Endurio

A Price-Stable Cryptocurrency for Everyday Transactions

Formerly known as: YggChain

Author: Antony Pham (antony@endur.io)
Contributors: Michael Chu, Ha Dang, Anna Doan

Version 0.06.04 (2018/10/13)

For the most updated version, see:
endur.io

Table of Contents

Abstract

> "*One of the main problems with Bitcoin for ordinary users is that, while the network may be a great way of sending payments, (...) Bitcoin the currency is a very volatile means of storing value.*" -- Vitalik Buterin on The Search for a Stable Cryptocurrency.

Price volatility and scalability keep hindering all cryptocurrencies to be widely adopted, far from the level of everyday transactions. *Stability of value* is one of the 5 must-have properties of money, and the lack of a proper scaling solution are the reasons why transaction throughput is extremely limited and the fee is getting higher and higher every day. Until these curses are lifted, cryptocurrency will forever be stuck in the basement of blockchain technology. And lifting those curses is no other than Endurio's purpose: to stabilize the currency price and to scale the network for everyone, every day and every transaction.

Introduction

Online retail and e-commerce market is growing rapidly these days, and surprisingly, cryptocurrency didn't take a significant part in it, yet. There are three fundamental problems that prevent cryptocurrency to become a major payment method of online business transaction: fluctuated price, long confirmation, and scalability (which directly affect transaction throughput and fee).

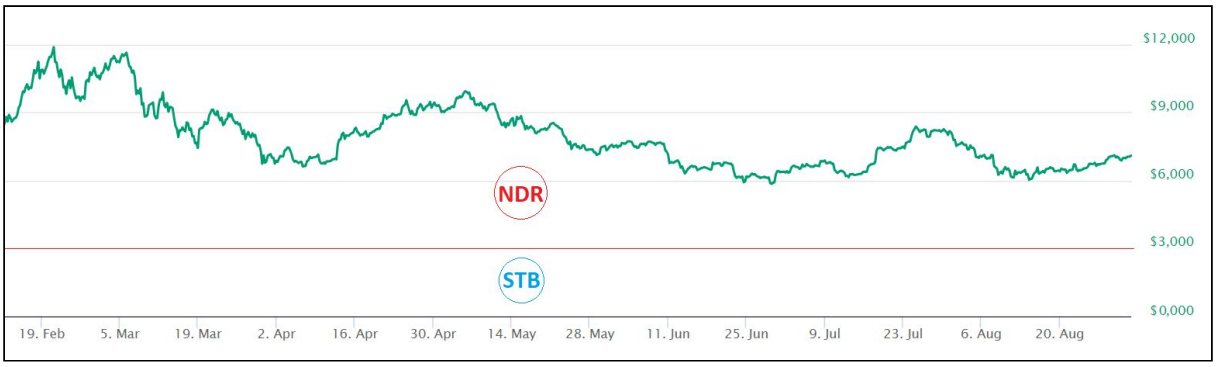
Endurio brings the real usability to cryptocurrency in retail and e-commerce market, with STB - a price-stable token for everyday usage, from paying for a beer to billions dollar business transaction without worrying about losing its value every other second. Powered by a public, permissionless blockchain with instant confirmation and Staking Service Network, where many kinds of decentralized service are built and served. Beneath all, Yggdrasil - an economic-driven sharding protocol scales the blockchain to any level of adaptation, remove all the network bottleneck for an unlimited transaction throughput, and the lowest transaction fee ever possible.

An Elastic Supply Stablecoin

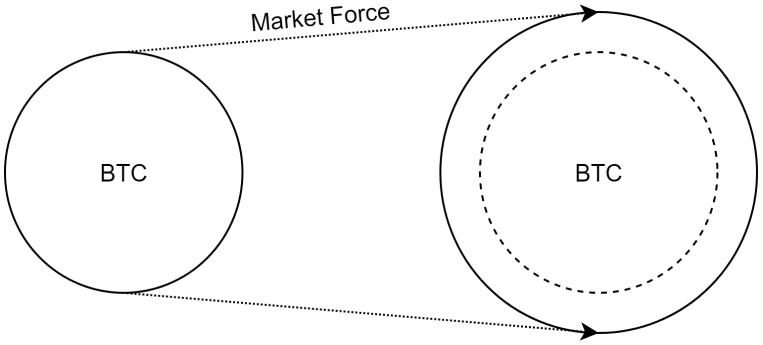
There's a chicken-and-egg problem of cryptocurrency: price volatility drives the end user away, only investors and traders in for the profit, and for-profit participants are highly affected by the market trend, hence the price is even more volatile.

