Setheum

White Paper - 4.0

Setheum - Money for All...

By Muhammad-Jibril B.A.
mba@setheum.xyz
https://setheum.xyz
10/24/2020

Abstract

We see a lot of cryptocurrencies coming up everyday, but what we don't see is a cryptocurrency that is decentralized, secure, scalable and having the option for price stability at the same time, especially one without debt or having to be centralized by a physical reserve in a corporate bank, and one that is also propadoptable(?what is propadoption? It's basically propping/fostering adoption). Setheum gives us the properties of both Fiat and Crypto with PES (Price Elasticity of Supply) without compromising decentralization or economic stability. A cryptocurrency that has scalable value and trust, setheum provides just that, backed by the resource of immutable trusted cryptography and efficient treasury system with elastic money supply that is immune to hyper inflation and price volatility, and is also 'propping diversity and incentivizing adoption' (propadoption).

The intent of Setheum is to improve upon the concepts of the Stablecoin decentralization, scalability, mass adoption, diversity and interoperability.

So, Setheum provides six (6) major solutions, the first of which is:

- Fixing the stablecoin inefficiency, narrow adoption strategies & use cases, and centralization Issues
- Propping and boosting Industrial synchronization and mass adoption of the Blockchain
- Filling the gap between financial markets, general-use and mass adoption of blockchain technology, especially stablecoins and cryptocurrencies in general.
- Solving the usability and sovereignty issue on most popular stablecoins.

Table of Contents

Brief History

We may say, It all started in 1976, when cryptographers Whitfield Diffie & Martin E. Hellman published their invention in the paper “New directions in cryptography”. IEEE Transactions on Information Theory IT-22(6), 644–654.

In 1982, cryptographer David Chaum first proposed a blockchain-like protocol in his thesis "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups.”

In 1983, S. Even, O. Goldreich, and Y. Yacobi published “Electronic wallet”. In Proceedings of Crypto '83.

Furthermore in 1989, David Chaum, Amos Fiat & Moni Naor published “Untraceable Electronic Cash (Extended Abstract)”. In the same 1989, H. Burkand and A. Pfitzmann published “Digital payment systems enabling security and unobservability”, Computer and Security,8(5):pp.399-416.

Further work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta, cryptographers at Bell Core (now iconectiv, a subsidiary of Ericsson). They wanted to implement a system where document timestamps could not be tampered with.

In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees to the design, which improved its efficiency by allowing several document certificates to be collected into one block. In the same 1992, T. Okamoto and K.Ohta published “Universal electronic cash”.

In CCS 1993, Gennady Medvinsky & B. Clifford Neuman introduced NetCash: A design for practical electronic currency on the Internet. In the same 1993, Stefan A. Brands published a technical report “An Efficient Off-line Electronic Cash System Based On The Representation Problem”. Yet in the same 1993, Niels Ferguson published the “Single Term Off-Line Coins”. Technical Report CS-R9318, Centrum voor Wiskunde en Informatica, Amsterdam.

In 1994, Niels Ferguson published yet another paper. “Extensions of Single Term Coins”. In the same 1994, Stefan A. Brands introduced “Untraceable Off-Line Cash in Wallets with Observers. In Advances in Cryptology: Proceedings of CRYPTO ’93, Santa Barbara CA”.

In 1995, Stefan a. Brands published yet another astounding paper “Off-Line Electronic Cash Based on Secret-Key Certificates”. In the same 1995, M. S. Manasse published “The Millicent protocols for electronic commerce”, in: *Proceedings of the First USENIX Workshop on Electronic Commerce, (New York, 1995)* (USENIX, Berkeley, CA, 1995). In 1995 yet again, B. Mihir, and J. A. Garay published “iKP — A Family of Secure Electronic Payment Protocols”, in: *Proceedings of the First USENIX Workshop on Electronic Commerce, (New York, 1995)* (USENIX, Berkeley, CA, 1995).

In 1996, Yair Frankel, Yiannis Tsiounis & Moti Yung published “Indirect Discourse Proofs”: Achieving Efficient Fair Off-Line E-Cash.

In 1997, Robert h.Deng, Yongfei Han, Albert B. Jeng, Teow-Hin Ngair, published “A New On-Line Cash Check Scheme”.

In 1998, M. Bellare, J. Garay, C. Julta & M. Yung introduced “VarietyCash: a Multi-purpose Electronic Payment System”.

In 1998 yet again, Nick Szabo designed a mechanism for a decentralized digital currency he called "bit gold". Bit gold was never implemented, but has been called "a direct precursor to the Bitcoin architecture.” In Nick Szabo’s bit gold structure, a participant would dedicate computer power to solving cryptographic puzzles. In a bit gold network, solved puzzles would be sent to the Byzantine fault-tolerant public registry and assigned to the public key of the solver. Each solution would become part of the next challenge, creating a growing chain of new property. This aspect of the system provided a way for the network to verify and time-stamp new coins, because unless a majority of the parties agreed to accept new solutions, they couldn’t start on the next puzzle.

