Setheum

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيم

White Paper

"For a cause. Light Upon Light"

By Muhammad-Jibril B.A.
https://linktr.ee/iamkhalifamba
https://setheum.xyz
11/22/2021

Abstract

We see a lot of cryptocurrencies coming up everyday, but what we don't see is a cryptocurrency that is decentralised, secure, scalable and having the option for price stability at the same time, especially one without debt or having to be centralised by a physical reserve in a corporate bank, and one that is also propping adoption. Setheum gives us the properties of both Fiat and Crypto with PES (Price Elasticity of Supply) without compromising decentralisation 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 decentralisation, scalability, mass adoption, diversity and interoperability.

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

- Providing Humanitarian Aid on-chain
- Fixing the stablecoin inefficiency, narrow adoption strategies & use cases, and centralization Issues
- Propping and boosting Industrial synchronisation and mass adoption of the Blockchain with all kinds of communities
- 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 decentralised 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" practises 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 the 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 (from the first whitepaper), I propose Setheum to change the lives of people and the situation of the NEEDY.

The Blockchain

Understanding The Blockchain

A blockchain is a decentralised, 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.

1st Generation - 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".

2nd Generation - 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 decentralised storages such as Ethereums Swarm.
[DApp = frontend + contracts **(**running i.e. on Ethereum**)]**

3rd Generation and Web3.0 (leapfrog)

The 3rd generation blockchain revolves around the idea of interoperability and the 3 Ss namely sustainability, scalability, and security. This is where we see Proof of Stake implementations that are environmentally friendly and alternative to Proof of Work for longtime environmental sustainability with works like Polkadot and Setheum. Here we see decentralised storage like Filecoin and IPFS, and Chia that use Storage Consensus mechanisms. Here we see state upgradability without forking like in Polkadot and Setheum, we see on-chain built-in DeFi systems like in the case of Setheum. We also see layer 0 solutions like Polkadot and layer 2 solutions alongside many innovations in the blockchain and crypto space.

But, we haven't seen specific significant contributions to the Islamic Finance market in this space, little to no DeFi presence of the muslim community and those Christians alike that seek out for halal (permitted) zero-interest theologically acceptable DeFi protocols and modes of making money apart from trading speculation on exchanges, staking on PoS and hodling tokens. This is why Setheum was completely rectified into the conclusive go-to DeFi network for people and communities alike that share my enthusiasm as well as those that share my concerns.

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 centralised 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.

setheum.xyz

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.

Propping Adoption: 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. Propping adoption basically means to support 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 familiar currencies, our day to day activities, our practical use cases of the blockchain, our communal utilities 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 Setheum Currencies to trade and transact more efficiently and rely on the network's Economic stability for long term benefits.

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 or cashouts.

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 maximise 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 centralised. Therefore no two hands to type the wrong numbers for "brrr";

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-Serp Stability System" (DS3) that introduces the SERP (Setheum Elastic Reserve Protocol), The Dinar (DNAR) and the Serp (SERP Tokens). My proposed price-stable "SETR" 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 and mechanisms based on the "PES" (Price Elasticity of Supply). 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 decentralised, 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 one of the best use cases for cryptocurrencies and a dam of market liquidity. Setheum Finance Protocol makes that balance of truthful trustless equilibrium between fiat currencies and cryptocurrencies. Setheum is leveraging Dinar:Serp cryptocurrency bilateral-collateral backing as the reserve assets for it's fiat-pegged stable currencies, and also maintains its decentralised nature while also avoiding extreme price volatility and hyperinflation. Setheum Finance has combined Bitcoin, Ethereum (discussing the S-EVM further down the pages), Fiat and Stablecoin features that maximise the better of all concepts. 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 [SERP Treasury], where everyone on the network is a participant in the economy and has some rights over the SERP 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.xyz

The Blockchain Network

Setheum is a DeFi operating system, liquidity exchange provider, and financial system that resolves the issues of liquidity and stablecoin reliability issues mostly raised by centralised stablecoins by creating algorithmic elastic stablecoins stabilised by prestine crypto assets and managed by the network's democratic governance system that gives back all upturn elasticity returns and market growth to the community. Setheum is built with the Substrate modular interoperable blockchain framework and is based on the Nominated Proof of Stake (NPoS) consensus algorithm. In Setheum, one can pay for transaction fees in any token currency without having to hold Setheum's native token. Setheum implements a free and fair economic system that pursues equality of opportunity and the maximisation of public utility in the crypto-economy.