But how can the market price of a free-floating asset be stabilized? Robert Sams' paper proposes a solution to use another asset to absorb all the price volatility of the stabilized token. Or in another word, the currency is separated into 2 tokens, one takes all price fluctuation, leaves price stability for the other; each has its own intended purpose:

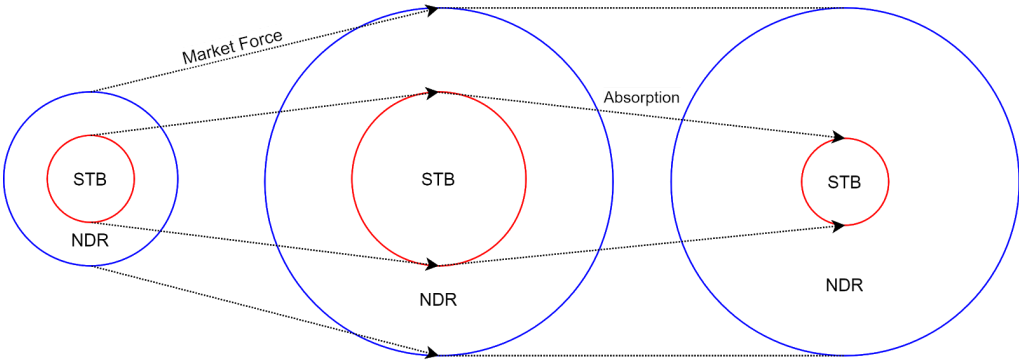
- NDR (Endurio): *High Risk - High Reward* token for investors and traders,
- STB (Stabilio): *No Risk - No Reward* stable-token for commercial users.



In gold, stock or Bitcoin, the supply is fixed or deterministic making each and every one of the currency units is fully exposed to the market force.

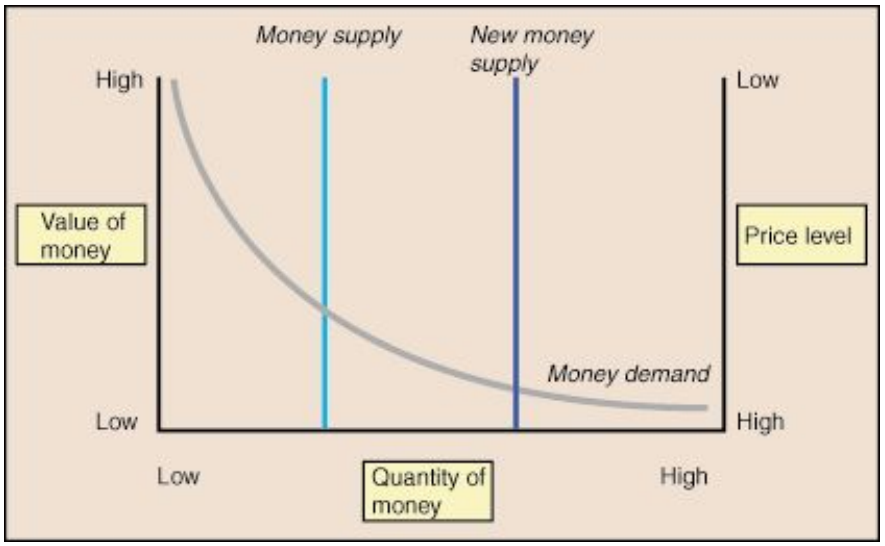


In Endurio - an elastic supply currency, the NDR token will absorb all the price volatility of the main price-stable token - STB, keeping its price around a desirable value (1.0 USD).

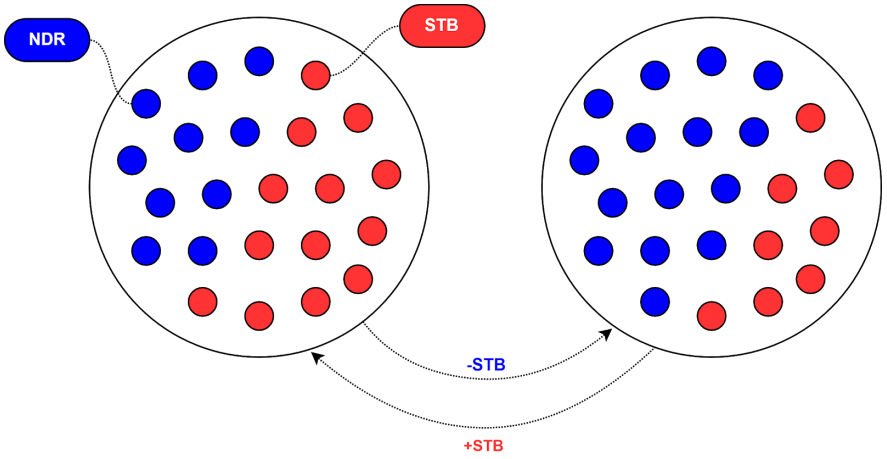


The Quantity Theory of Money

In monetary economics, the Quantity theory of money states that the general price level of goods and services is directly proportional to the amount of money in circulation, or money supply.



Endurio leverages this theory to stabilize the price of its currency - STB, by expand the circulating supply when its price is higher and contract when the price is lower than a **target value** (1.0 USD).



The supply of STB is changed by converting them from and to NDR. NDR supply is also changing along with STB supply in revert direction, effectively swings the price of NDR up and down to absorb STB's price volatility.

