

Decentralization

Does it actually matter?

Decentralization

Does it actually matter?

Crypto is currently learning what a bear market is while the economy is about to face a recession. Ethereum is going through its second bear market whereas Bitcoin has done this about five times already. Many of the altcoins are down 90% or more, and we have just experienced the collapse of an entire blockchain ecosystem as well as the wipe-out of a top 5 coin.

This is when the weak get slaughtered and the strong survive, everybody is struggling and nobody feels fortunate. Enter the biggest names in crypto such as Celsius, BlockFi, Voyager, and oh so many hedge funds like Three Arrows Capital (3AC) that got liquidated and had to be bailed out or simply went bankrupt.

In this whitepaper, we focus on what is core to blockchain and its applications: Decentralization. The architecture that is core and part of so many buzzwords like Decentralized Governance, Decentralized Finance (DeFi), Decentralized exchanges (DEX), and Decentralized Applications (dApps).

But what does decentralization have to do with bankruptcies and the blowing up of the biggest names in crypto? A lot. In the following, we will evaluate how decentralization affects a system and how it differs from centralization – a difference which is most notable in times like this when things go wrong. We will also show how decentralization ultimately creates stronger foundations on which economies can be built upon.

What decentralization means

Decentralization is about ownership and control. If something is decentralized, it must not be ownable or controllable by one or just a few entities. It also must not be controlled by large entities such as companies or be regulated by any state.

The table on the next page shows the key differences between centralized and decentralized systems. So let's discuss these a little bit more in-depth: In crypto, a system is decentralized if changes to the rules or protocol are done by consensus and no single entity can



	CENTRALIZATION	DECENTRALIZATION
Ownership	 One to many	 Many (no controlling entity)
Decision-making	 Top-down	 Consensus
Decision time	 Fast	 Slow (requires majority)
Requirements	 Trust in decision-maker	 Distributed operation and control
Risks	 Corruption, exploitation	 Capture, concentrated ownership
Works well with...	 Competition	 Public goods, open protocols
Works badly with...	 Monopolies	 Individual products and services

make changes. This means that both ownership and operations need to be distributed among many entities in a way that no single unit has a controlling part in either.

Decentralization has two key attributes: Security and stability.

We can trust that the system will work as expected and in the best interest of most users as no majority would not accept the changes otherwise. This comes at the cost of a rigid system where decisions are slow and hard to be implemented and throughput is limited.

As a result, decentralized protocols are useful for things that are foundational infrastructure for many such as public goods like money, payment systems, and smart contracts. For applications built on top more centralized solutions are often better for they allow more nimble innovations. If such products and services can be built on decentralized infrastructure they can overcome a lot of the traditional overhead due to the safety and openness of blockchains.

With all that said, decentralization is not a black or white state but there are some key-thresholds that matter to achieve certain properties with their advantages as well as their disadvantages. For instance, if one entity has full control over a system, it is easy to make effective decisions, manage it and drive improvements. However, the controlling entity may have different motivations than other stakeholders. That creates the potential for exploitation and all kinds of problems. Put simply, this is usually about a controlling entity dominating the little guy. That is why in our society, we create rules and regulations to ensure everything functions to the benefit of all. Therefore, a centralized solution only functions with a good working society and the appropriate rules.

In short, centralized systems need to be regulated to work, such as property rights. The rules create trust and safety. That allows people to build things in peace and for the long-term benefit of society, which then leads to productivity and prosperity.

Humans have excelled at building systems within such a regulated environment, which is why we dominate the world of the living so dramatically. All this is only possible because we have centralized bodies that have control over things and can reap their rewards and thus ensure everyone is safe within our society. So why come up with a different way of running things? Why not rely on the rule of law and democratic procedures?

Our systems are quite inefficient and very expensive. For example, think of taxes. If you live in Germany, you will be paying close to half of what you earn as taxes plus 19% VAT on everything you spend on your already taxed money. In short, you end up retaining a small minority of the wealth you generate. Additionally, all these rules and regulations are not made for the digital age. As discussed in [The Value of Blockchains and Cryptocurrencies](#), those technologies have been invented long before even machines existed.

Blockchains run things differently. They facilitate the creation of value differently than our traditional economy enables by countries. Decentralization is a core part of that. It is a means to an end and allows things to function without the need for centralized hierarchical structures to enable its key advantages.

Decentralization in Bitcoin

When discussing decentralization in Bitcoin, we have to take a look at its two basic layers, user functionality and operations.