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.

Recognizing strong regionalism in money, we provide SETUSD (pegged to $1) and SETR (pegged to $2). For number details on the currencies, read further below. The SETUSD is maintained by a CDP (Collateralized Debt Position) System based on the SERP whereby the users of the CDP maintain the value just like MakerDAO (without the interest rates of stability fees) and the SERP maintains the SETR's stability with the SetheumDEX (aka. SetSwap) and the SETUSD, creating an independent ecosystem that neither needs external mechanisms to stabilise nor to expand as it also ha inflation rates and mechanisms governed by the Financial Council (an on-chain governance council) that incentivizes users to spend or trade (read further below to see the uniqueness of the Setheum DEX and other Setheum products);

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 its currencies, which is basically the multiplication of the Monetary Base (MB or M0) with Fractional Reserve Banking.

Setheum mints SETR through an elastic money supply relying on PES and through the on-chain SERP inflation mechanisms and the EFE (Exchange Fee Evaluator - read further below for the unique EFE), so the amount of SETR to be minted is proportional to the pairing of DNAR:SERP and its price relative to the SETUSD versus the corresponding DEX pool relative to its fiat peg and its market cap. Whenever SETR or SETUSD is minted automatically by the SERP, some amounts are used for T1 tokens (SETM, SERP, DNAR) buyback (read further below for these numbers too) and these SERP:DNAR tokens are used in exchange to buy back excess SETR:SETUSD from the market through the built-in DEX

(SetheumDEX/SetSwap). In the long term this provides a very strong backing for the SERP's stablecoins as the values of the T1 tokens increase overtime in the market;

Once the system has detected that the price of a SetCurrency has deviated from its peg, it must apply pressures to normalise 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, the DNAR:SERP reserve pairs absorb SetCurrency contraction costs through newly minted tokens that get swapped on the SetheumDEX/SetSwap for the SetCurrencies which then gets immediately burned in the SERP directly before it even leaves the DEX.

The Contraction and Minting method in SERP, is inspired by the Terra model of contraction and minting for price-stability two years back when I first went into designing how Setheum should be, and I went through writing and scrapping a lot of whitepapers over the years. But the SERP improves much on that.

Setheum Fiscal Policy

Users of the setheum network get what I'd like to call Cashdrops from the SERP-Treasury that was issued due to a need for price stability by increase in supply or due to SERP inflation mechanisms for economic growth.

CashDrops are essentially cashback given (from the CashDropFund in the SerpTreasury, so it's not unlimited) to the users of the SetCurrencies whenever they claim on their transactions. So, each transaction has a sort of toggle button that says "claim cashdrop" before the transaction is sent (transfers "to" only).

Setheum Elastic Reserve Protocol (SERP)

The Setheum Elastic Reserve Protocol (SERP) is the backbone of the Setheum Economy, it is the stablecoin financial system of Setheum first of its kind and unique to Setheum.

The Serp implements algorithmically stabilised stablecoins that are serped or stabilised algorithmically with the Serp Reserve Assets called the "Serp and Dinar" which are a Tier-1 token class (free-floating cryptocurrency) on Setheum, sort of like the gold-standard but superior in technology and system utility, **bilateral-backing (with SERP & DNAR)** and a lot more.

Elasticity is a proportionate change in one variable over the proportionate change in another variable:

$$pes \ = \ \frac{\%\Delta QS}{\%\Delta P}$$

$$serptes \ = \ \frac{\frac{mp}{pp}\times S}{1} \ || \ \frac{\frac{pp}{mp}\times S}{1}$$

Where **QS** is the quantity of supply and **P** is the price, representing the %Change in Quantity / %Change in Price. Where **S** is the total Supply, **mp** is the market-price, **pp** is the peg-price.