Stablecoin Protocol

Two-tokens System

The Endurio Stablecoin Protocol consists of 2 types of token:

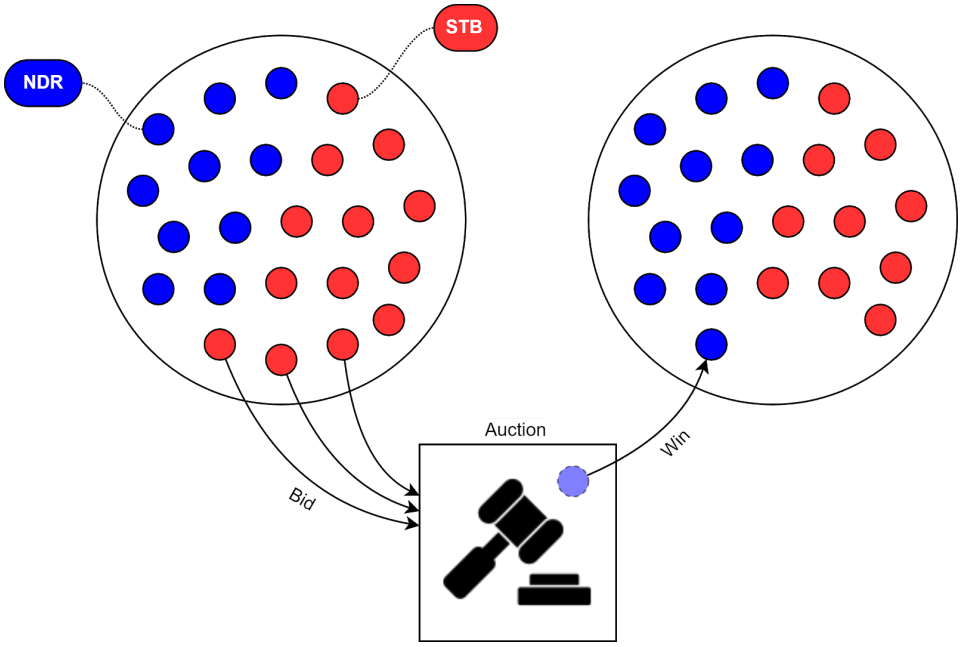
- NDR (Endurio) - represents the value that is contributed to the network from outside (by capital investment, mining or providing service to the network). The holders of NDR take the role of stock/shares holder, which they bear the responsibility to maintain and stabilize the network; they are rewarded with transaction fees, exchange fee and all the capital value gain when the network grows. Obviously, like any other investment, their risk is losing capital value when the network shrinks.

- STB (Stabilio) - represents the service provided by the network. The holders of STB take the role of customer, for currency service Endurio provides. Their benefit will be protected by the protocol with the highest priority.

To keep the price of STB stable, the following process is continuously repeated:

1. STB price is fed from the outside, or calculated using internal values of the network. (See Exchange Rate Feed)
2. If the STB price is **x%** higher than the **target value**, an **x% expansion** is taken place in the next phase.
3. If the STB price is **c%** lower than the **target value**, a **c% contraction** is taken place in the next phase.

The conversion between NDR and STB is the main mechanism for Endurio stablecoin economic.



Expansion & Contraction

In the event of **x% expansion**, when there is total **N** of STB in circulation, exactly **N * x%** number of STB is created (out of thin air) and sold in an on-chain public auction for NDR. The price of STB/NDR is completely market-driven, which is usually a little less than the current market price, effectively drive the market price of NDR higher. The NDR(s) used to buy auctioned STB(s) will be burnt and taken out of circulation.

The auction ends with new transactions included in the chain. The results are:

- The total supply of STB is increased by **x%**, and the token price is decreased by **x%** to exactly the **target value**. Newly created STB is given to the highest bidders of the auction.
- The total supply of NDR is decreased, and the token price is increased, benefits all current NDR holders. The highest bidders will be the most benefit, because not only

they have their remains NDR price increased, they also sold their NDR for a higher price than the market through the auction of the newly created STB.

Contraction process is exactly the opposite of Expansion.

Dynamic Target Value

Ideally, STB will always be anchored to the most stable purchasing power unit of human (and aliens that we know of), which can be anything proposed by the Oracles in the Staking Service Network. Be it a single fiat currency (USD), a basket of fiat money (XDR), or a market basket, it's all up to the user of the network to decide.

The price feeding system of Endurio allows Oracles to feed the anchored price level of any market value they desire. This provides the flexibility and adaptability for the system in case of a sudden change in the world economy. The change of anchored value should be seamless and effortless, yet economically stable and secure.

In the simplest event of the anchored unit change, where the **target value** of STB is switched from 1.00 USD to 0.86 EUR, each Oracle services only need to update a field in their configuration file. Any other parts of the network, including end user experience, is unaffected.

The real world scenario will not be so simplistic, because not all Oracle services can update their configuration at the same time, some of them don't even want to change. So at a time, we will have a network of 40% Oracles feeding value anchored to 1.00 USD, and 60% Oracles feeding value anchored to 0.86 EUR. This also doesn't affect the network at all, the effective anchored value is a basket of 2 fiat currencies: 40% USD and 60% EUR. This works seamlessly with any basket of values fed by the Oracle network, without any agreement beforehand.

Short-run Stabilization

While mainstream economists agree that the quantity theory holds true in the long run, there is still disagreement about its applicability in the short run. But for a free market asset, long-term assurance of price stability is well enough. Short-run stabilization is provided by the market itself when we can assure that the price will eventually return. In an assured sideways market, traders can profit by buying low and selling high, effectively stabilize the price even closer to the target value. Over the time the more adopted STB is, the more stable the token price will be.