When attempting to design transactions with a digital coin, you run into the "double-spending problem." Once data has been created, reproducing it is a simple matter of copying and pasting. Most digital currencies solve the problem by relinquishing some control to a central authority, which keeps track of each account’s balance. This was an unacceptable solution for Nick Szabo. "I was trying to mimic as closely as possible in cyberspace the security and trust characteristics of gold, and chief among those is that it doesn’t depend on a trusted central authority," he said.

The phrase and concept of "smart contracts" was developed by Szabo with the goal of bringing what he calls the "highly evolved" practices of contract law and practice to the design of electronic commerce protocols between strangers on the Internet.

In 1999, Stephan A. brands published yet another beautiful paper, “Electronic Cash. In Handbook on Algorithms and Theory of Computation” with editor MIKHAIL J. ATALLAH, chapter 44. CRC Press, Boca Raton. ISBN 0-8493-2649-4.

In ICICS 2001, Greg Maitland & Colin Boyd published “Fair Electronic Cash Based on a Group Signature Scheme”.

All these inventions were neglected and almost forgotten until when we needed them the most in the 2007-2008 financial crisis, what a crash, I had wish we saw the black swan coming earlier and took all preventive measures, but we just simply didn’t trust crypto, and now it’s proven us totally wrong, though it hurts to be wrong we have to admit we must transition to a better economic stability strategy.

On the 7th of April 2008, MICHAEL NÜSKEN published “WORKSHOP e€ (ELECTRONIC MONEY).”

Then in the same catastrophic 2008, Blockchain was invented by a person (or group of people) using the alias Satoshi Nakamoto, to serve as the public transaction ledger of the cryptocurrency “bitcoin”. The identity of Satoshi Nakamoto remains unknown to date. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains that are readable by the public and are widely used by cryptocurrencies. Blockchain is considered a type of payment rail.

Now in this catastrophic 2020, I propose Setheum to change the lives of people and the situation of the financial markets and head for a smooth bull ride in the entire global economy.

The Blockchain

Understanding The Blockchain

A blockchain is a decentralized, distributed, and oftentimes public, digital ledger consisting of records called *blocks* that is used to record transactions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. A blockchain has been described as a *value-exchange protocol*. A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

Blockchain 1.0 - Bitcoin (Cryptocurrency)

Cryptocurrency is the first implementation of distributed ledger technology (DLT). This allows financial transactions based on blockchain technology or DLT (for the sake of simplicity often seen as synonyms) to be executed with Bitcoin being the most prominent example in this segment. It is being used as “cash for the Internet”, a digital payment system and can be seen as the enabler of an “Internet of Money”.

Blockchain 2.0 - Ethereum (Smart Contracts)

Ethereum blockchain aims to execute ‘Smart Contracts’ to reduce the cost of verification, execution and fraud prevention. They are independent computer programs that automatically execute predefined conditions. A DApp can have frontend code and user interfaces written in any language that can make calls to its backend, like a traditional App. But a Dapp can have its frontend hosted on decentralized storages such as Ethereums Swarm.
[DApp = frontend + contracts **(**running i.e. on Ethereum**)]**

Blockchain 3.0 - DApps

DApps or Dapps have decentralized data storage and decentralized communication channels which run on centralized servers. A Dapp has the front-end/user interfaces written in any language, running on decentralized storages such as Ethereum Swarm, whereas the back-end runs on a decentralized peer-to-peer network. The front-end can make calls to its back-end like in a traditional app.

Blockchain 4.0 - Blockchain for Industry

Blockchain 4.0 is making Blockchain 3.0 usable in real-life commercial usage. Some real-life scenarios are for supply chain and approval workflows, safe and secure IoT data collection, payments and financial transactions, and fitness and health management. Especially *Industry 4.0 demands*. Industry 4.0 meaning in short terms automation, enterprise resource planning, and integration of different execution systems. However, this industrial revolution demands an increasing degree of trust and privacy protection — this is where blockchain kicks in.

Blockchain 5.0 - Blockchain of Everything (BoE)

Blockchain 5.0 is improving on the higher level Blockchain 4.0.. it makes more usability and diversity as a higher standard and a new generation Blockchain with more impact on mass adoption and diversification than all of its predecessors combined. The Blockchain 5.0 is a level only few are approaching so far as we know, despite the needs for a system like this.