If price is above peg, **mp/pp**, else if price is below peg, **pp/mp**;
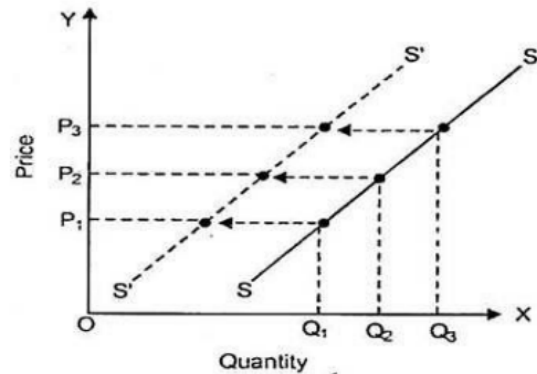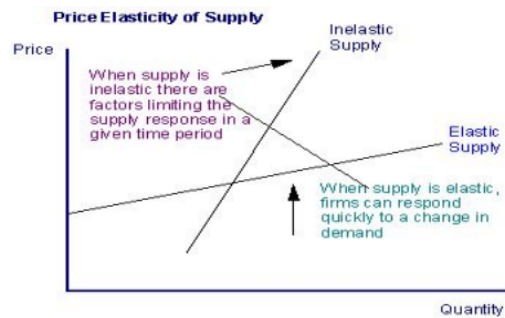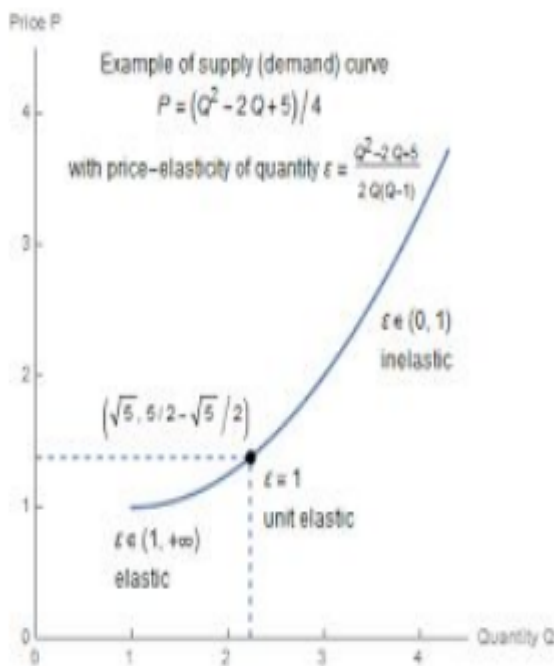
The SETR is automatically adjusted by the SERP-TES, while the SETUSD is adjusted by the SERP-SetMint based on CDPs (Collateralized Debt Positions).

When a Setheum StableCurrency goes higher than its peg in price (higher demand than supply), then that height in demand is injected into the economy to stabilise the price of that stablecurrency, we call that a SerpUp, the opposite is done for a SerpDown to Serp down the supply.

The supply injected into the economy during upturns/serpups of a stablecurrency is distributed as such **40% to buy back the Serp Reserve Asset for burning, 10% to the "Setheum Public Fund", and 50% to the "CashDrop Pool" for users to claim.**

The SERP also issues a per period inflation rate balance for the Setheum stable currencies, the inflation rate can be adjusted through the governance under the Setheum Shura Council with a democratically voted approval by the members of the Shura Council.
The Governance is discussed further below.

The injected inflation balance will be distributed as such in the table below:

Treasury	BuyBack DNAR	BuyBack SERP	BuyBack SETM	CashDrop Pool
20%	20%	20%	20%	20%

CashDrops

CashDrops are essentially cashback given (from the CashDropFund, so it's not unlimited) to the users of the SetCurrencies whenever they claim on their transactions. So, each transaction has a toggle button that says "claim cashdrop" before the transaction is sent (transfers "to" only).
Below is the CashDrop claims minimum transfer amounts that can claim and cashdrop rates per currency of claim (these parameters can be updated via network runtime upgrade with the approval of the governance council of Setheum):

Currency	Min. Claimable Transfer	Max. Claimable Transfer	Claim Rate
SETR	1 SETR	200_000 SETR	4%
SETUSD	10 SETUSD	700_000 SETUSD	2%

Tokens & Stablecoins

There are two classes of currencies, free-floating tokens (what I like to call the "Tier-1 Tokens" (T1)), and stable-currencies (what I like to call "Tier-2 Tokens" (T2) OR simply "SetCurrencies") in Setheum. They are explained in the table below with initial details and characterizations.