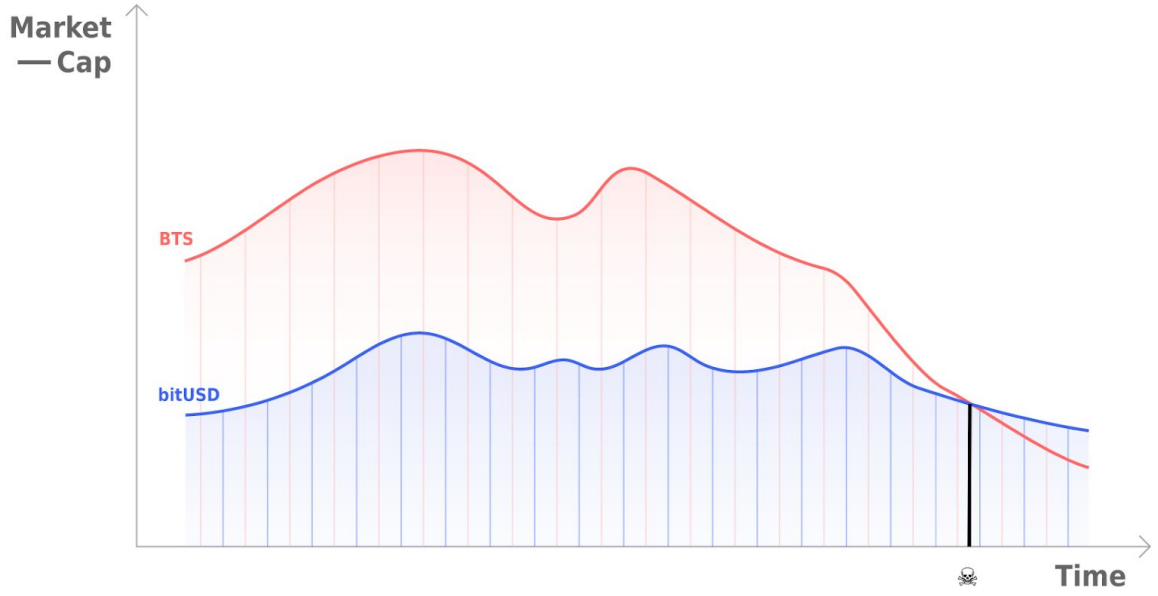
Black Swan Event

What happens when the coin price drop too low? This is the most frequently asked question for every collateral stablecoin projects, and such events do happen to them every once in a while. Endurio is not a collateral stablecoin, but an elastic supply stablecoin. That doesn't mean it is immune to all black swan events, it means that the chance is extremely unlikely, and how the system handles it is much more elegant.

Collateral stablecoin is essentially a collateral loans system, where you lock your asset (BTS, ETH) up into a contract, to borrow money (BitUSD, DAI) from people who need a stable-price asset. The problem is that the borrowers always have 2 choices:

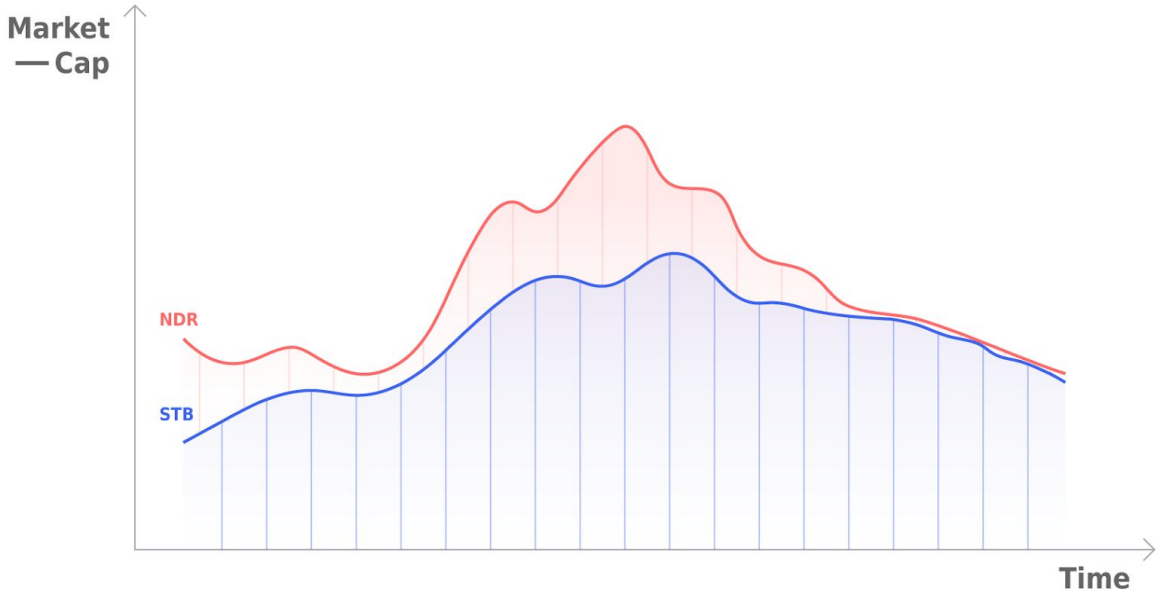
- to repay the debt (BitUSD, DAI) and get their locked up asset (BTS, ETH) back, or
- to abandon their collateral asset, and run away with their debt.

