



White Paper - 3.0

Blockchain 5.0 - Blockchain of Everything (BoE)

Solving The Blockchain Trilemma with BoE

(Trilemma to Monolemma to Equilemma to Equilibrium)

By Muhammad Jibril A Bashir

<https://twitter.com/iamKhalifaMBA>

<https://instagram.com/i.am.khalifa>

<https://setheum.xyz>

11/8/2020

Abstract

It is a fact that there is an existing so-called “Trilemma” in the blockchain world, where there is a choice between Decentralization, Security, or Scalability, but is that solvable? I bring about a bigger lemma, the blockchain “Equilemma”, what is the blockchain equilemma, why is it important, is there perhaps a solution and if yes, what is this solution. I bring about a solution for this equilemma and how wide are the use cases when solved and some ideas that could be built on Setheum.

With protocols upon protocols, Setheum is a blockchain of protocols, or the blockchain of blockchain to be more elaborate, that balances the unbalanceable in elegance. The implementation of smart contracts, the elasticity of crypto, diaprivacy (Differential Auditable Privacy), propadoption mechanisms, Applied Setheum, Setheum Monetary Policy, Tokens and PoS staking, Validator Rewards and Penalties, The Setheum Elastic Reserve Protocol, Flash Loans (Zero-interest Loans), stability and trust in Setheum will be part of many aspects of Setheum in this white paper.

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?I'll define it soon). Setheum gives us the properties of both Fiat and Crypto with PES 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 Blockchain Trilemma, stablecoins, Flash Loans, Differential Auditable Privacy (Diaprivacy), Propadoption.. to achieve security, decentralization, scalability, privacy, mass adoption, diversity and interoperability in blockchain technology.

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

- ❖ Solving The Blockchain Trilemma
- ❖ 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 cryptocurrencies.
- ❖ Solving the usability and sovereignty issue on most popular Blockchains
- ❖ Solving Forking issues



Table of Contents

- ❑ Brief History
- ❑ The Blockchain Equilemma
 - ❑ The Blockchain
 - ❑ Blockchain 1.0
 - ❑ Blockchain 2.0
 - ❑ Blockchain 3.0
 - ❑ Blockchain 4.0
 - ❑ Blockchain 5.0
 - ❑ The Trilemma
 - ❑ The Monolemma
 - ❑ Introducing Setheum
 - ❑ The Equilemma
 - ❑ Sustainability
 - ❑ interoperability
 - ❑ Diaprivacy (Differential Auditable Privacy)
 - ❑ Elasticity & Economic Stability
 - ❑ Propadoption
 - ❑ Filling the Financial Gap
 - ❑ Setheum Finance Protocol
 - ❑ Setheum Monetary Policy
 - ❑ Setheum Fiscal Policy & Setheum Payment Protocol (SettPay)
 - ❑ XCMP (Cross Chain Messaging Protocol)
 - ❑ Code Execution - WASM (WebAssembly)
 - ❑ Setheum Tokenization Protocol (STP)
 - ❑ Governance
 - ❑ Consensus
 - ❑ Staking, Nominating and Validating
- ❑ Conclusion
- ❑ Applied Setheum - Applications
- ❑ Acknowledgements
- ❑ References and Further Reading



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 Equilemma

Understanding The Blockchain, The Trilemma And The Equilemma

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 Ethernets 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.



Limitation #1: Scalability

The first limitation is scaling - decentralized applications built on top of Ethereum are inhibited by a shared rate of 15 transactions per second. This is due to the fact that Ethereum still uses Proof-of-Work and that Ethereum dApps compete for the limited resources of a single blockchain.

Limitation #2: Usability

The second limitation is the relatively low flexibility granted to developers. Because the EVM is a sandbox that needs to accommodate all use cases, it optimizes for the average use case. This means that developers have to make compromises on the design and efficiency of their application (for example, requiring use of the account model in a payments platform where a UTXO model may be preferred). Among other things, they are limited to a few programming languages and cannot implement automatic execution of code.

Limitation #3: Sovereignty

The third limitation is that each application is limited in sovereignty, because they all share the same underlying environment. Essentially, this creates two layers of governance: that of the application, and that of the underlying environment. The former is limited by the latter. If there is a bug in the application, nothing can be done about it without the approval of the governance of the Ethereum platform itself. If the application requires a new feature in the EVM, it again has to rely entirely on the governance of the Ethereum platform to accept it.