Ticker	Name	Class	Initial Supply	Price	Init Market Cap (Ecosystem = $7,283,200,000)
SETM	Setheum	T1	3,133,000,000	$0.2	$626,600,000
DNAR	The Dinar	T1	70,000,000	$3.0	$210,000,000
SERP	Serp	T1	258,000,000	$0.7	$180,600,000
SETR	Setter	T2	1,566,500,000	$2 (stablecoin)	$3,133,000,000
SETUSD	SetDollar	T2	3,133,000,000	$1 (stablecoin)	$3,133,000,000

setheum.xyz

The SetMint Protocol

Multi-Collateral CDPs on SetMint

Every SETUSD issued through SetMint is backed in excess by a crypto asset and is stabilised against the USD through the SetMint Protocol - a dynamic system of Zero-Interest Collateralized Debt Positions (CDPs) in extension to the SERP - the Setheum Elastic Reserve Protocol, on-chain governance and incentivized key actors.

The CDP mechanism design is inspired by the first decentralised stablecoin project MakerDAO, which has become the DeFi building block in the Ethereum ecosystem.

Together with a set of incentives, supply & demand balancing, and risk management mechanisms, as the core components of the Setmint protocol, the value of a SetDollar (SETUSD) is pegged to the value of a US Dollar (USD), with relative stability and this helps stabilise the SETR through the Setheum Elastic Reserve Protocol (SERP).

Every CDP holds the collateral assets deposited by the user who opened the CDP that created the SETUSD tokens, together with its associated SETUSD debt position. The deposited collateral assets inside the CDP are locked and cannot be withdrawn by the user until the associated SETUSD debt is paid back. Active CDPs are always over collateralized with the collateral with value that exceeds the value of the debt.

Unlike Ethereum, where an external liquidator is required to monitor and close dangerous positions, which is by and large due to the limitations of Ethereum, the SetMint Protocol is able to use Off-chain Worker - an automatic scheduler service unique to Substrate - to automate this process and inherently increase security and stability of the stablecoin.

Inspired by MakerDAO Protocol, the CDP (Collateralized Debt Position) protocol on Ethereum. The Setheum CDP has zero interest rates, zero stability fees, and is fully halal and collateralized.
This differentiates SetMint from any other CDP Protocol, making it by far the only halal loan protocol in the entire industry. And it is ***Multi-Collateral.***

Just reserve some collateral to mint some **SETUSD**, when returning the loan just return exactly what was loaned and unreserve the collateral with no fees and no interest.

This lets the muslim world also participate in the industry and take part in trading and yield making strategies that are within their dome of principles, for me this is a gamechanger that I wished was there for me, therefore I am building it for people like me who need it but haven't been given the chance to be pleased by it, and also non-muslims that want to break-free from the interest-based alternatives to a more efficient system based on truth, fairness and equality.

setheum.xyz

The SetMint CDP Process

- **Depositing Collateral**
  First of all, to create a CDP, the user sends a request to the SEtMint protocol that deposits the cryptocurrency that will be locked as collateral to open a CDP and become a CDP holder.
  While multiple types of crypto assets are supported by the SetMint protocol, only one single type of asset is collateralized in the creation of a particular CDP.

- **Borrowing SetDollar and Opening CDP**
  The user then sends a request to borrow the desired amount of SETUSD tokens, capped by the quotient of the value of the crypto assets deposited and the collateral-to-debt ratio (check the table below for the numbers).
  The SetMint protocol would lock the asset deposited, then mint the SETUSD tokens accordingly, and mark the same amount as a debt in the CDP. The locked collateral will not be released until the outstanding debt in SETUSD is paid, which would then be burnt from existence.