To repay or not to repay? That is the question any rational borrowers can easily answer, it depends on "*Which is worth more?*" or to be precise, "*Which will be worth more?*"



This is a mockup chart of BTS and BitUSD (*unstacked*). The system is healthy when the market cap of collateralized BTS is much higher than the market cap of borrowed BitUSD. BitShare requires borrowers to over-collateralize their BTS with at least 200% value of borrowed BitUSD, (MakerDAO requires 150%.) The system will break when the BTS price (along with its market cap) is dropped by 50%, (and ETH by 34%.) That the point where their locked up asset is no longer worth more than the debt they owe.

In Endurio, there is no loan nor debt, no borrower nor lender; *nobody owes anyone anything*. No one has such an easy choice to abandon an asset for another. NDR is used to absorb the price volatility of STB, not collateralized it.



This is a mockup chart of NDR and STB market cap (*stacked*). All the circulating NDR is used to stabilize STB price, and as long as the NDR market cap is not zero, the STB price can be stabilized.

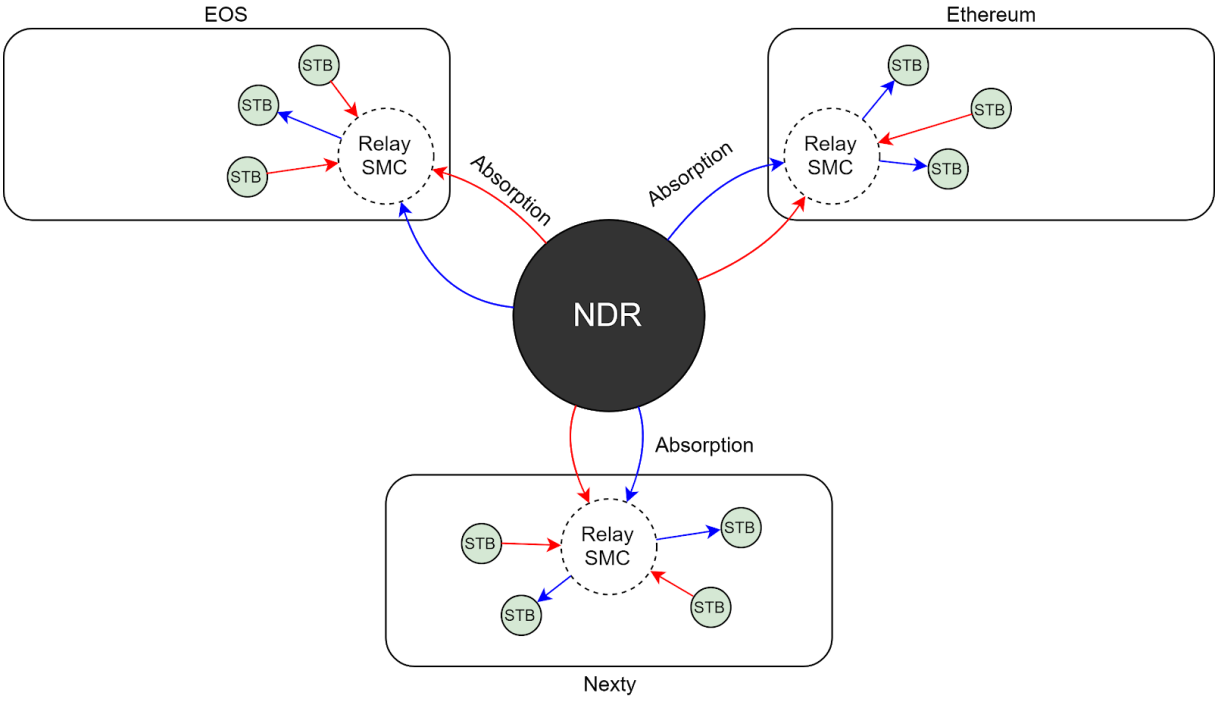
To recap, BitShare stablecoin will be unstable when the price of BitShare is quickly dropped by 50%, same with MakerDAO when ETH price dropped by 34% in a very short time. While STB price is unstabilizable only when NDR lost all of its value, a.k.a. 100% price drop.

Neither Seigniorage Shares nor Endurio has a magical mechanism to keep or raise the price of a token by itself. Seigniorage Shares only stabilizes a token around a **target value** to provide more usability for retail and e-commerce user, who don't want to take the risk of fluctuating price. It solves the chicken and egg problem of cryptocurrency and brings usability to the token. Retail users don't care (much) about the market trend, they just need a token to store and spend. The high level of usability will keep the stable-token in velocity, without being highly affected by the market force.