User functionality: From an end-user perspective, the functionalities Bitcoin provides are nothing new. It's just another digital asset and a payment network. In their essence, Paypal, banks, and stock brokers provide the same services. Decentralization only leads to

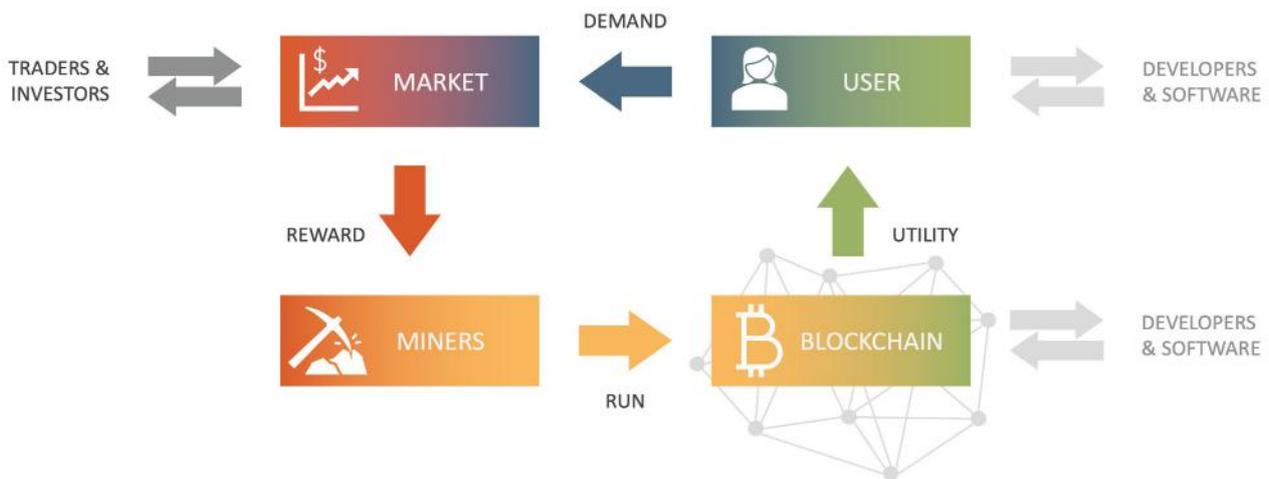
minor differences. For example, signing up for an account is quicker in crypto but getting your account back after you lost access is easier with a central service. Basically, decentralization does not make much of a dent for better end-user functionality.

Operations: Where Bitcoin differs vastly, is how digital assets and the payment network are managed and governed. The entire system is run by a decentralized network and protocol, meaning different Bitcoin stakeholders are sharing power and responsibility. Additionally, within each group of stakeholders (i.e. all the miners) work and power is decentralized, so they need to agree before changing anything. For instance, no single miner can choose to update the Bitcoin software. It takes a majority of miners to accept the change. After miners create a change, for example a fork, the market has to accept it, else the change will be ineffective. To give an example, the Bitcoin Cash BCH change proposed by miners was not accepted by the market and resulted in most miners jumping back on the old unchanged system.

Furthermore, the system is designed so that each stakeholder does what is in their best interest. All motivation is designed to work via the incentive of each individual. As long as everyone's best interest lines up with the job that needs to be done, the system keeps working properly. If that were not the case, the system would have a design flaw and not be safe.

For a better understanding how and why this system is successful, let's discuss the stakeholders of Bitcoin:

Users use Bitcoin because it gives them utility, i.e. they want to use Bitcoin to make transactions, store value, or invest in Bitcoin.



The stakeholders of Bitcoin: The market is the ultimate ruler. Everyone acts in their own best interest, and by design this just so happens to increase utility, which in turn increases adoption and leads to price appreciation. As all stakeholders benefit from higher rewards, this creates a positive feedback loop when new participants join and negatively affects the price when they leave. This is why adoption is so important.

The more use people get out of Bitcoin, the more they will use it and vice versa. This is represented by the market and price which will reflect the demand of users for the utility.

Miners get a fee for running nodes and building blocks, competing among each other for the block, and fee rewards. They also keep the network secure by validating all transactions and updating the ledger with all transaction history. If the price goes up, mining yields more rewards, and more miners will compete for it by providing energy and computing power to secure the network. Thus, a higher price creates more security which increases utility for users.

Developers and service providers build the software that miners and node operators run, as well as wallets and other tools for users so that using Bitcoin becomes easier and better over time.

All the stakeholders meet via the **market**, where all the incentives ultimately flow through. Everything gets better when the price goes up and stakeholders tend to get

hurt when the price goes down. Higher prices also attract more users and vice versa.

The decentralization hierarchy

With decentralization, there is a hierarchy of importance. The more power a stakeholder group has, the more it is important that it is decentralized. Since all power ultimately comes from the market price, the holders of the token, who make the ultimate price decision, are the most important. After that, there come the miners or validators who run the system, then the software, wallets and all the builders of the ecosystem.

Distribution of tokens: Holders and users set the price. The most important thing is that a broad and large user base comes to a consensus on what the price is. If few people have all the coins, the price can be manipulated or changed too rapidly when few actors “change their mind” or simply want to exploit their position. Thus, many users having coins as well as nobody having too many coins is important here. Notice also from a monetary perspective that tokens work best when

many people are using them, so both technically (or for security) and for functional value the token distribution is the most important aspect of decentralization.