- **Paying back SETUSD**
  So, If the CDP holder wants to close an active CDP that is not at risk, they need to deposit enough SetDollars (SETUSD) to pay back the outstanding debt in the CDP, with no-interest policy, there is no need to pay a stability fee or any accumulated interest whatsoever, this is unique to Setheum.
  And with the SERP (Setheum Elastic Reserve Protocol) in place, it can absorb any instability in the stablecoins.

- **Closing the CDP**
  After receiving the outstanding SetDollars in debt, the CDP becomes debt-free, then the CDP holder is able to retrieve their collateral back and the CDP is then closed by the SetMint.

Price Stability Mechanisms in the SetMint

The SETUSD is designed to peg to the US Dollar at a ratio of 1:1 that the Network aims to maintain the value of one SetDollar approximately to one US Dollar at all times.
Our unique strong peg to US Dollar is achieved through an automatic SERP-TES elasticity algorithm, an automatic risk management algorithm within the SetMint Protocol together with community governance.
The SERP-TES has been discussed above, more details on the risk management are further below.

Risk Management in the SetMint

The Financial Council has governance rights and responsibilities for managing risks of the SetMint on the Setheum Network, including authorising manual or automatic (algorithmic) adjustments of risk parameters.

Since multiple types of assets with different risk profiles are accepted as collaterals of CDPs, all risk parameters of CDPs and liquidation parameters are set up separately across various collateral types and are to be adjusted by the SetMint Protocol automatically or by voting from the Financial Council.

Adjusting Risk Parameters of CDPs

- **Liquidation Ratio:**

    The price fluctuation of an underlying collateral affects the risk profile of the borrowed SETUSD, hence adjusting the liquidation ratio to a degree creates a stability shell for the stablecoin.

    The collateral-to-debt ratio of all active CDPs is monitored constantly by the system, by dividing the current market value (in SETUSD) of the collateral locked in the CDP by the outstanding debt balance.

    Once the current collateral-to-debt ratio of an active CDP becomes low enough that it reaches a certain threshold - the Liquidation Ratio, the system will automatically trigger a liquidation of the CDP. A riskier collateral type is usually associated with a higher Liquidation Ratio, and the opposite is true, and vice versa.

- **Liquidation Penalty:**

    The liquidation penalty is a disincentive for users to leave a position in danger, hence provides additional safeguard and stability for the stablecoin.

    All active CDPs are constantly monitored by the SetMint system, once the value of a CDP collateral has fallen below the liquidation ratio, the CDP is regarded to be risky and is automatically liquidated by the system then a liquidation penalty in SetDollar (SETUSD) will be charged to the CDP holder and sourced from the collateral auction or swapped by DEX (SetheumDEX / SetSwap).

- **Debt Ceiling:**

    For each type of crypto asset that can be used as collateral for CDPs, a maximum amount of total outstanding debts in SETUSD - the Debt Ceiling, is preset to cap the total collateral of such assets in the SetMint on the Setheum network, which ensure both diversification and risk management of the collateral portfolio.

    Once the Debt Ceiling for an asset is reached, no new CDP can be generated until some existing CDPs are closed.

setheum.xyz

Collaterals currently are **SETM**, **SERP**, **DNAR**, **SETR**. More collaterals could be added through runtime upgrades by system governance. The collateral parameters are as below:

Collateral	Liquidation Rate	Liquidation Penalty Rate	Required Liquidation Rate	Max. Debit Value
SETM	105%	5%	110%	25,800,000 SETUSD
SERP	105%	5%	110%	25,800,000 SETUSD
DNAR	105%	5%	110%	25,800,000 SETUSD
SETR	10te3%	3%	106%	33,000,000 SETUSD

Initial Token Allocations

Currencies	Treasury	SPF	DEX Offering	Foundation	Team	Advisors and Partners	CashDrop Pool
SETM	10%	10%	20%	20%	32%	8%	-
SERP	-	10%	30%	20%	32%	8%	-
DNAR	-	10%	30%	20%	32%	8%	-
SETR	-	10%	20%	20%	32%	8%	10%
SETUSD	-	10%	20%	20%	32%	8%	10%