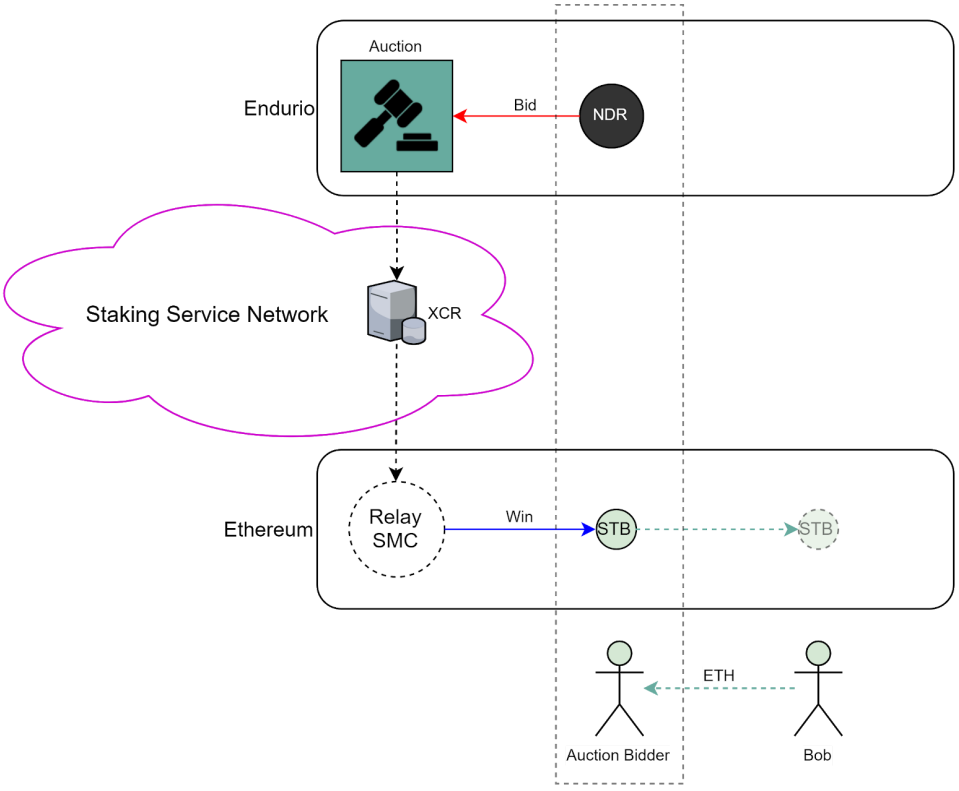
No financial system, traditional or digital, can assume that it is unaffected by or immune to Black Swan Events, but some system is more robust against them than others. The Quantity Theory of Money is well researched by economists and the elastic supply mechanism is what all fiat money now are made of. Thus, we believe Endurio's stablecoin will be the last one to fall if any critical crisis ever happens to the blockchain ecosystem, or specifically stablecoins.

Stabilization as a Service (Cross-Chain Token Absorption)

With our decentralized cross-chain relay service network, NDR can be used to stabilize tokens in any other foreign ledger. The value of NDR will grow even larger with all the stable token market from each supported ledger, while Endurio can contribute to blockchain ecosystem by providing price-stable tokens for all smart contract flatforms.



This feature is provided by the Cross-Chain Relay service (XCR) of the Staking Service Network.



Consensus

Proof of Work is fair, cryptographic secure, highly available, and with the right setting, can be the most decentralized consensus for a public blockchain. But it is energy consuming and

suffers from exogenous governance where people who run and benefit from the network does not risk anything if the network falls.

Meanwhile, stake-based consensuses are not mature enough and have to sacrifice some valuable properties of the public blockchain, especially decentralization and objectivity. Stake-based consensus often has some mechanism to randomly choose the sealers (or block producers) before the block is produced, giving them **a sense of privilege** which can be cheated, neglected, or totally abused. Selected sealers can be offline, intentionally delay the task, or gather together to coordinate an attack that damage or at least slow down the network. Some kind of punishment often come along to patch it, but they're mostly subjective and too complex to be practically useful.

In Proof of Work, everybody has to race for the right and reward, giving them **a sense of competition**. Even if one has the largest mining power in the world, there's no guarantee that he(she) will win a block, so everyone has to work as hard as they can. Any cheating attempt will cost them not only the mining power but also the chance to win an enormous reward.

Hybrid consensuses are used by some projects, but they are often *not tightly coupled*. The stake is either used to validate the mined block (Decred) or is locked up to provide additional services to the system (Dash). In those cases, stake doesn't involve much in the consensus, but only provides governance and service with reward; Proof of Work still does all the job.

Selective Staking Proof of Work

Selective Staking Proof of Work (S²PoW) is a hybrid consensus, with PoW and PoS tightly coupled together to power a fully decentralized, highly available and energy efficient public blockchain. It combines the two consensuses to have the advantages of both worlds:

- Security and high availability of PoW
- Energy efficiency and endogenous governance of PoS

S²PoW can either be described as:

- a PoS consensus where randomly selected stakeholders racing to win a block, or
- a PoW consensus where only a small percentage of the network has to work at a time.

Instead of mining 24/7 to compete with the whole world, each miner only mines (for example) 1% of the time to compete with 1% of the network at a time. The result is the same winning chance, with much less energy consumption.

Stake as Identity

Stake in S²PoW provides identity and authority, to prevent Sybil attack and provide a strong incentive for stakeholders to protect the system they invested in. The more stake a miner have, the better chance they will find a block. So splitting the stake out to multiple addresses do not provide any benefit.