Cryptocurrencies, Differential Auditable Privacy (Diaprivacy), Smart Contracts, DApps, DAOs, Blockchain Protocols, ,Industrial Scale Blockchain, Stable Economic Policy, Secure Governance, Fully Decentralized Algorithmic Stablecoins, a unique monetary Regime, a unique Fiscal Regime, a unique method of Staking and passive income, High Speed, Open Source.

With over 80 (see them close to the end of the paper, all 80 practical use cases with some examples and ideas) Industrial, Financial and Daily Use Cases all at scale, this is Setheum, the First ever Blockchain 5.0, the first ever Blockchain of Everything (BoE).

On this version of the white paper, we have decided that Setheum will be implemented on the Polkadot Network based on Substrate. I had the initial version the way it is because I wanted to solve the scalability issue of the Polkadot network, but I changed my decision looking at the progress of the network to the future I wanted it to have, and I always wanted to join the network but now I am more confident that the network will soon get to where we want it to. After all, it is better to come together and build what we already invest in, rather than reinventing the wheel.

Sustainability: Sustainability is a notion introduced in the domain of environment . It has been extended to almost every field. Albeit the technical means in the previous sections are unquestionably important to the development of blockchains, this topic goes far beyond pure technical realm. The balance and growth of an industry is always governed by a number of factors. We need a network that is based on PoS (Proof of Stake) so as to be sustainable, have low carbon footprint and better chances for smaller validators that don't have the resources to mine on PoW because it is overpowered by strong highly resourced miners and mining pools - making the network more centralized and breaking the core value of the network. That's why we need PoS consensus on Setheum.

Interoperability: Blockchain Interoperability is the ability of a blockchain to communicate seamlessly with another blockchain outside its scope of protocols. Blockchain interoperability generally tackles the ability of sharing states and transacting across different chains . Blockchains can be seen as isolated databases, without proper interfaces for intercommunication of data. Blockchain interoperability could enrich use cases for blockchains like portable assets, payment-versus-delivery and cross-chain oracle. Ideally, different blockchains would be abstracted, such that a user can readily manipulate all the functions without accurate understanding of each blockchain.

Elasticity & Economic Stability: Elasticity is a measurement term that applies to a variable's sensitivity to a change in another variable. In most cases, this sensitivity is the difference in price relative to changes in an array of other factors. In the field of business and economics, elasticity is a reference to the degree to which individuals, consumers, or producers modify their demand. Alternatively, when the supplied amount in response to price or income changes, it is primarily a way to evaluate the change in consumer demand mainly due to a change in price. We need a blockchain with a built-in elasticity system for it's stablecoins in order to curb inflation and volatility in the stablecoins standard of the blockchain, that's why SERP (Setheum Elastic Reserve Protocol) is introduced. The SERP mechanism will be explained in this paper.

Propadoption: How can cryptocurrencies reach mass adoption and foster diversity of use cases in our day to day lives as effectively as the fiat does and even advantageously better. Propadoption basically means to prop diversity in use cases and propagate adoption.

So for setheum to support diversity and foster adoption of its network, we need to first create a relationship between our financial market, our fiat currencies, our day to day activities, our practical use cases of the blockchain, and our cryptocurrencies.

To do just that, I introduced an efficacious Monetary Regime, an adoption incentivizing Fiscal Regime, the SERP to foster economic stability, and the Equilibrium of blockchain forces - Setheum Blockchain to connect them all with our financial markets and our daily activities.

Filling The Financial Gap

Economics thinking and research faces what the Institute of New Economic Thinking (INET) has dubbed “a crisis of conformity”. Our current monetary policies are clearly against equality and transparency, something the blockchain provides and Setheum as a protocol adds efficiency and stability to this and gives eloquence to the blockchain.

An example in finance that anyone who's traded treasuries is familiar with, is: “Failure to Deliver”, so for example, ***bank A*** will sell a bond to ***bank B***, who borrows it from ***bank C***, and the same bond in a day, might trade across a dozen banks. And if one back office ***fails to make delivery*** of that bond, you get what’s called a “**Cascading Failure to Deliver.**” Because no one knows who actually owns the bond, and that can take weeks to fix. So imagine if you just have a shared database, a database that each of those banks held, that was kept accurate in real time, and that no one could maliciously change or manipulate.
You would know who owns what bonds and you might be able to eliminate half of the existing back offices in big banks, resulting in massive cost savings.

So, to fill the financial gap, Setheum provides the infrastructure for Financial markets & Institutions to develop a reliable blockchain that shares the security, diversity and mass adoption of the Setheum Network, can be permissioned and independently governed, and can issue tokens and make use of the vast array of Sett stablecoins to trade and transact more efficiently and rely on the network’s Economic stability for long time interests.

The general public will also now have the ability to spend cryptocurrency, send/receive cryptocurrency, and earn passive income with cryptocurrency on the Setheum network, without having to engage in tough cryptocurrency acquisition processes in the future.

