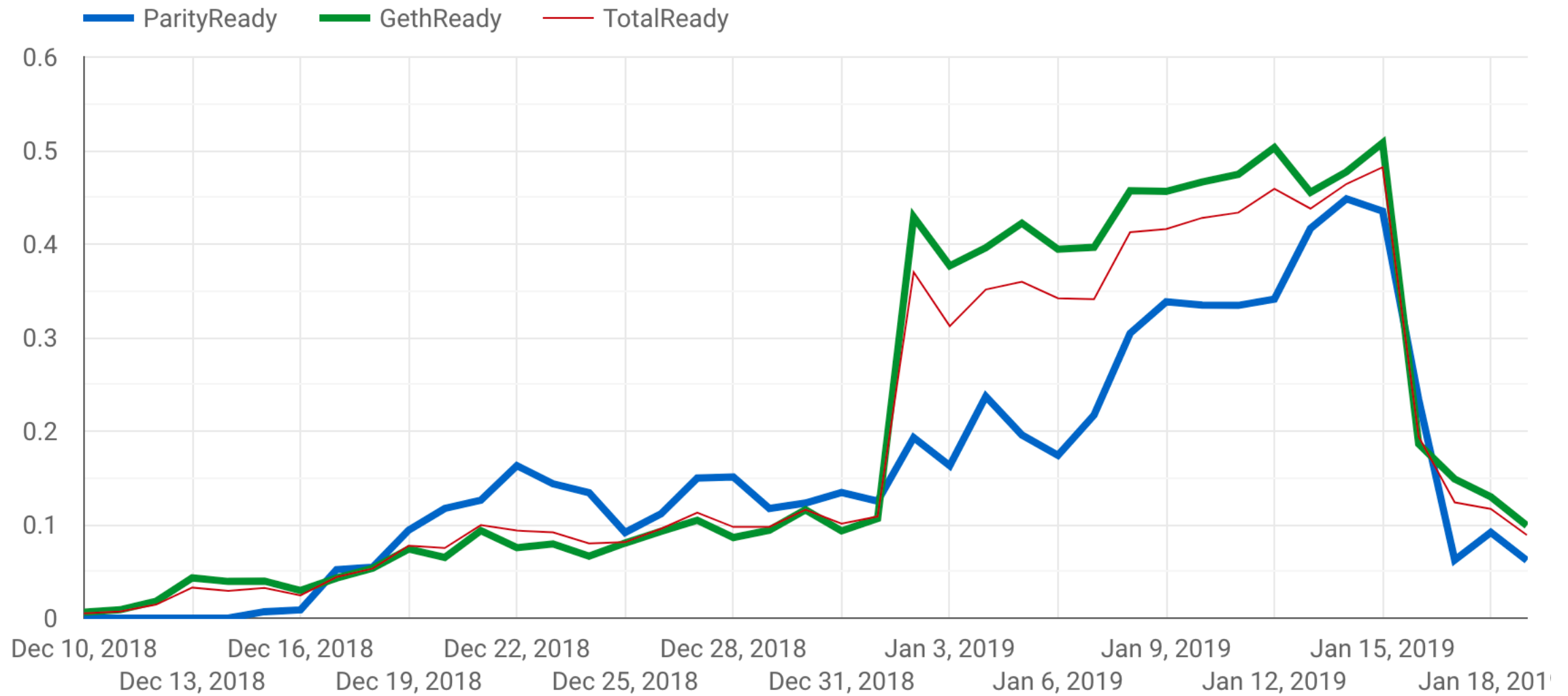
Jan 15 - bug was found, network downgraded, it's a coordination to avoid failure



Jan 1st:

- Parity (*unofficial client*) had natural growth
- Geth (*official client*) jumped

It seems that an external force pushed upgrade rate, and most interesting is that it has affected only official nodes. Thousand of nodes in one day



Maybe something like this forced most of the nodes to upgrade in that day:

```
[3:43:01 AM] Vitalik Buterin: ok can you guys stop trading  
[3:43:05 AM] Tristan D'Agosta: Okay
```

(That was a fragment from exchanges chat, when ETH found the hack of The DAO contract)

Centralized solution is usually more effective. Most of the current blockchains are centralized and are fine with that.