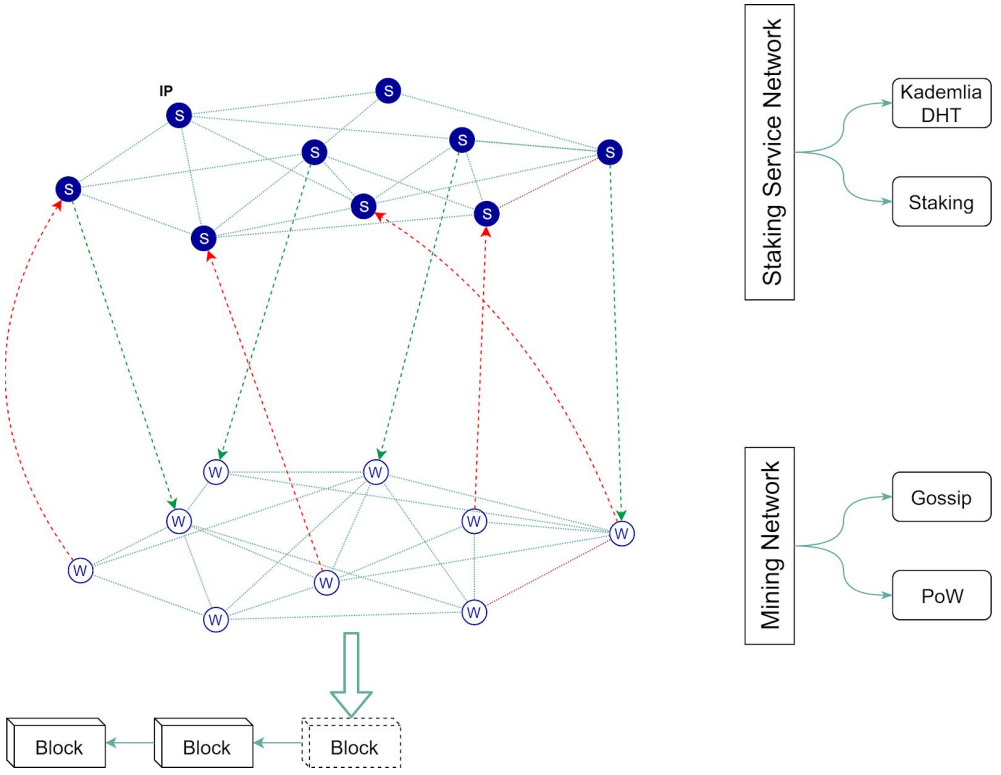
Mining to Compete

Mining in S²PoW provides cryptographic security and competitive nature for the consensus. The more mining power, the better chance miner have to win a block. But because the difficulty is selective (see Technical Paper), miners will not mine all the time, but only when the odd is in his(her) favor.

For maximum decentralization, S²PoW uses Programmatic Proof-of-Work, an improvement of Ethash to be even more resistant to ASIC devices. And to further prevent the risky centralization of pool mining and pool staking, S²PoW also requires miner signature and full block data (instead of only Merkle root) to make sure every miner takes full responsibility of the block content he/she produces.

Staking Service Network

Staking Service Network (SSN) is a second layer network built on top of the S²PoW layer of a public blockchain, to provide many services that are not possible or inefficient to be implemented in the consensus layer.



With Staking Service Network (SSN), anyone holding NDR can join and serve the network for a portion of block reward. Endurio currently has the following types of Staking Service:

- Input Locking Service (ILS): lock the transaction input to provide consistency and instant confirmation for the network.
- Oracle: feed data from outside of the network.
- Market: process the market order, including the EndurAuction.
- Cross-chain Relay: relay states from and carry actions to other ledgers.

Instant Confirmation

One of the most desirable services can be implemented in the SSN is the Input Locking Service (ILS). The ILS allows one single node to pledge their stake that a single UTXO can only be included in a particular transaction. If there's a double-spend, there must be conflicted signatures by that node, which has enough stake to repay the victims and be punished.

Input Locking Service provides instant confirmation with 100% warranty no double-spend for all transactions. This allows Endurio to have a wonderful user experience while keeping the block time long enough to preserve the security and consistency of the chain.

Block Reward

For each block is mined, exactly 1.0 NDR is produced and distributed as below:

- 50% for Proof of Work miners,
- 40% for SSN nodes selected for the locks,
- 10% for development subsidy,

After the chain is sharded, the block reward is split into each shard pro-rata, so at any time, there is only a total of 1.0 NDR is mined out for the whole network in a block time.

