

Forum:[Hack Forums](#)

Thread: [Decentralization Defined & Its Significance](#)

Kill Joy - August 13, 2017, 2:25 am

Introduction

A lot of people believe they understand what the word decentralized means in relation to a digital currency such as Bitcoin. Well I am here to tell you that you are probably wrong in your belief. If you don't understand what decentralized means, please continue reading.

Key Words to Understand

Centralized - A single authority controlling, directing, and making decisions. Take for an example, the United States government. The U.S. Dollar is printed by the U.S. Mint with the permission of the U.S. Congress. This is declaring that the U.S. Dollar is backed by the government and can therefore be trusted by anyone underneath the government. If the U.S. government disappears, so does the U.S. Dollar. In computer-related terms we can say that one machine is telling what all the other machines should do.

Decentralized - A system in which no single person, institution, or machine is telling what others should do. Bitcoin is an example of a decentralized currency due to the fact money is no longer printed and given value by the institution, but rather created and given value by the people using it. In computer-related terms, this means there is no specific machine needed for it to work.

Distributed - Essentially is the same definition as decentralized but can now be spread out on multiple machines. This doesn't mean if a machine stops working the whole system does.

Three Types of Decentralization

When it comes down to it, decentralization and centralization can be categorized by three different types. Architectural (de)centralization - How many different physical systems make up the network and how many can stop working at any given time without the network shutting down? If we have 10 computers, how likely is it for one computer to go down? How likely is it for 5 computers to go down?

Political (de)centralization - How many individuals or institutions control the network?

Logical (de)centralization - Does the network look like a jumbled mess or does it look like a well-structured design? If the design was cut in half, would the system still be able to function as normal in two separate instances?

Spoiler ([Click to View](#))

Blockchain technology is at the root politically decentralized and architecturally decentralized, but they are logically centralized.

Why Decentralization is Important for Cryptocurrency

If you understand what Decentralization means, you may not know why it is important and why it is so popular with Cryptocurrencies. In the beginning of this thread we talked about the U.S. Government and the U.S. Dollar being centralized. Centralization makes it very easy for the controlling party to determine most anything for the system, whether it be good or malicious intent.

Attack Resistance - Networks that are decentralized are often not economically beneficial to attack. The reason for this is due to the fact there are no crucial central control points to attack. The economic size surrounding the system is much larger; therefore, being much more expensive to attack. Let's say that an attacker manages to control 51% of a blockchain. It would still would not be economically beneficial for the attacker to harm the network as the value within the network would plummet.

Collusion Resistance - Since the U.S. Government is centralized and the controlling system for the U.S. Dollar, members and leaders have the ability to collude together to change, disrupt, or destroy the U.S. Dollar depending on their own self interests. With a decentralized system, colluding together becomes much harder as you would need to control more than half a network to technically control the network.

Fault Tolerance - Decentralized networks are less likely to fail due to the fact that there are so many different machines that make it up. It would be hard to target each individual system to bring down an entire network. As we have already mentioned above, even cutting half of the network apart, both still would be able to function without the other. Even if an individual or institution had 51% of control of a network, Attack Resistance would still be a protecting factor.

[Further reading.](#)

There are still some factors within each of the above points that can potentially still be exploited, such as the Collusion Resistance. Still, with a decentralized system, it makes these points harder to exploit. I hope you all learned something new today. If you have any questions post them below and I'll answer them when I can.

regard - August 13, 2017, 2:36 am

Great read!

Keep up with these articles. Loving them! XD

Kill Joy - August 13, 2017, 2:37 am

(Aug 13, 2017 02:36 AM)regard Wrote: [\[CITE\]](#) Great read!

It should follow that IOTA's tangled structure would make it distributed rather than decentralized. IOTA is both distributed and decentralized. Same with Bitcoin.

Froggy - August 13, 2017, 12:39 pm

Informative thread! I'm starting to understand this shit a little more.

Don Genovese - August 13, 2017, 2:04 pm

Nice thread mate. Great read.

Charger - August 13, 2017, 2:06 pm

KJ with another quality thread about cryptos.

Very nice!

Kill Joy - *September 14, 2017, 1:41 pm*

Bringing this back up to spread the knowledge.