So what is the problem with centralization?

Central Point is a Point of Failure

But what kind of failure?

- Any central point can be used to get some advantage, it's a power, especially in a context of money
- Control of a public blockchain is a **power** which governments, big corporations and criminals want to control
- **Humans are weak**, they are especially exposed if they are part of that central point





- Most people think it's impossible to force any changes, "*because Open Source*"
- Unfortunately not every problem easy to notice. Otherwise we wouldn't have software bugs
- **Some backdoors can intentionally planted in a code and pass all verifications, only authors would know how to use them.**
- **There're many examples**

NSA BULLRUN

- Information about the program's existence was leaked in 2013 by Edward Snowden
- NSA has been actively working on inserting vulnerabilities into commercial encryption systems.
- One of planted vulnerabilities was a backdoor added to random number generator Dual_EC_DRBG

Juniper Backdoor

- Juniper replaces secure ANSI X9.31 to less secure Dual_EC
- And changed other parts of software at the same time, like [seems to be intentionally] added some bugs in different places
- Altogether it allowed to decrypt and listen to traffic

BEA-1

- Backdoored Encryption Algorithm, version 1. Paper “*Proposal for a Backdoored AES-like Block Cipher*”, Arnaud Bannier and Eric Filiol, 2017
- Compliant with FIPS-140 requirements (US NIST standard for crypto) and resist to linear/differential attacks
- All looked good, but because of a hidden backdoor, it can be broken on a laptop

Is blockchain affected?

- Many people already don't trust ZCash because of "*Trusted Setup*", people think that someone has a "master key", and it's hard to prove opposite
- Power was already misused, we had transaction reversal, artificial inefficiency in the code to keep control over community, economic changes forced by power
- Many blockchain projects has violated a lot of laws, SEC rules, gambling laws, and so on. A government may prosecute founders or force them to cooperate, we wouldn't know if latter happened already



F15 Categorization



- *“Every disagreement can be solved by using pure power”*
- If a problem is big enough, the ultimate power is fighter jets, who has more of them is right
- Fighter jet can stop anything. Except blockchain, you can't stop it. Or can you?

The criteria:

“How many F15 you need to force changes”

**Let's check
blockchains again**

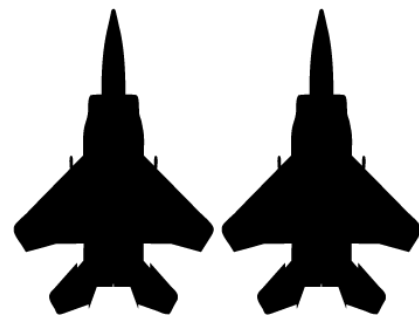
Blockstream Office Locations



- F15 are used to symbolize amount of external power that can affect blockchain infrastructure and decision in some way
- It's a subjective categorization, not real fighter jets



Most protected from an enemy power



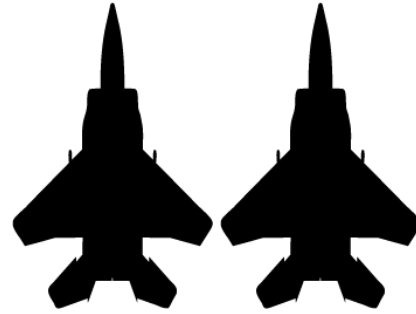
...