Distribution of mining and validation:

Miners run and operate the system and can initiate changes to the protocol (forks). If few actors have control, they can act maliciously and make everything unsafe and untrustworthy for the rest of the users. This is why it is important that many miners and validators exist, and that not too many have too much of a share of the pie.

Distribution of development: The development of the protocol is also important to be decentralized, which means it is better if there are different versions and many people and teams are contributing to improving the system. It is not quite as critical, and Bitcoin would function if there were only one party doing this but it helps for safety and innovation if there are different version builders.

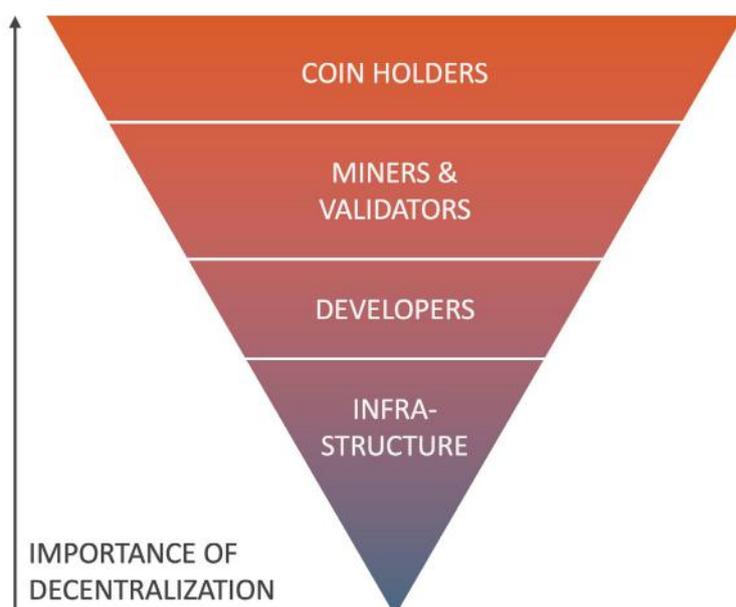
Distribution of software and tools: Again it would be possible to only have one Bitcoin software or wallet, and sometimes fewer

standards are better but it would be problematic if, for example, there was a bug in the one software and everything would stand still. So, having options also creates better security as well as usability.

What does it all mean?

Decentralization is a means to an end. It is something you do not see but without it, blockchains cannot function. The features that blockchains provide only work flawlessly if decentralization is in place. As such anybody using or building on top of blockchains should be aware of it. If we want to trust a blockchain we must know that the mechanics of it work and that they are sufficiently decentralized so that it cannot be attacked or manipulated. Only then can amazing functionalities be unleashed such as a bearer asset and a system that settles transactions right away. Autonomously, automatically, safe, and digital – those are powerful and valuable attributes we get with decentralization.

Let’s take a look at decentralization within the two most common cryptocurrencies before we briefly discuss other blockchains.



The decentralization hierarchy:

Decentralization amongst coin holders is the most important aspect of decentralization. Mining/validation is also extremely valuable in creating a decentralized system, followed by the open source development and breath of infrastructure provided. Bitcoin leads when it comes to infrastructure and integration into existing financial infrastructure, while Ethereum has more wallets with non-zero value and a more diverse developer ecosystem.

Bitcoin and Ethereum

Coin distribution

As mentioned earlier, the most important aspect for decentralization is the user base. When tokens are concentrated, there is risk of centralization which breaks the security assumptions of blockchains and the whole system is at risk of being useless and without value.

The number of active addresses for both Bitcoin and Ethereum have been growing steadily over time.

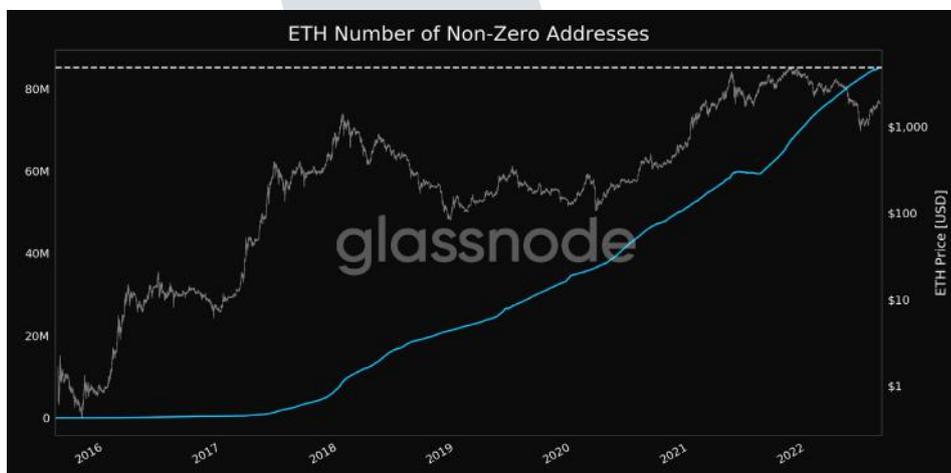
Another very important aspect however is the distribution of coins. Bitcoin and Ethereum have a very high concentration of coins among big accounts. Ethereum had an ICO,

and Bitcoin had a few years where most of the coins were gobbled up by a few miners including Satoshi. The question now is whether some of those coins are moving to new users?