Vesting Schedule on Allocations

Currencies	Advisors and Partners	SPF	Foundation	Team
SETM	50% for 7 years	50% for 9 years	50% for 23 years	50% for 23 years
SERP, DNAR	52% for 5 years	52% for 7 years	52% for 19 years	52% for 19 years
SETR	30% for 3 years	30% for 3 years	30% for 3 years	30% for 3 years
SETUSD	25% for 2 years	25% for 2 years	25% for 2 years	25% for 2 years

setheum.xyz

Built-In Exchange (SetSwap - DEX)

Inspired by Uniswap V2, Setheum has a built-in Decentralised Exchange that I like to call "**SetSwap**" (or **Set**heum**Swap**). In SetSwap there is what I call the EFE (Exchange Fee Evaluator) that is the first of its kind and unique to Setheum (one of the Setheum originals).

The EFE essentially lets available two types of Exchange fees, one for Tier-2 paired pools (LPs paired with at least one Setheum stablecurrency for example "BTC_SETUSD_LP"), then another fee structure for every other pool that is not a "T2-Paired-LP" on the DEX.

Exchange Fee Evaluator (EFE)

The EFE structure takes less fees from traders that swap with a "T2-Paired-LP'' than it takes from a "non-T2-Paired-LP" (i.e. "BTC_DNAR_LP"). The difference between these fees is then paid to the pool by the SERP by issuing the T2-token to the pool to balance out the full Exchange Fee. This lets the traders pay less fees while the Liquidity Providers earn more. This in turn attracts more traders, more trading volume, more liquidity, more market attractiveness, more trading opportunities and more natural economic growth based on market drive and demand, which in turn props the market value of the Serp and the Dinar and the entire Setheum tokens which in turn improves overall market performance and economic growth. The initial Exchange Fees are as such, exchange fee is 0.3%, stablecurrency exchange fee is 0.1%, and the EFE (effect/difference) is 0.2%. They can be updated with governance through runtime upgrades.

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. Decisions get enacted on-chain and are binding and autonomous. Setheum has several on-chain, permissionless bodies. The primary one is "the Shura Council", which comprises a set of accounts that are elected. There is also a Technical Committee for making technical recommendations (e.g. emergency runtime upgrade to fix a bug), and other councils explained below. There will be 3 Chambers / Councils of the Setheum Government, as follows:

1. **Shura Council:** General governance like approving runtime upgrades, it is basically the General Council.
2. **Technical Committee:** 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.
3. **Financial Council:** They will be responsible for governing the Financial Sector of the Network, DEX financial governance, Multiple Oracle registrations, SERP inflation rates, buybacks and CashDrop rates et al., for example.

Consensus

Setheum's finality protocol for consensus is the very healthy GRANDPA consensus algorithm. GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement) finalisess 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. Setheum uses BABE for block authoring and GRANDPA for finality.

Specification Sheet

Key	Value
Currencies (symbol = decimals, index)	SETM = 18, 0; SERP= 18, 1; DNAR = 18, 2; SETR = 18, 3; SETUSD = 18, 4;
Native Token (symbol = decimals, index)	SETM = 18, 0;
SS58 Prefix	25
EVM chain_id	25888

ERC20 Contracts - Predeployed Contracts	<pre>- SETM contract address:
	`0x0000000000000000000000000000000001000000`.
	- SERP contract address:
	`0x0000000000000000000000000000000001000001`.
	- DNAR contract address:
	`0x0000000000000000000000000000000001000002`.
	- SETR contract address:
	`0x0000000000000000000000000000000001000003`.
	- SETUSD contract address:
	`0x0000000000000000000000000000000001000004`.
	- LP_SETM_SETUSD contract address:
	`0x0000000000000000000000010000000000000004`.
	- LP_SERP_SETUSD contract address:
	`0x0000000000000000000000010000000100000004`.
	- LP_DNAR_SETUSD contract address:
	`0x0000000000000000000000010000000200000004`
	- LP_SETR_SETUSD contract address:
	`0x0000000000000000000000010000000300000004`
	- Token contract address:
	`0x0000000000000000000000000000000000000800`.
	- StateRent contract address:
	`0x0000000000000000000000000000000000000801`.
	- Oracle contract address:
	`0x0000000000000000000000000000000000000802`
	- Schedule contract address:
	`0x0000000000000000000000000000000000000803`
	- DEX contract address:
	`0x0000000000000000000000000000000000000804`</pre>