Yggdrasil Sharding Protocol

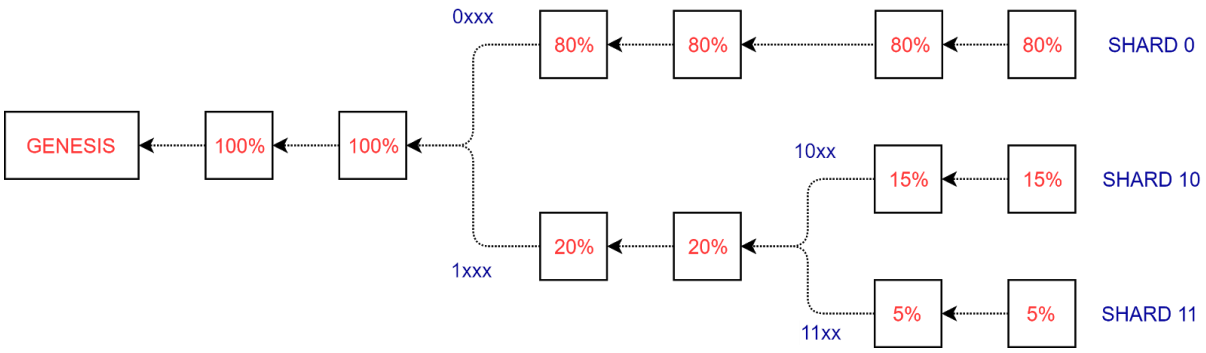
In order to be the currency of everyday transaction, Endurio should scale to any level of adaptation. Scalability is the biggest issue with Bitcoin, Ethereum, and all other blockchains. A lot of research and development is ongoing with this issue, most notable projects including:

- State Sharding for Ethereum 2020.
- Transaction Load Balancing of Zilliqa.

They are all advanced and promising with their own challenges. Endurio comes with its own mechanism: Yggdrasil - an economic-driven blockchain sharding protocol. It sidesteps many challenges other pure-technical sharding protocols (like Ethereum) has to face, including:

- Scalability and decentralization of super-full and top-level nodes (where all state from all shards is verified).
- High frequency of low-performance cross-shard transactions.

Yggdrasil sharding protocol has no super-full node, each node always works on only one shard at a time, and most of the transactions occur locally in one shard. These features make it an extremely efficient scaling solution, just like the sharding architect of the traditional database.



Security

The security of Yggdrasil sharding protocol relies on its economic-driven property. By splitting shards by transactions value, Yggdrasil utilizes the economic incentive to protect more valuable transactions with more mining and staking power, keeping the network at an evenly distributed security level.

In pure-technical sharding schemes, transactions are usually split randomly, while mining and staking power is split evenly between shards. This allows high-value transactions can occur in all shards, while the security level of each shard is divided. Yggdrasil keeps all the high-value transactions in one shard, with higher security, while letting all low-value transactions in the other shard, with less security. Any adversary attempts to attack either shard should face the same cost versus benefit problem. It's easier to attack the lower shard, but also less worthy.

The protocol itself does not force the transaction value limit on each shard. Users can still receive transactions with high-value on low shards (for lower fees or for bad intention). But doing so, they risk their own money getting double-spent or reverted. It is the user's responsibility to only accept high-value payment in high order shard, and reject ones in low order shard. Every wallet applications should perform this check, and alert its user when there's such a suspicious incoming transaction.

Centralization-Proofness

Sharding (along with ASICS-resistant algorithm) also prevents the centralization of control over the network. By splitting the mining reward and Service Node requirements, more participants can join the network to provide their service. Miner with less powerful rig can mine in the lower shard, for smaller, but steadier price. The same with Service Node requirements, owning even a small amount of NDR can still allow one to run a Service Node in low order shard.

Compare To Other Projects

Endurio is not the first attempt at a stablecoin, many projects with different approaches are being developed and running. This table will give a quick glimpse of what to expect from Endurio compare to others stablecoin attempts.

	Endur.IO	Basis	DAI	USDT

Tokens	2	3	2+	1
Token function	NDR: high risk - high reward investment	Shares: low risk - high reward investment	MKR: governance token	
		Bond: high risk - low reward investment	ETH: collateral investment	
	STB: no risk - no reward stablecoin	Basis: no risk - no reward stablecoin	DAI: loosely IOU token	USDT: IOU token
Stablecoin Creation	**Converted from NDR** with market-driven exchange rate, autonomous	**Out of thin air**, autonomous	**Out of thin air**, manually by ETH holder	**Out of thin air**, manually by Tether (the company)
Capital Value Flow	Circulated **inside the system**	Given directly to Share holder possession, **outside of the system**	Given directly to ETH holder possession, **outside of the system**	Given directly to the company, **outside of the system**
Expansion	On-chain public bidding	Pro-rata distribution	Increase interest rate.	Centralized process..
Contraction	On-chain public bidding	Issuing bond.	Decrease interest rate. Enforce liquidation of risky collateral.	Centralized process.
Pegged Value	Basket of Values voted by SSN	USD	USD	USD
Consensus	S²PoW	N/A	Ethereum Smart Contract	Centralized service.
Supply limit	No	No	66% of collateral ETH	No
Instant Confirmation	Yes	No	No	No
Sharding	Yes	No	No	No
On-chain Governan	Yes	No	No	No
Tx Fee	Minimal	N/A	Very high	N/A

Conclusion

There a reason crypto market always goes up and down together at the same time, because there isn't much utility for them yet. People only in for the profit, and for-profit participants naturally act according to the market trend. They spend their day worrying about the profit and loss of their investment, so they are highly affected by the market. End users of a true currency come for the utility, usability and convenience Endurio provides. Over time, the high usability will attract enough token velocity to withhold any financial crisis happen to the crypto world, making Endurio the most endurable cryptocurrency ever possible.

Contact

If you have any thoughts or want to be involved in the project, feel free to email the authors as shown on the title page. For the most up-to-date version of this whitepaper, please visit endur.io.