Yes, they are. I think it is critical to acknowledge that medium to small holders seem to be growing steadily such as addresses holding one Bitcoin as well as smaller accounts. This is a good and important trend. It shows an ever wider distribution not just of coins overall but good distribution of users with significant value.

Mining distribution

Today, Bitcoin mining is fairly centralized with few entities dominating and even fewer entities producing the chips needed for mining.



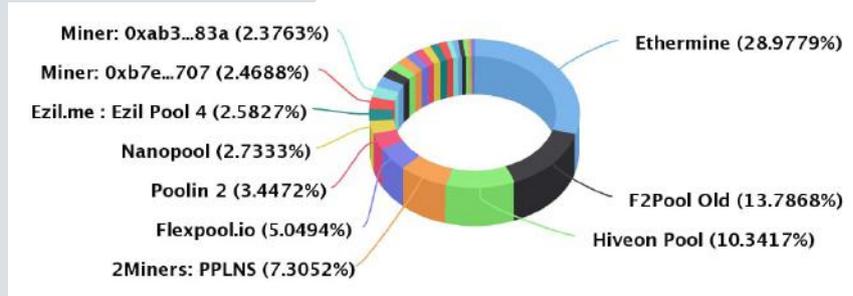
Non-zero addresses: The adoption of crypto currencies has been surprisingly consistent even in market cycles with prices to crashing 70-90%. Though this is a rough way to measure adoption, it provides a clear trend towards decentralization. | Source: [@glassnodealerts](https://twitter.com/glassnodealerts)



Addresses holding coins: Not only are small value addresses growing but also the number of addresses with significant value, such as the value of a car, are constantly increasing, even with a lot more volatility than wallets with smaller amounts. | Source: [@glassnodealerts](https://twitter.com/glassnodealerts)

Bitcoin mining is a zero-sum game. To mine profitably one needs an advantage over other miners because of the cost of electricity and energy as well as the hardware that is necessary for mining. We see in the hashrate distribution that a handful of miners control most of the mining power. So while the “one CPU one vote” idea from Satoshi was a great way to allow decentralization in the beginning, the mining of today is one key centralization risk factor of Bitcoin.

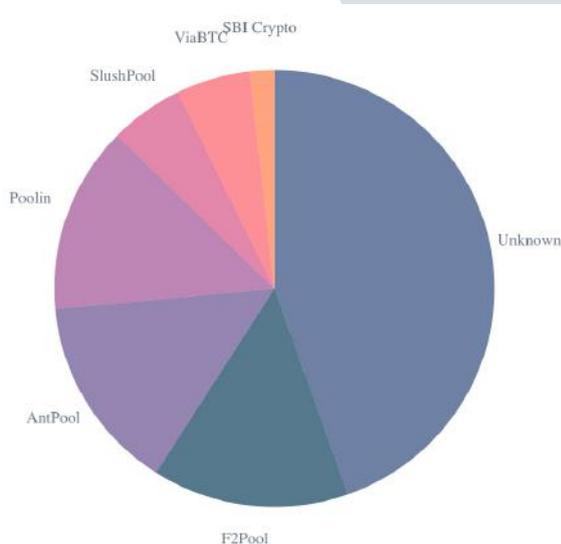
Ethereum needs to be looked at from a different perspective. It currently relies on GPU mining and works just like Bitcoin mining with the difference that anyone with a gaming PC or GPU can participate, while becoming a Bitcoin miner is quite a bit more complicated as established above. Still, the concentration of mining in very few pools looks very similar to Bitcoin. Vitalik Buterin and the community had seen this issue from the start, and thus Ethereum has had a switch to Proof of Stake



Top 25 miners by blocks: There is no significant difference between the PoW mining of Bitcoin and Ethereum. Both are highly centralized by a few entities. | Source: etherscan.io