Setheum Finance Protocol

The financial system of Setheum

As we already know, price-stable cryptocurrencies combine the best of both worlds, both fiat currencies and cryptocurrencies like Bitcoin, but not many have a clear plan for the usability let alone the adoption of such a currency.

Cryptocurrencies and stablecoins in particular, were designed as a direct result of shortcomings in financial markets and in the global economy – lack of capacity for cross-border payments, high transaction fees, opacity on banking systems, investor risks, market hours and exchange limitations, etc. And since the value of a currency is driven by it’s network effects, a successfully progressive new digital currency needs to maximize adoption in order to be useful.

Creating just another stablecoin is not enough, the “use case” is what matters more. Are there any practical use cases apart from trading in exchanges, airdrops and staking?

Setheum Finance Protocol brings us a solution, the ultimate solution in fact, where no portion of the stability mechanism is centralized.

I propose “Setheum Finance Protocol” to push cryptocurrencies to reach their full potential, by addressing every practical use case of a stablecoin as a result of Setheum’s “Dinar Sett Stability System” (DS3) that introduces the SERP (Setheum Elastic Reserve Protocol), the Dinar (DNAR) and the SETT (Setheum Tokens). My proposed price-stable “SETT” is not just price-stable but also growth-driven, it is the exemplary price-stable cryptocurrency in the forefront towards the wider growth of blockchain adoption, it achieves stability through an elastic money supply, enabled by stable minting mechanisms based on the “Dinar”. Setheum Finance also uses seigniorage created by its minting operations as transaction stimulus and more to be discussed on the next subtopic (Setheum Fiscal policy), thereby facilitating adoption.

There is high demand for decentralized, price-stable currencies that should be both fiat-pegged and absolutely cryptonomic in nature, eliminating fiat’s inflational fracas and bitcoin’s volatile nature. And when it succeeds, then it will have a significant impact as the best use case for cryptocurrencies. Setheum Finance Protocol makes that balance of truthful trustless equilibrium between fiat currencies and cryptocurrencies. Setheum is leveraging Dinar cryptocurrency as the reserve asset for it’s fiat-pegged stable currencies, and also maintains its decentralized nature while also avoiding extreme price volatility and hyperinflation. Setheum Finance has combined Bitcoin, Fiat and Stablecoin features that maximize the best of all three. The price-volatility of cryptocurrencies is a well-studied problem by both academics and market observers (see for instance, Liu and Tsyvinski, 2018, Makarov and Schoar, 2018).

Most cryptocurrencies, including Bitcoin, have a predetermined issuance schedule that, together with a strong speculative demand, contributes to wild fluctuations in price. Bitcoin’s extreme price volatility is a major roadblock towards its adoption as a medium of exchange or store of value. Intuitively, nobody wants to pay with a currency that has the potential to double in value in a few days, or wants to be paid in a currency if its value can significantly decline before the transaction is settled.

But other cryptocurrencies that have infinite supply also have speculations as to how they can sustain hyperinflation in the long run, what happens to their PPP (Purchasing Power Parity) when their always infinitely increasing supply is a matter of concern.

So we need a balance right in the middle, and a mechanism to curb both volatility and inflation, in order to harness the economic stability of cryptocurrencies - their best day to day use cases hide behind the curtains of economic stability.. Setheum gets rid of that curtain, for God says let there be light, so then why do we prevent it from reaching us even though we’re in the dark.

The problems of high volatility are aggravated when the transaction requires more time, i.e; for deferred payments such as mortgages or employment contracts, as volatility would severely disadvantage one side of the contract, making the usage of existing digital currencies in these settings prohibitively expensive.

At the core of how the Setheum Protocol solves these issues is the idea that a cryptocurrency with an elastic money supply would maintain a stable price, retaining all the censorship resistance of Bitcoin, and making it viable for use in everyday transactions just like the fiat. However, price-stability is not sufficient for the wide adoption of a currency.

Currencies inherently have strong network effects: a customer is unlikely to switch over to a new currency unless a critical mass of merchants are ready to accept it, but at the same time, merchants have no reason to invest resources and educate staff to accept a new currency unless there is significant customer demand for it. For this reason, Bitcoin's adoption in the payments space has been limited to small businesses whose owners are personally invested in cryptocurrencies.

The reality is that while an elastic monetary policy is the solution to the stability problem, an efficient fiscal policy can drive adoption and a strong technology can prop diversity in use cases, therefore cultivating propadoption. In addition, the Setheum Protocol offers strong incentives for users to join the network with an efficient fiscal regime, managed by the Setheum Reserve, where everyone on the network is a participant in the economy and has some rights over the treasury.

