Thijs Maas [Follow]

Interested in the challenges between blockchains and the law — founder of www.lawandblockchain.eu

Jun 9 · 9 min read

Everything they don't want you to know about EOS.

If you would have told me last year that a startup without a product was to raise over $4 billion, I would have probably not believed it. In fact, I still find it hard to believe. Yet, EOS, a blockchain-startup without a product, managed to do just that. Everything about the platform, which is launching today, sounds great on paper. However, the truth is often less rosy as it would appear.

The EOS promise

EOS is a relatively new project in the blockchain space that aims to radically improve on what is on the market today. The decentralized operating system will, much like Ethereum, allow developers to build decentralized applications through smart contracts.

The unique selling points of EOS are that the platform will eventually allow for industrial-scale applications, through elimination of transaction fees and an ability to support millions of transactions per second. EOS developers expect that the platform will at least handle 1000 transactions per second upon launch. In contrast, Ethereum can currently handle around 15 transactions per second.

Ethereum Challengers: EOS

Delegated Proof of Stake. ERC20 token swapped for native token at launch.

	ETHEREUM	EOS
SCALABILITY	~15 transactions/second; PoS & sharding will improve this	1000s of transactions/second at launch. Millions w/ parallelization
GOVERNANCE	Similar to BTC, with additions (e.g. Ethereum Foundation)	DPoS. Producers elected by token holders & subject to constitution
DEVELOPMENT COMPLEXITY	Solidity language; fixes & updates hard to implement	Many languages supported via WASM. Fixes and updates easy
TIMELINE	Scalability improvements may take years	Release Candidate TestNet live, MainNet launching June 2018
GENERALIZED FEATURES (identity, authentication, file storage, etc.)	Intentionally avoided	Robust permissions, user identity, storage, assorted other features
ADOPTABILITY	Not grandma-friendly, losing keys is catastrophic, fees	Human-readable addresses, no fees, key recovery, anti-hacking
MARKET POSITION	First mover advantage. Many developers and $$ behind it	Billions of dollars, VC backing, Everipedia and more apps

Source: **bitgenste.in/eos**

Of course, this radical improvement in transaction throughput has sparked a wide interest in EOS. The company behind EOS, Block.one, has raised $4 Billion to develop it and its ecosystem through a fundraising tactic called an Initial Coin Offering. They managed to do so *without even having a working product…* In fact, when they started the ICO, they hadn't even wrote a single line of code.

This shouldn't be possible. Still, it can be somewhat justified by the radical improvements that EOS promises over other smart contract platforms and the overal hype about such platforms so far. But how does EOS aim to deliver on its promises in the first place?

Through a simple trade-off: EOS decreases its decentralization for an increase in scalability.

Decentralization is one of the main characteristics of a good cryptocurrency. Simply said, decentralization provides for censorship resistance. This censorship resistance is achieved by involving a large amount of parties in the production and validation of blocks. Basically, the larger this set of parties, the better. The problem is that all these parties have to constantly sync their blockchain to one-another. In the case of smart contract platforms, each block creator (whatever the consensus mechanism) has to also execute the code of every single smart contract. This is a very tedious process and it limits the overall capacity of the network significantly.

The idea behind EOS is that the processes of storing the blockchain, the 'block propagation' and the execution of smart contract code should be handled by only 21 parties, called Block Propagators (BPs). These BPs use optimized hardware and only have to sync with each other, instead of a large network. This allows EOS to have a transaction output like no other crypto before it.

Aside from this insane transaction throughput, EOS also promises that transactions on the network will be completely free!

Sounds amazing right? So what's the catch?

Catch #1: A New Maffia

Don't get me wrong: I believe that the general public is more interested in scalability than decentralization. Designing a system that trades a bit of the one for the other is not necessarily a bad design choice. However, it has to be done right.

After all, if you take away the decentralized nature of a blockchain you take away the one thing that a public blockchain does better than a traditional database: censorship resistance.

Without it, there is actually no point of using a blockchain, as you might as well use a traditional databases and legacy computing services.

So, Is 21 BP's enough to be decentralized?

If the block producers were fully anonymous and had no way of communicating with each other, then maybe. But this is not the case.

First, it is necessary to understand how the BPs are chosen. In essence, anyone who has any EOS can stake their tokens to vote for candidates that wish to become a BP. The 21 that are voted into office are allowed to create blocks, and, as such, they also receive block rewards.