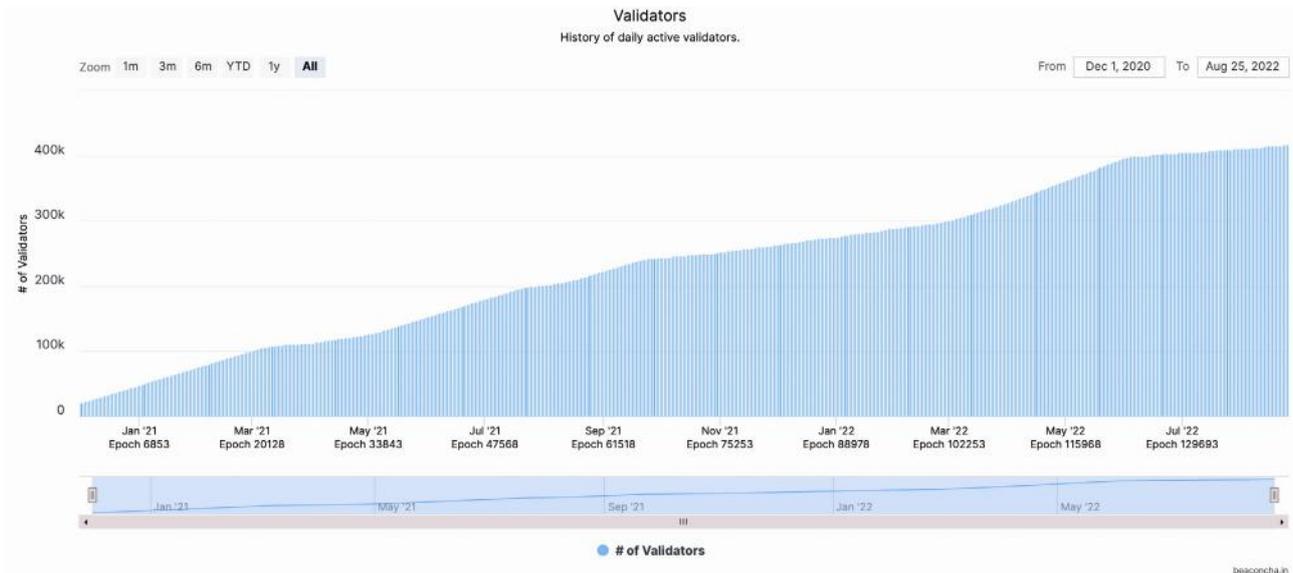
(PoS) on the roadmap pretty much from its inception.

If Proof of Stake works, it will allow anyone to provide capital and get the same return for that capital. This would reduce the need to first ensure an advantage over others before being ready to invest as a proof of work miner. PoS may provide some other risks such as pool concentration and frankly, I am hesitant to call victory on PoS until it has some track record. Existing PoS systems have been shown to be vulnerable. However, what makes me positive, is that the Ethereum community has recognized the need to further decentralize mining and is now close to switching to an improved system. According a recent tweet by [@VitalinButerik](https://twitter.com/VitalinButerik), the merge is scheduled to happen around September 15.



The hashrate distribution: Mining is controlled by a handful of entities and quite centralized. | Source: blockchain.com

What is required for decentralization to function is for everyone to enjoy the same benefits. The fact that PoW is all about gaining an advantage of energy cost and hardware ultimately leads to centralization. For Ethereum 2 (the PoS version) which has validators running in parallel to the Ethereum chain we already have roughly four hundred thousand validators. Of course, most of them come from pools and exchanges. Yet it is fairly easy for any individual to run such a validator on a regular laptop from home. This means anyone can partake in validation at roughly the



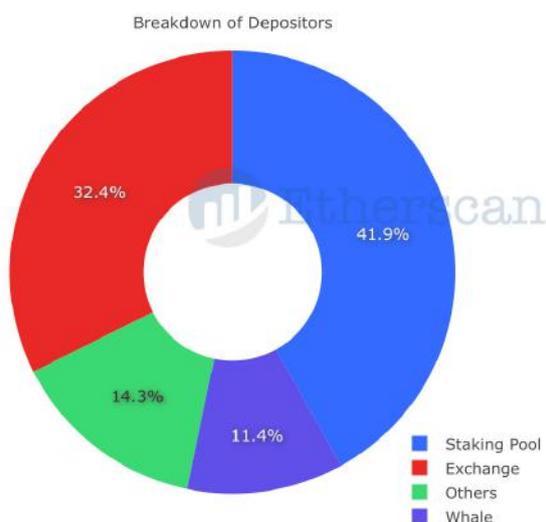
The amount of Ethereum 2 validators is constantly growing. The growth is limited to roughly 800 per day by the protocol. | Source: beaconcha.in

same cost and benefit ratio. This foundation is critical to making decentralized operations possible.

We see that about only forty percent of validators seem to be run by individuals (whales and others), while most of the validators are operated by pools either via exchanges or

pools directly. Pools are owned by many individuals so it only becomes an issue if several operators become malicious and literally steal funds. For instance, [TRON Allegedly Orchestrated a Hostile STEEM Takeover](#).

However one critical design advantage of PoS is that the honest validators could create a fork with around 40% of the stake (or less) and if the market would support that chain & corresponding coins, exclude the “bad actors” even if they have the majority. This threat will keep validators honest and create a massive game theoretical force to stay honest in the first place, as explained in [User-Activated Soft Fork from Malicious Supermajority](#).



OS validation is significantly dominated by pools, which leads to centralization. However, these pools represent more individuals since every dollar has the same yield, while in PoW professional entities tend to have an economic advantage. | Source: etherscan.io

Software distribution

When it comes to the development of Bitcoin and Ethereum both are running a little different approach. Bitcoin has one main client that is managed by blockstream. Still, it is open source development and many other clients have been developed by other teams. Ethereum has made sure from the beginning that several implementations exist.