That is, the Setheum Protocol with its equanimity in fostering stability and propping adoption in the Setheum Finance Protocol, represents an eloquent complement to 'Fiat currencies' and 'Cryptocurrencies' as means of payment and stores of value.

Setheum Monetary Policy

The existential objective of a stable currency is to retain its purchasing power. Given that most goods and services are consumed domestically, it is important to create cryptocurrencies that track the value of local fiat currencies. Though the US Dollar dominates international trade and Forex operations, to the average consumer the dollar exhibits unacceptable volatility against their choice unit of account.

Recognizing strong regionalism in money, SETT aims to be a family of cryptocurrencies in an "STP Standard" ('Setheum Tokenization Protocol' Standard) that are each pegged to their respective equivalents. SETT is the 'basket token' (a token which is made up of all the tokens on the STP258 Standard) of the Setheum Finance and all the stablecoins on that protocol are defined by the Sett standard. (So when i say Sett, i might mean any of the tokens of the Sett family and i might mean the basket token, it depends on the context of the statement.). The STP258 standard contains the major global fiat currencies that can be atomically swappable in the Setheum Reserve using the SERP (Setheum Elastic Reserve Protocol) on the Setheum Network.

Unlike today's popular monetary policies, it is a unique one in the Setheum Reserve, first of all the Monetary Aggregates are extended and incorruptible in Setheum Finance, so Setheum does not compute high-powered money (HPM) into SETT, which is basically the multiplication of the Monetary Base (MB or M0) with Fractional Reserve Banking.

Setheum mints Sett through an elastic money supply relying on PES, so the amount of Sett to be minted is proportional to the pairing of Dinar versus the corresponding Sett currencies relative to its fiat peg and its market cap.

Once the system has detected that the price of a Sett currency has deviated from its peg, it must apply pressures to normalize the price. Like any other market, the Setheum Financial market follows the simple rules of supply and demand for a pegged currency.

So, contracting money supply, all conditions held equal, will result in higher relative currency price levels. That is, when price levels are falling below the target, reducing money supply sufficiently will return price levels to normalcy. Expanding money supply, all conditions held equal, will result in lower relative currency price levels. That is, when price levels are rising above the target, increasing money supply sufficiently will return price levels to normalcy.

Of course, contracting the supply of money isn't free; like any other asset, money needs to be bought from the market. Central banks and governments shoulder contractionary costs for pegged fiat systems through a variety of mechanisms including intervention, the issuance of bonds and short- term instruments thus incurring interest expenses, and hiking of money market rates and reserve ratio requirements thus losing revenue. Put in an easy way, central banks and governments absorb the volatility of the pegged currencies they issue. In the short term, validators absorb Sett contraction costs through validating power dilution. During a contraction, the system mints and auctions more validating power to buy back and burn. This contracts the supply of Sett until its price has returned to the peg, and temporarily results in mining power dilution.

As minting and contraction take place, the supply is distributed accordingly, and Setheum Finance will provide a way to atomically swap 'Sett token' for any of the Sett tokens in the family/basket contained in the STP258 Standard. So, basically, SETT mints tokens according to the preference of the user, you can choose to use SettUSD(SettUSD) or SettSAR(SettSAR), and can swap that back into the basic token via the Atomic Shifter Tunnel, basically atomic swap where one token is burnt to produce the other. These tokens minted by SETT, are called "***Prototokens***" or ***settTokens***, because the are tokens derived from the supply of a basket token in a blockchain on the network, that is backed by the main staking token of the Setheum Network. So,it's a complex but efficient mechanism.

So, if Alice has $100 USD worth of SETT, Alice could mint 100SettUSD (100SettUSD) or it's equivalent of SettSAR (SettSAR), or any one of the currently 34 available SettTokens. In the mid to long term, validators are compensated with increased staking rewards. First, the system continues to buy back staking power until a fixed target supply is reached, thereby creating long run dependability on available validating power, the system increases validating rewards afterwards. In summary, validators bear the costs of Sett volatility in the short term, while being compensated for it in the long-term. Compared to ordinary users,

validators have a long-term vested interest in the stability of the system, with invested infrastructure, trained staff and business models with high switching cost.

The Contraction and Minting method in SERP, is inspired by the Terra model of contraction and minting for price-stability. But SERP improves much more on that. And the fiscal policy and staking rewards are processed uniquely on Setheum.

Setheum Fiscal Policy and Setheum Payment Protocol (SettPay)

Setheum Payment Protocol is basically the face of Setheum Finance, this is what validators, exchanges, DApps (E-Commerce platforms, payment platforms, Games, Streaming Apps, etc.) are required to communicate with in order to access newly minted Sett.