Being a BP is awesome. At the EOS' current price (at time of writing), a BP will be awarded $1.64 million USD in block rewards per year. Moreover, another +- $102 million USD will be divided among BP's running in the election by ratio of their received votes. On average, let's say that a BP will be rewarded about **$2.5 million USD a year**.

As such, incentives exist to buy votes by, for example, offering kickbacks on the block rewards to anyone that votes for you. Once elected, all BPs will want to remain in power. Therefore, there is an incentive to maintain the established order, which means elected block producers will form alliances to vote for each other. In Lisk, another crypto using a very similar system, this has led to the emergence of two very powerful maffia-like coalitions: Elite and GDT. A great write-up hereof can be found here.

Once such coalitions are formed, decentralization of the EOS platform will be no more than a myth. Consequently, censorship resistance will be non-existent. The coalitions can even start extorting businesses building on EOS in various ways. We can imagine a scenario where a business' transactions are censored by the cartels unless it behaves in a certain way or pays money to BPs.

Now you might say that such censorship would hurt the BPs. It would lead to public backlash and subsequently, a decrease in the price of EOS. As the BPs are likely to hold EOS themselves, this would hurt them.

However, it is possible to 'hide' your censorship. Straight up censoring a business' transactions is not the only way to hurt it. The BP cartels could for example make it more difficult for a specific business to function, through small changes in how the network works. After all, decisions on what is allowed or not on the network are in the hands of the 'democratically elected' cartels.

By censoring in an indirect, hidden fashion, any possible public backlash is minimized. After all, the only thing that the BPs will have to do is provide an explanation of why they made the protocol changes. As long as this justification is plausible enough to fool the generally uninformed public, we wouldn't even know if any extortion is going on…

Sure, maybe the BPs will act ethically. However, having to rely on their promises to do so goes against everything that crypto was first created for.

Catch #2: 'free' is never actually free

While EOS boasts about its free transactions, we are left to wonder: if this was possible, why do other crypto's not provide it?

Transaction fees are generally used to give incentives to block creators/miners to secure the blockchain. They incentivize rational actors to put in their best efforts to validate and update the state of the blockchain in hopes of being rewarded for it.

Every blockchain needs such incentives. The only thing different about EOS is that these incentives are created by the rewards given to BPs I have described above. The coins that will be minted for this will amount to a total inflation rate of 5% on a yearly basis.

So sure, I don't have to pay a transaction fee when I send money. However, these fees are just hidden as they are accounted for in the BPs rewards.
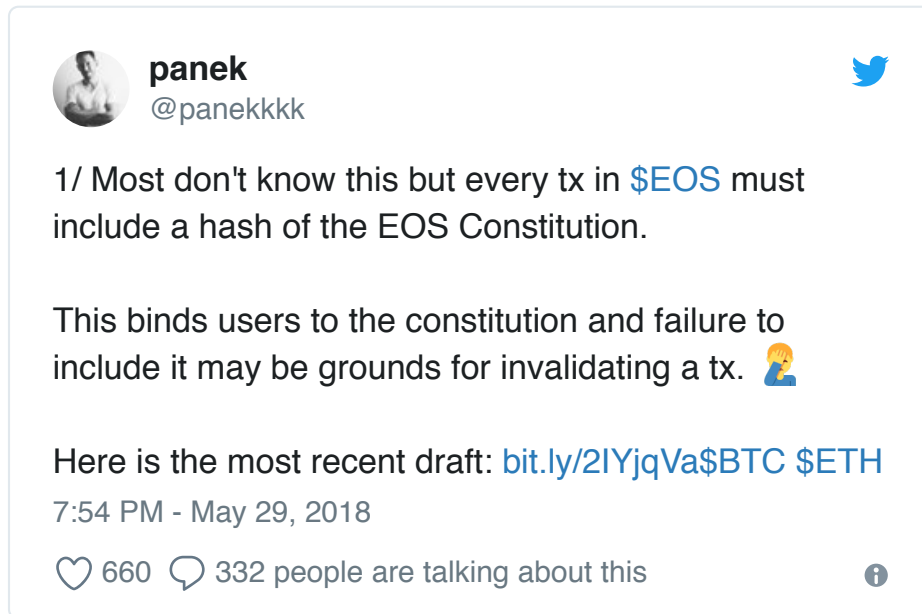
Instead of calling transactions free, it would be more accurate to say that my transaction fees are imposed on everyone who owns any EOS, in the

form of inflation.