Building layers on top of the main blockchain is working in a similar culture. Bitcoin has the lightning network which has evolved as the standard for instant and super cheap layer two Bitcoin transactions even used by El Salvadore. Ethereum on the other hand has several teams competing to win the layer 2 race with a few projects all offering similar functionality (cheaper fast transactions) yet a clear standard has not yet been developed due to the many choices for app developers and users. Likely a standard will emerge by market forces.

For both blockchains, we have a few different solutions such as wallets, explorers, etc. that allow for a healthy ecosystem to develop.

Other blockchains

Decentralization is quite expensive, meaning some costs and inefficiencies come with a decentralized system.

This is called the blockchain dilemma.

There is a relationship between decentralization, security, and scalability. To gain scalability, either security, decentralization, or both have to be sacrificed. In other words, decentralization in combination with security leads to slow performance. Hence, the rather limited transaction throughput of Bitcoin and Ethereum.

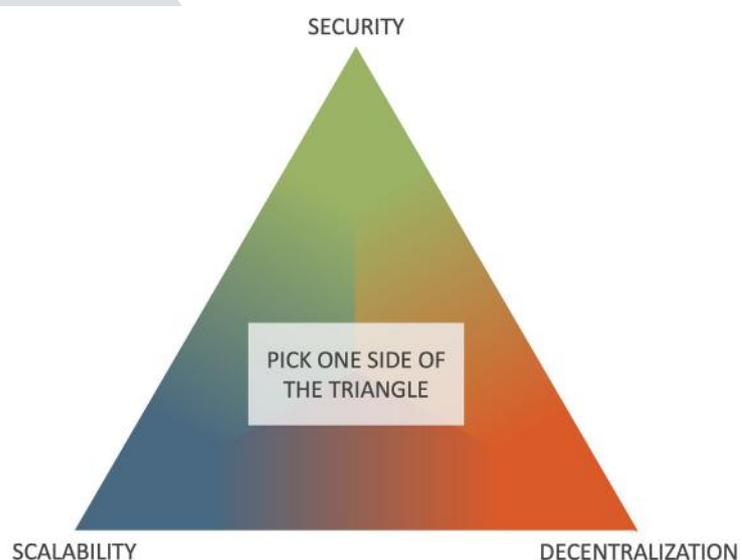
Other blockchains are trying to solve that dilemma of decentralization to the benefit of higher-level user functionality, while Bitcoin and Ethereum tend to value decentralization

most. Some of these sacrifices make sense for certain sets of applications. However, my personal belief is that these features will be replicated on the relevant layer 2 solutions. Time and the market will tell which approach is right.

Decentralization in practice: CeFi vs DeFi

In the past months, we witnessed the collapse of many protocols as well as the blowup of one of the top 5 blockchains altogether. We saw many companies and hedge funds go insolvent. In all cases, retail customers and users have suffered losses. As we are in a bear market, the validity of business models is being tested. Only now do we see what works and which approach is not going to make it.

What is the difference? Traditional systems (CeFi) usually collapse due to individuals being fraudulent or managing risk inappropriately. It is a failure of the people in charge. Customers give their funds to a company, the company then puts people in charge to manage these funds, and people make mistakes either maliciously or due to incompetency.



The blockchain dilemma states you can only pick two of its three core benefits: security, scalability, and decentralization. | Based on: cryptolog.nl

Often, there is no clear cut between the two. To protect customers, we need regulations and their effective enforcement. Bankruptcy processes and courts will lead to the resolution of companies that went insolvent unless they are bought out or bailed out by new investors.

A decentralized system (DeFi) works differently. The system is either designed correctly and works, or it has flaws. If it has flaws it will get exploited, i.e. by a hacker or investor that understands how the system functions better than the broad market. The key difference here is that a decentralized system has to work perfectly from the start. Thus, most decentralized protocols are not decentralized at the beginning. Usually, a team has control during the startup phase. Scammers exploit this by building systems that look legit only to then run with the funds they have control over, these so called “rug pulls” is how much fraud happens in crypto. Because there is no social protection system available it is much harder to go after scammers in crypto than in the real world.

In summary, centralized and decentralized both are systems that do not work perfectly and thus can enable fraud. The key difference is, when it does not work - in a decentralized

system this is a matter of the wrong design or structure, whereas in a centralized system behavior and actions by people are what leads to failure.