Least protected from enemy power



- Bitcoin
 - has a stable protocol, less depends on core progress currently
 - suspicious community and opposing to changes, ask tough questions
 - too many different forces/groups makes is ineffective to target one
- Monero
 - future still depends on core dev team
 - though it's pseudonymous and distributed
 - financing comes from different sources
 - hard to attack (but much easier than bitcoin)



- Grin
 - interesting new project, right first steps
 - vulnerable only because it's young and small
- Dogecoin
 - there is literally no one in charge! much unstoppable



- Ethereum
 - known leaders and financing
 - code needs a lot of changes before maturity
 - many central points/many vulnerabilities
- Ethereum Classic
 - unfortunately now is just one coordinated group which controls everything, from code to finances, media, community, etc
- ZCash
 - control is too concentrated as well, tech is sophisticated for a broad community to be involved



For the most of other blockchains you don't need any power at all, you just call CEO and make an agreement. Zero F15.

***“But we’re using blockchain
just for some basic and
legal stuff, who cares?”***

I want to remind that

**Internet was launched
and designed to survive
nuclear war. Literally.**

- Internet was made by DARPA - Defense Advanced Research Projects Agency or US Department of Defense
- TCP/IP is also known as “*DoD Four-Layer Model*”, where DoD is Department of Defense



- Memorandum on Distributed Communications by Paul Baran from RAND Corp
- Research a network that can survive an enemy attack
- Proposed packet-switching, and other things that became a basis of modern internet