Block authoring	BABE
Finality	GRANDPA
BlockTime	6 seconds
BlockSize / `BlockLength`	1.25MB to 3.75MB

setheum.xyz

BlockHashCount	2400 (`4 hours`)

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 Setheum (SETM) with a validator(s). Validators will produce new blocks, validate chain blocks, and guarantee finality. It is important to note that validators will only earn rewards if they have enough staked SETM to qualify to be in the active set. The active set will update every era, which is `2 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. **The Staking rewards range from a minimum of 2.58% to a maximum of 25.8%, ideal stake of 50%;**

Initial Airdrop Event (IAE)

Setheum's initial Token Offering will not be a traditional ICO, IEO or IDO. It will instead be an IAE, an Initial Airdrop Event that will take place on our Community Social Media outlets. In this event, we will give away the IAE Allocated tokens as allocated above in the tables, in an airdrop on Setheum to the participants of the IAE.
There will be a referral program in the IAE with a large number of participants. We will not require you to pay anything to join, it is absolutely free to join IAEs and this is also a free IAE. The DEX Offering will be done as a liquidity provision to the SetSwap (Setheum's built-in DEX), with SETUSD liquidity pairs. Users can buy the Tier-1 tokens (SETM, SERP, DNAR) on the SetSwap with the stablecoins (SETR, SETUSD) they get from the Airdrop Event.

Beware of imposters, we will never ask for your private keys, or to send us anything, or contact you individually or send you links on emails or DMs, and we will certainly not recommend that you use unknown and untrusted wallets.
So, keep in touch and wait for the IAE. We will announce it on our Social Media accounts. Follow us on the accounts on our website https://setheum.xyz

Conclusion

Setheum has a unique approach to the problems facing the space and provides opportunities that incentivize adoption and usability and most importantly because it helps people with a means to survive, thrive and get educated through its public fund (SPF). Setheum has amazing investment opportunities with astonishing usability. 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, decentralisation, scalability, efficiency, diversity and

setheum.xyz

adoption, Setheum is set to implement the neom of finance in the Web3 Ecosystem extending hands to the halal consumer market and the Islamic Finance community.

References and Further Reading

1. Setheum Labs Blog: https://medium.com/setheum-labs
2. MakerDAO: https://makerdao.com/en/whitepaper
3. Uniswap V2: https://uniswap.org/whitepaper.pdf
4. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008 https://bitcoin.org/bitcoin.pdf
5. Ethereum: https://ethereum.org/en/whitepaper
6. Substrate: https://www.parity.io/blog/what-is-substrate
7. NPoS: https://research.web3.foundation/en/latest/polkadot/NPoS/index.html
8. 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
9. Never Fork Again https://medium.com/polkadot-network/never-fork-again-438c5e985cd8
10. The Effect Of Conformity On Economic Decision Making https://digitalcommons.bucknell.edu/honors_theses/140/
11. What does Scalability vs Elasticity mean for blockchains? https://hedgetrade.com/scalability-vs-elasticity-for-blockchains-explained/
12. 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
13. FSB's concerns highlight algorithmic stablecoin opportunity https://www.finder.com.au/fsbs-concerns-highlight-algorithmic-stablecoin-opportunity
14. 5 Reasons ECommerce should embrace blockchain https://www.elasticpath.com/blog/5-reasons-ecommerce-should-embrace-blockchain-infographic
15. Blockchain + Elastic logistics https://medium.com/@victoria27/blockchain-elastic-logistics-486f768b5c45
16. The Other Trilemma: Governing Global Finance https://www.moneyandbanking.com/commentary/2017/7/23/the-other-trilemma-governing-global-finance