Let’s discuss two prominent real life examples from the recent past that show how decentralized systems with flawed design can and will be exploited:

Luna and UST

Luna was a Proof of Stake blockchain that came with a decentralized arithmetic stablecoin called UST (pegged to the Dollar) as well as a coin called Luna (now Luna classic). UST could be printed by burning Luna, and UST could be burned for the equivalent value in Luna. This is a very basic design that cannot work because as soon as the market cap of Luna comes somewhat close to the market cap of UST, a run on the bank will happen where smart UST holders will destroy or sell their UST and dump the Luna they receive. That creates a vicious cycle of the supply of Luna growing exponentially, which will further reduce its market cap leading to both tokens going towards zero value. That will happen as soon as demand for UST starts to shrink. Since any business has downturns, this will happen with near certainty. Most likely, in this case a smart hedge fund saw this flaw, made short bets on Luna and probably also on Bitcoin or bigger markets, and then pushed the Luna price down causing the collapse of Luna, which due to the heavy destruction of value had a pretty stark effect on the market. A smart investor with deep pockets could probably gain a few billion dollars by destroying over a hundred billion dollars in value for other investors. Luna was an example of a blockchain where the design of the incentive structures was flawed and thus this blockchain ultimately did not work.



Celsius Network

Celsius is a US company that operates a CeFi platform. This means DeFi customers can deposit funds and earn yields. The thing is the yields were quite high. In the backend, Celsius was cutting traditional finance deals such as borrowing the customer deposits to hedge funds and other institutions to earn more yield than in DeFi. However, to get these high yields, quite a few risky deals had to be made, and some of the institutions got rekt in the bear market. Likely Luna was also part of the deals. As a result, Celsius went insolvent. Customers are now stuck and cannot get their deposits back while deals are being worked on to save the company and customer deposits. Celsius has loans and contracts with various parties including DeFi protocols.

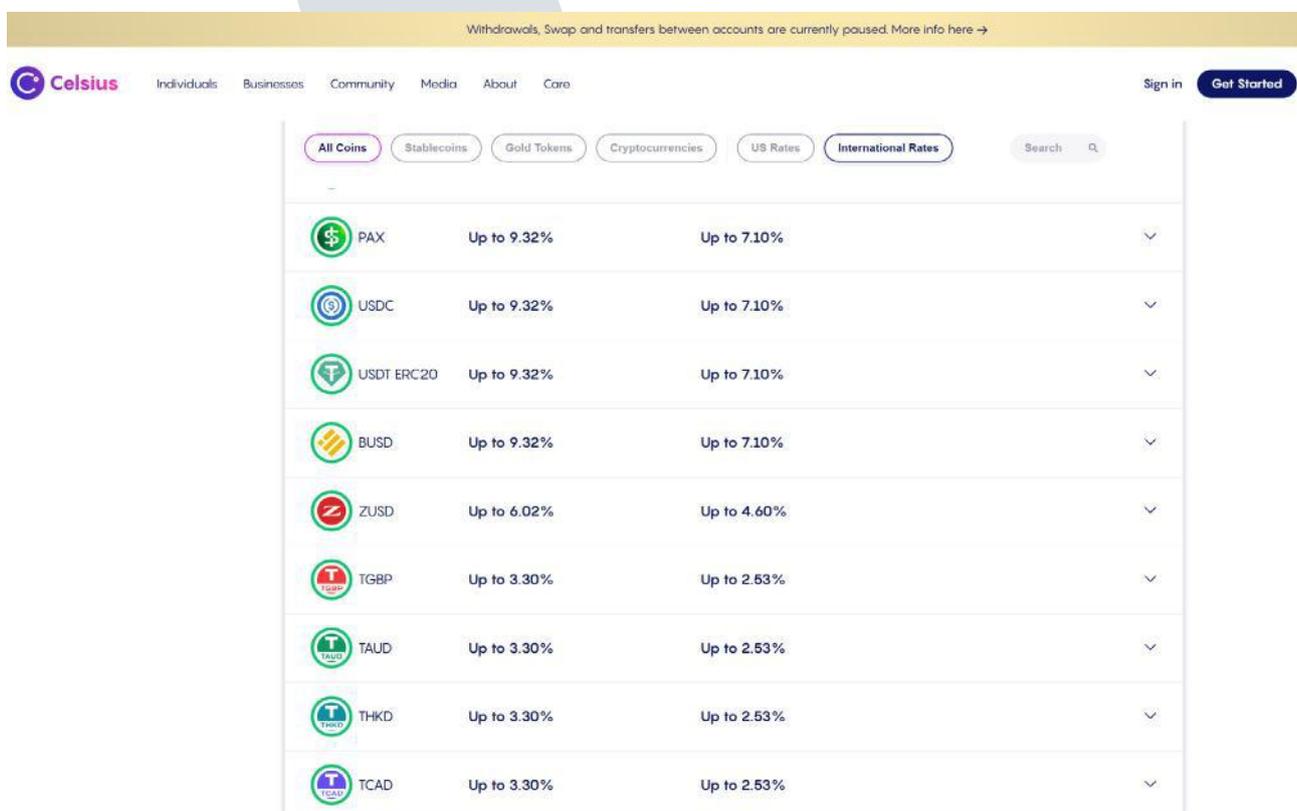
The interesting thing here is that DeFi gets paid first before any customers and other

partners because the contracts are automatically enforced. There are no negotiations or courts that define what happens with anything done in DeFi.

These examples show the value decentralization provides.