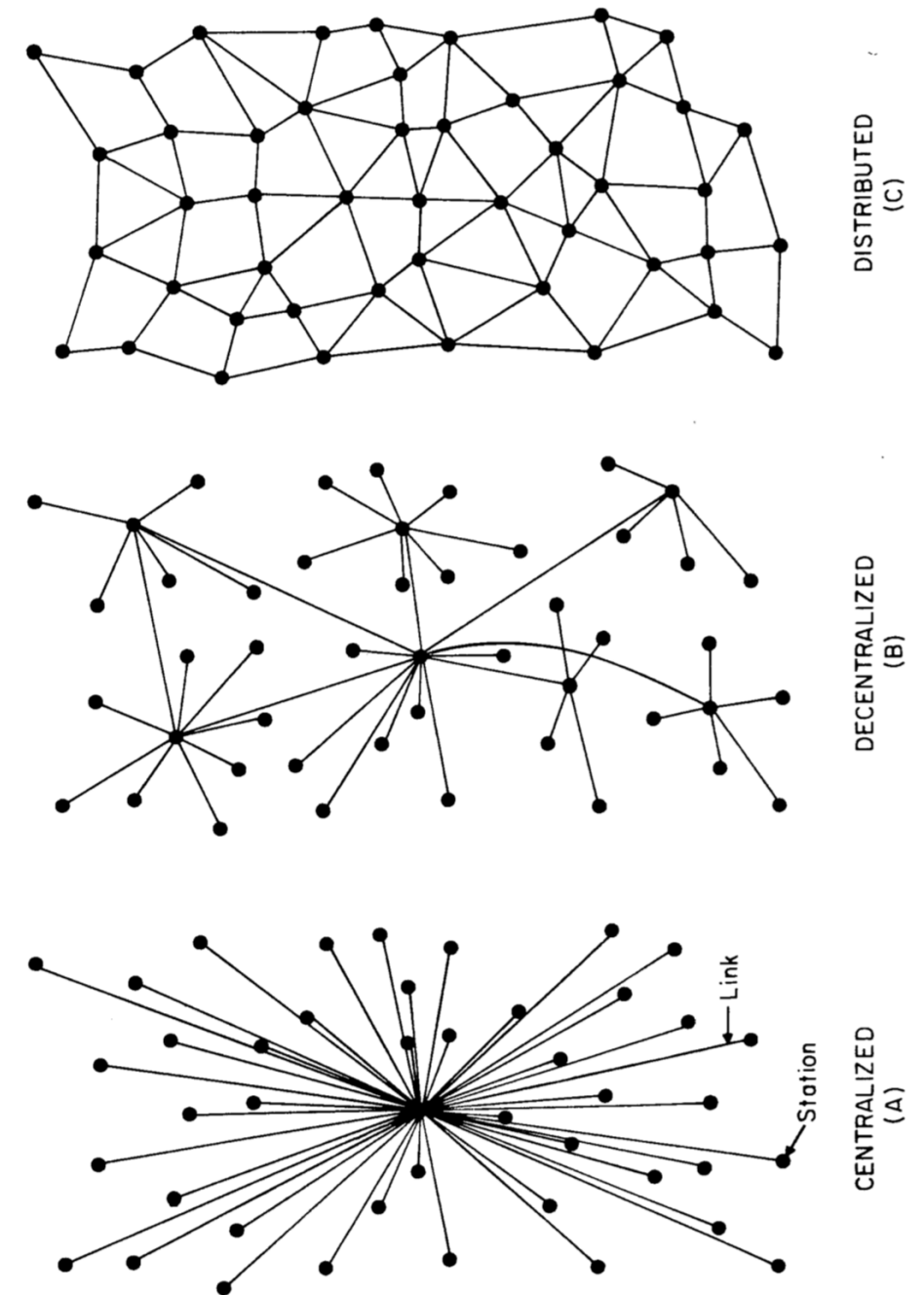


FIG. 1 — Centralized, Decentralized and Distributed Networks

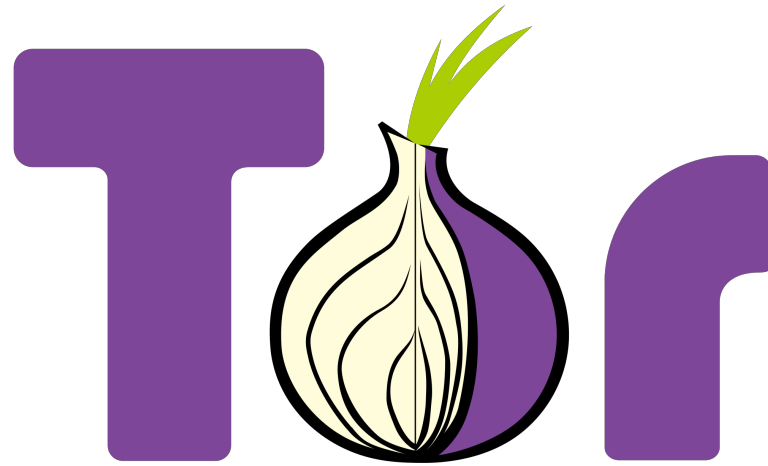
MEMORANDUM

RM-3420-PR

AUGUST 1964

ON DISTRIBUTED COMMUNICATIONS:
I. INTRODUCTION TO
DISTRIBUTED COMMUNICATIONS NETWORKS

We will soon be living in an era in which we cannot guarantee survivability of any single point. However, we can still design systems in which system destruction requires the enemy to pay the price of destroying n of n stations. If n is made sufficiently large, it can be shown that highly survivable system structures can be built--even in the thermonuclear era. In order to build such networks



- Initial funding for Tor's development has come from the federal government of the United States, initially through the Office of Naval Research and DARPA
- *“After analyzing documents leaked by Edward Snowden, The Guardian reported that the NSA had repeatedly tried to crack Tor and had failed to break its core security”*

- Most of modern internet was build by defense organizations, designed for extreme conditions like surviving a nuclear war
- But is being used to post photos on Facebook
- **Such extreme criteria allowed to build a network that can be an universal communication layer for everything**



Blockchain
networks



Peer 2 Peer
networks



Internet
network

A public blockchain cannot be controlled by a single party (“country”), because there’re few of them who wants power

A global public communication network can succeed only if it controlled by no one (i.e. “decentralized” and F15-survivable)

Thank you!

Igor Artamonov

igor@artamonov.ru

@splex