Setheum distributes newly minted SETT as discounts and cashback to the users of SettPay whenever they transact with SETT or any of the SETT based tokens. This happens in the upturn of SETT. When SETT is minted in the upturn, 50% of the newly minted SETT will go back to the ecosystem through SettPay as discounts and cashback, while the other 50% goes to the Validators of the Network to buy back DNAR for burning and increasing staking rewards in proportion to the percentage of DNAR supply burnt.

So when we talked about ‘Alice’ swapping or minting 100SettUSD, we were referring to the Setheum Payment protocol in the background. This part of the Setheum Finance is responsible for distributing what comes from the Setheum Reserve (SERP), so all minted sett have to pass through this, actually are minted from it. Same way, an ecommerce site/platform can harness this beauty of Setheum to attract more users/customers with amazing discounts, the site can sell with discounts without paying for customer acquisition. And these tokens are also tradable like all other tokens on the Setheum Network and atomic swap amongst the settTokens and even between SettTokens and the SETT BasketToken is also available, this swap process is also called “Atomic Shift” on Setheum, due to the nature of how the tokens are minted, SETT is put in, and the system burns it into newly minted SettTokens, and vice versa. This takes place in a tunnel called the “Atomic Shifter” between the SERP and SettPay in Setheum Finance. So without the SERP, Sett Prototokens will not be minted from SETT, and SETT too, let alone distributed.

Setheum Tokenization Protocol (STP)

This is the Protocol that gives the standards on the tokens that can be built on Setheum. The STP has two main STP Standards, which are the ”STP258” and the “STP20” standards.
The STP258 Standard is also called the ‘SETT Standard’, it is the standard with which the Sett family of tokens are governed. Then the STP20 Standard is the standard in which every other token on the Setheum Blockchain would be governed, the number 20 on STP20 is inspired by the ERC20, and this standard has similar features to the ERC20 standard.

Governance

Governance is the way rules, norms and actions are structured, sustained, regulated and held accountable.
Setheum has a multicameral governance system with several avenues/chambers to pass proposals. All proposals ultimately pass through a public referendum, where the majority of tokens can always control the outcome. For low-turnout referenda, Setheum uses adaptive quorum biasing to set the passing threshold. Referenda can contain a variety of proposals, including fund allocation from an on-chain Treasury. Decisions get enacted on-chain and are binding and autonomous. Setheum has several on-chain, permissionless bodies. The primary one is “the Council”, which comprises a set of accounts that are elected in Phragmen fashion. The Council represents minority interests and as such, proposals that are unanimously approved by the Council have a lower passing threshold in the public referendum. There is also a Technical Committee for making technical recommendations (e.g. emergency runtime upgrade to fix a bug).

There will be 4 Chambers / Councils of the Setheum Government, as follows:

- General Council
- Technical Council
- Monetary Council
- Financial Council

1. **General Council:** The General Council will consist of 5 members from the start, they will be in charge of the governance of the general activities of the Network, while every DNAR holder has the right to vote Referendum and suggest proposals. The General Council will initially start with the First Liberators of the Network, then the DNAR holders will be responsible for voting the General Council Members.

   The tenure for the General Council Members is 5 years for now, any future change in constitution laws will be voted for by DNAR holders. There are no limits to how many tenures any Council Member could serve at the moment, any future change in constitution laws will be voted for by DNAR holders. The current denomination is subject to change to best fit the Setheum Network.

2. **Technical Council:** The Technical Council will consist of 3 members from the start, they will be in charge of the governance of the Technical aspects of the Network like bug fixes and maintaining open source projects for example. The Technical Committee will be voted by the General Council.

   The tenure for the Technical Council Members is 4 years for now, any future change in constitution laws will be voted for by DNAR holders. There are no limits to how many tenures any Council Member could serve at the moment, any future change in constitution laws will be voted for by DNAR holders. The current denomination is subject to change to best fit the Setheum Network.

3. **Monetary Council:** The Monetary Council will consist of 3 members from the start and as the name implies, they will be governing the Monetary Regime of the Network. They will also be voted by the General Council. The tenure for the Monetary Council Members is 4 years for now, any future change in constitution laws will be voted for by DNAR holders. There are no limits to how many tenures any Council Member could serve at the moment, any future change in constitution laws will be voted for by DNAR holders. The current denomination is subject to change to best fit the Setheum Network.
4. **Financial Council:** The Financial Council will also consist of 3 members from the start and as the name implies, they will be responsible for governing the Financial Sector of the Network, DEX financial governance for example. They will also be voted by the General Council. The tenure for the Financial Council Members is 4 years for now, any future change in constitution laws will be voted for by DNAR holders. There are no limits to how many tenures any Council Member could serve at the moment, any future change in constitution laws will be voted for by DNAR holders. The current denomination is subject to change to best fit the Setheum Network.

Consensus

Setheum's finality protocol for consensus is the very healthy GRANDPA consensus algorithm. GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement) finalizes batches of blocks based on availability and validity checks that happen as the proposed chain grows. The time to finality is expected to be very fast.