In a recent Tweet, Rhyan Adams points out that while capitulations in CeFi happen via complex human driven legal processes, in DeFi these actions are completely automated on the blockchain. "It's almost like DeFi works better," he summarizes ([full statement](#)). I have personally been a victim of the Mt. Gox failure and am still quite a few Bitcoins stuck there. Since then, I am hesitant to store any significant amount of value on centralized exchanges, banks, or companies. I prefer being able to move any amount of my wealth within one block without the ability of someone to interfere with it.

Withdrawals, Swap and transfers between accounts are currently paused. More info here →



Coin	Rate 1	Rate 2
PAX	Up to 9.32%	Up to 7.10%
USDC	Up to 9.32%	Up to 7.10%
USDT ERC20	Up to 9.32%	Up to 7.10%
BUSD	Up to 9.32%	Up to 7.10%
ZUSD	Up to 6.02%	Up to 4.60%
TGBP	Up to 3.30%	Up to 2.53%
TAUD	Up to 3.30%	Up to 2.53%
THKD	Up to 3.30%	Up to 2.53%
TCAD	Up to 3.30%	Up to 2.53%

Yields offered like these by Celsius are only possible to attain with lots of risks. In the case of Celsius the risk blew up during the bear market, leading to bankruptcy and resulting in heavy customer loss. | Source: celsius.network

So... does decentralization actually matter?

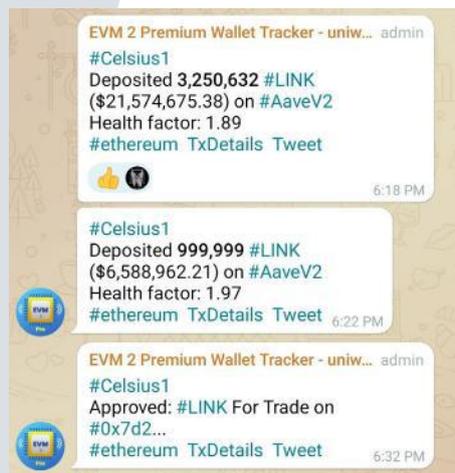
Blockchains without decentralization make little sense for it is what provides the main benefit compared to traditional finance, even if it is just under the hood like the engine of your car – you do not see it, yet it generates most of the value of the vehicle.

We have learned that decentralization in our blockchains is not perfect, but it is going in the right direction. Notably, the adoption of many users is providing the most basic foundations for further evolution. When it comes to the running of the network in a decentralized way, we see that the trend has gone the opposite way with mining becoming more and more dominated by few professionals. This is happening due to PoW's architecture that creates an advantage for bigger players with access to cheap energy and chips. Yet, run in different countries and by different companies, it is still decentralized enough. In addition, new solutions like Ethereum's PoS are on the way after a long innovation cycle. We have yet to see if decentralization works.

Our current bear market has shown that decentralization on the application layer of DeFi makes quite a difference. The big CeFi applications or companies like BlockFi, Celsius, and Voyager (among many others) went bankrupt, and thus lost or froze customer funds, while the big DeFi protocols have worked flawlessly during price volatility. The reason behind this is that decentralization is inherently much safer because all the control mechanisms are automated and transparent.

The books of Celsius on the other hand were a black box. Customers simply had to trust that the company was run well. On the blockchain, everything is open including every position of every participant as well as any actions such as liquidations, making the risks were perfectly transparent and verifiable. If you are on Crypto Twitter, you already know that every move of Celsius DeFi assets was

watched and reported like a sporting event, for example as shown in the tweet on the left by [@uniwhalesio](#).



Overall, I am optimistic for the future. Crypto is on a clear path to improve society on new economic layers. Most importantly there is a constant flow of adoption by users and technology as more and better infrastruc-

ture is being built. Innovations are constantly being unleashed, creating more and more advantages of decentralization. For example, it is now possible to trade and take loans on decentralized platforms – that is quite a significant improvement from earlier days of “just” storing and sending assets. Aside from new functionality, Bitcoin has been defending its key architecture to stay decentralized and Ethereum has been working to improve its consensus to enable better and longer lasting decentralization. Other protocols and applications can leverage this, learn from it, and build on top.

In summary, we are moving in the right direction. More people find use for crypto, and its tools as well as the technological foundations are getting ever stronger.

About the authors

Philipp Knirck studied Business Informatics and brings over 15 years of consulting experience in Europe, America, and the Middle East across industries. He now has settled in Switzerland, exploring new markets, building successful teams and achieving measurable results. His specialties are blockchains, cryptocurrencies and NFTs. He consults organizations on how to implement blockchain technology into their core processes in a way that creates value.



Melanie Zollinger holds a master's degree in Business and Economics. She has over 7 years of experience in Marketing in the consulting industry and occasionally accompanies IT projects from a communications aspect. She has co-written numerous specialist articles on IT project management, digital transformation and industry trends, validation and compliance topics, and most recently on blockchains and cryptocurrencies.