Other red flags

- The EOS ICO was open to investors for 12 months. However, funds paid were not in lock-up during this period and secondary markets for EOS were opened with high liquidity. Therefore, as far as I can reason, the following scenario was a possibility for Block.One: Have people buy EOS → Use their funds to buy EOS in your own ICO → Have both the funds and the EOS → Repeat → Watch EOS price rise as it looks like the interest in your ICO is gigantic → Start selling your free EOS on secondary markets → profit.

- Dan Larimer, the mastermind behind EOS, has a somewhat dubious history. Although he is a great developer and innovator, previously having created blockchain-projects such as Bitshares and Steem, there are some stories that put him in a bad light. Take for example the stories of him cheating during the early days of Steemit mining. Also, as former colleague Charles Hoskinson said: "Larimer hasn't finished a project yet." In the meantime however, he has gotten filthy rich.

- The EOS Token Purchase Agreement basically states that EOS tokens are absolutely worthless and do not provide any rights at all to the buyer. This definitely raises some concerns. However, it is most likely in the agreement because Block.One is trying to completely distance itself from the development of the platform itself. Whether this would have any chance of standing up in court is something else altogether.

- EOS TOKENS HAVE NO RIGHTS, USES OR ATTRIBUTES. The EOS Tokens do not have any rights, uses, purpose, attributes, functionalities or features, express or implied, including, without limitation, any uses, purpose, attributes, functionalities or features on the EOS Platform. Company does not guarantee and is not representing in any way to Buyer that the EOS Tokens have any rights, uses, purpose, attributes, functionalities or features.

- NOT A PURCHASE OF EOS PLATFORM TOKENS. EOS Tokens purchased under this Agreement are **not** tokens on the EOS Platform. Buyer acknowledges, understands and agrees that Buyer should not expect and there is no guarantee or representation made by Company that Buyer will receive any other product, service, rights, attributes, functionalities, features or assets of any kind whatsoever, including, without limitation, any cryptographic tokens or digital assets now or in the future whether through receipt, exchange, conversion, redemption or otherwise.

- PURCHASE OF EOS TOKENS ARE NON-REFUNDABLE AND PURCHASES CANNOT BE CANCELLED. BUYER MAY LOSE ALL AMOUNTS PAID.

- EOS TOKENS MAY HAVE NO VALUE.

- Security is the most important element of any blockchain project. The fact that Block.One's internal systems have been hacked during its ICO, leading to millions in investor's funds being stolen by phishers, does not provide for much confidence in the company's abilities to make secure systems.

- Continuing on the subject of security, Block.One has announced a $10.000 bounty for every bug found in its software. Within a week, a single security researcher was able to rack in $120.000 by finding and reporting bugs. Of course I am not saying bug bounties are a bad thing and I realize that any software will have some bugs, but this just seems a bit too easy.

- EOS has written a 'constitution', which is a binding set of rules for everyone who uses the network. I won't go in-depth on this revolutionary concept, which is *definitely* not similar to General Terms & Conditions /s. However, it is oh so very clear that it hasn't been written by someone with a background in law. In fact, it is pretty hilarious. The tweet-storm below only scratches the surface. I strongly believe the lack of thought that has been put into this constitution is a huge missed opportunity. A combination of a set of clear rules on and strong legal remedies against colluding BP's would be a detrimental mechanism to reducing BP's incentives to collude.

panek
@panekkkk

1/ Most don't know this but every tx in $EOS must include a hash of the EOS Constitution.

This binds users to the constitution and failure to include it may be grounds for invalidating a tx. 🤦‍♂️

Here is the most recent draft: bit.ly/2IYjqVa$BTC $ETH

7:54 PM - May 29, 2018

♡ 660   ◯ 332 people are talking about this   ⓘ

If you found some more red flags, let me know—I'd be glad to add them. I would also love to receive any refutations of points made in this article and I will adjust it accordingly.

The current state of EOS

EOS BPs have voted to launch the network today! It should be live at 13:00 UTC. The latest development is a decision of the BP's to issue new EOS tokens, which is apparently for the RAM needed to create the accounts. This is absolutely hilarious, as it is a perfect illustration of what's wrong with EOS. No cryptocurrency community in its right mind would change the total supply of tokens. After all, a fixed/predictable max supply of tokens is the one thing that gives a crypto value. Indeed, it seems that the first decision by EOS' BPs ever might just set a precedent to break this fundamental rule. This is just comedic gold.

Oh well, at least it is constitutional :')

. . .

If you enjoyed the article enough to read to hear, why not leave some claps! It helps me out immensely. Also, it's pretty darn satisfying to hold that button.