Setheum is able to provide stronger guarantees with fewer validators per shard. Setheum achieves this by making validators distribute an erasure coding to all validators in the system, such that anyone - not only the shard's validators - can reconstruct a block and test its validity. The random validator assignments and secondary checks performed by randomly selected validators make it impossible for the small set of validators to collude.

Staking, Nominating and Validating

Setheum will use a Nominated Proof of Stake (NPoS) mechanism to secure the network. Nominators will nominate validators to be in the active set of validators by staking their Dinar (DNAR) with a validator(s). Validators will produce new blocks, validate Parachain blocks, and guarantee finality. It is important to note that validators will only earn rewards if they have enough staked DNAR to qualify to be in the active set. The active set will update every era, which is 24 hours on Setheum. Setheum is able to provide strong finality and availability guarantees with much fewer validators. Therefore, Setheum uses Nominated Proof of Stake (NPoS) to select validators from a smaller set, letting smaller holders nominate validators to run infrastructure while still claiming the rewards of the system, without running a node of their own. And so with Setheum able to stay alive even when most of the network goes offline, Setheum will be able to survive WWIII.

Conclusion

Setheum has a unique approach to the problems facing the blockchain and provides opportunities that incentivize adoption and usability. Setheum has amazing investment opportunities with astonishing usability and reasonable ROI. Setheum is the brainchild of a cluster of ideas and challenges that inspire the founding of it. And so with the expected level of equilibrium, security, decentralization, scalability, efficiency, diversity and adoption, Setheum is set to implement the neo-blockchain, the blockchain 5.0.

Applied Setheum

Top 80 Applications & Use cases

1. E-Commerce & Retail
2. Token Systems
3. Arbitrage trading
4. Foreign Exchange
5. Financial derivatives
6. Staking Pools, Staking & Passive Income
7. Stability-as-a-Service (For Banks)
8. Mortgage
9. Halal Loans / Flash loans (profit based loans, zero-interest loans)
10. Borderless Payments
11. Escrow
12. Blockchain for blockchains
13. Permissioned and permissionless Blockchains
14. Diaprivacy Applications
15. Crowdfunding
16. ICOs & STOs
17. Fashion Industry
18. Healthcare & Insurance Industry
19. Logistics Industry
20. Supply Chain
21. R&D
22. Ride Hailing
23. On Demand
24. Hotels Industry
25. Oil & Gas Industry
26. Cyber Security Industry
27. Identity and Reputation Systems
28. Decentralized Apps (DApps)
29. Decentralized Cloud Computing
30. Decentralized Exchanges
31. Decentralized File Storage
32. Open Source Communities
33. Team Collaboration Industries
34. StartUp Incubators
35. Hedge Funds
36. Banking industry
37. Bond Management and Tracing
38. Gaming Industry
39. Streaming Industry
40. Transportation Industry
41. Entertainment Industry

42. Sports industry
43. Theme Parks
44. Independent International Organizations
45. Weakened Economies / Currencies (i.e Zimbabwe and Uzbekistan)
46. Fitness industry
47. Agricultural iNDUSTRY
48. Auctions industry
49. Travel & Tourism Industry
50. Advertisement Industry
51. Decentralized Autonomous Organizations
52. Internet of Things (IoT)
53. Artificial Intelligence and Machine Learning (AI & ML)
54. Automobile Industry
55. Mining Industry
56. Real Estate
57. Holdings and International Corporations/Conglomerates
58. Governments and Legislatures
59. Charities and Fundraising
60. Zakat & Wakf
61. NGOs
62. Non-Profits
63. Hospitality industry
64. Lending
65. Education Industry
66. Judiciary
67. Auctions
68. Payroll
69. Global Aid / International Aid
70. Voting (I recommend internal voting on permissioned Blockchains on top of Setheum)
71. Identification and Authentication Systems
72. Regulatory Boards
73. Law Firms
74. Space Industry
75. Cosmologists
76. Pharma Industry
77. Archeology & History Preservation
78. Manufacturing Industry
79. Social Media
80. Venture Capitalists (VCs)

References and Further Reading

1. Blockchain - Wikipedia
   https://en.wikipedia.org/wiki/Blockchain#:~:text=A%20blockchain%20is%20a%20decentralized,alteration%20of%20all%20subsequent%20blocks.
2. The Economics of Sovereign Debt, Bailouts and the Eurozone Crisis - Europa.eu
   https://www.ecb.europa.eu/pub/conferences/shared/pdf/20171120_fiscal_conference/8b_presentation_Martin_ppt.pdf
3. The Value In Cryptocurrency Explained By A Crypto Hedge Fund CIO - YouTube
   https://youtu.be/aVUqXuIcpZ4
4. Never Fork Again
   https://medium.com/polkadot-network/never-fork-again-438c5e985cd8
5. Monetary Aggregate - Investopedia
   https://www.investopedia.com/terms/m/monetary-aggregates.asp#:~:text=A%20monetary%20aggregate%20is%20a,supply%20in%20a%20national%20economy.
6. S. Nakamoto, ”Bitcoin: A peer-to-peer electronic cash system,” 2008
   https://bitcoin.org/bitcoin.pdf
7. The Evolution of Embedding Metadata in Blockchain Transactions
   https://arxiv.org/pdf/1806.06738.pdf
8. An Anonymous Fair Exchange E-commerce Protocol By Indrakshi Ray and Indrajit Ray
   https://www.cs.colostate.edu/pubserv/pubs/Ray-iray-research-icec01.pdf
9. The Effect Of Conformity On Economic Decision Making
   https://digitalcommons.bucknell.edu/honors_theses/140/
10. What does Scalability vs Elasticity mean for blockchains?
    https://hedgetrade.com/scalability-vs-elasticity-for-blockchains-explained/
11. 5 reasons ecommerce should embrace blockchain [infographic]
    https://www.elasticpath.com/blog/5-reasons-ecommerce-should-embrace-blockchain-infographic
12. A Brief Introduction to Differential Privacy
    https://medium.com/georgian-impact-blog/a-brief-introduction-to-differential-privacy-eacf8722283b
13. An overview of blockchain scalability, interoperability and sustainability
    https://www.eublockchainforum.eu/sites/default/files/research-paper/an_overview_of_blockchain_scalability_interoperability_and_sustainability.pdf
14. FSB’s concerns highlight algorithmic stablecoin opportunity
    https://www.finder.com.au/fsbs-concerns-highlight-algorithmic-stablecoin-opportunity
15. Towards Fair and Privacy-Preserving Federated Deep Models
    https://arxiv.org/pdf/1906.01167.pdf
16. 5 Reasons ECommerce should embrace blockchain
    https://www.elasticpath.com/blog/5-reasons-ecommerce-should-embrace-blockchain-infographic
17. Differential privacy: an introduction for statistical agencies
    https://gss.civilservice.gov.uk/wp-content/uploads/2018/12/12-12-18_FINAL_Privitar_Kobbi_Nissim_article.pdf
18. Blockchain + Elastic logistics
    https://medium.com/@victoria27/blockchain-elastic-logistics-486f768b5c45
19. DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-based Incentive

https://eprint.iacr.org/2018/679.pdf

20. Citizen-Centered, Auditable, and Privacy-Preserving Population Genomics https://www.biorxiv.org/content/10.1101/799999v1.full.pdf
21. Finality In Blockchain Consensus https://medium.com/mechanism-labs/finality-in-blockchain-consensus-d1f83c120a9a
22. Connecting blockchains together https://consensys.net/academy/blockchain-basics-book/connecting-blockchains-together/
23. A verifiably secure and proportional committee election rule https://arxiv.org/abs/2004.12990
24. Proof Of Stake (Wikipedia) https://en.wikipedia.org/wiki/Proof_of_stake
25. Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on POS and PBFT and Its Application in Blockchain https://www.researchgate.net/publication/340614907_Hybrid_Consensus_Algorithm_Optimization_A_Mathematical_Method_Based_on_POS_and_PBFT_and_Its_Application_in_Blockchain
26. Overview of Polkadot and its Design Considerations https://eprint.iacr.org/2020/641.pdf
27. POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK https://polkadot.network/PolkaDotPaper.pdf
28. Ethereum White Paper https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
29. GRANDPA: A Byzantine Finality Gadget https://github.com/w3f/consensus/blob/master/pdf/grandpa.pdf
30. Poster: GRANDPA Finality Gadget https://www.researchgate.net/publication/337095861_Poster_GRANDPA_Finality_Gadget
31. WebAssembly (WASM) - Wikipedia https://en.wikipedia.org/wiki/WebAssembly
32. WebAssembly (WASM) - MDN https://developer.mozilla.org/en-US/docs/WebAssembly
33. The Scalability Trilemma in Blockchain https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df
34. The Other Trilemma: Governing Global Finance https://www.moneyandbanking.com/commentary/2017/7/23/the-other-trilemma-governing-global-finance
35. Solving the Blockchain Trilemma https://www.coinbureau.com/analysis/solving-blockchain-trilemma/
36. Solving The Scalability Trilemma https://www.qredo.com/blog/solving-the-scalability-trilemma
37. The financial trilemma https://www.sciencedirect.com/science/article/abs/pii/S0165176511000115#:~:text=The%20financial%20trilemma%20states%20that,three%3B%20one%20has%20to%20give.