Limitation #4: Forking

The fourth limitation is that once governance is forking. In blockchain technology, a **fork** is defined variously as:

- "what happens when a blockchain diverges into two potential paths forward"
- "a change in protocol" or
- "a situation that "occurs when two or more blocks have the same block height"

Forks are related to the fact that different parties need to use common rules to maintain the history of the blockchain. When parties are not in agreement, alternative chains may emerge. While most forks are short-lived some are permanent. Short-lived forks are due to the difficulty of reaching fast consensus in a distributed system. Whereas permanent forks (in the sense of protocol changes) have been used to add new features to a blockchain, to reverse the effects of hacking, or catastrophic bugs on a blockchain as was the case with the bitcoin fork on 6 August 2010 or the fork between Ethereum and Ethereum Classic. Setheum Solves this in a number of approaches.

These limitations are not specific to Ethereum but to most blockchains trying to create a single sovereign blockchain governance that would fit all use cases without extensive sovereignty. This is also where Setheum comes into play just as in many sectors.



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 Setheum is 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). Forking is not even a choice on blockchain 5.0 with Setheum's implementation of Upgrades using WASM. But before we meet Setheum, let's meet the trilemma, the monolemma.. and then the Equilemma just after a glimpse at the face of Setheum. 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.

The Trilemma

Blockchain projects are known for their vision and ambition - but what they prioritize and what they're known for can vary. The projects usually rotate around three core concepts: decentralization, scalability and security.

The Blockchain Trilemma addresses the challenges developers face in creating a blockchain that is scalable, decentralized and secure - without compromising on any facet. Blockchains are often forced to make trade-offs that prevent them from achieving all 3 aspects:

1. Decentralized: creating a blockchain system that does not rely on a central point of control.
2. Scalable: the ability for a blockchain system to handle an increasingly growing amount of transactions.



3. **Secure:** the ability of the blockchain system to operate as expected, defend itself from attacks, bugs, and other unforeseen issues.

While some developers believe that the blockchain data structure itself has inherent limitations that prevent it from scaling, many architects believe that it's possible to build a blockchain project that hits all three targets: one that is scalable, decentralized, and secure and I myself believe this.

The Monolemma

So, a monolemma is when the main objective of all options in an argument is common, but perceived to be uncommon due to the difference in approach and different levels of convenience. So an Equilemma can in fact be an extended monolemma, if and only if what is needed is a balance of all approaches parallel to each other to achieve the common objective, just like it is in this case.

Decentralization: Decentralization is the core component of public blockchains. In traditional finance, the system is entirely centralized. Customers pass control of their assets to banks, from their personal documentation to their assets, for the banks to handle with full control. Bitcoin and other early cryptocurrencies offered a decentralized and transparent alternative, serving as the issuance and storage of money, without the need for a centralized entity. Decentralized systems matter because they empower permissionless ownership where anyone can use and build on the platform. Decisions are made by consensus, which means transactions are approved by a group of nodes as opposed to an individual node. Once these transactions are verified by consensus, they can't be altered after the fact. Therefore, risk isn't placed in one central entity, and trust doesn't rely on another individual when conducting a transaction. The trade-off of pure decentralization, however, is speed. If a transaction requires multiple confirmations before reaching consensus, then inherently, it would take longer than if a transaction can be confirmed by a single entity. Bitcoin is known to be robustly decentralized, but at the same time, pretty slow.. Of course this won't be the case for Setheum.

Scalability: Scalability is important for mass adoption. Scalability is among the key traits of a blockchain. It is indicative of the blockchain's capability to adapt and perform adequately under an increasing or expanding workload or scope. A blockchain that ends up scaling well will be able to maintain or even boost its efficiency. It's the question of how much a blockchain system can sustain, and whether the system can operate smoothly as demand increases. Higher block time means nodes are less fault tolerant, higher throughput means a higher probability of failure between nodes, which is why we've seen a number of high profile, high speed blockchains compromise on decentralization with a minimal number of nodes or block producers in general.. of course this won't be the case with Setheum.

Security: As a novel, promising technology looking to make its name by improving existing infrastructure, the security of a blockchain system is paramount. To be truly considered secure, a crypto protocol needs to be resilient in the short term and immutable in the long term, in other words the protocol needs to be able to prevent or recover from short term attacks without making changes to the previous state of the distributed ledger.



The Protocol Throughput, which defines the number of 'Transactions Per Second' (TPS) a network can handle plays a major role in defining how resilient a protocol is against spam and TPS based attacks, such attacks are possible because decentralized network nodes tend to be asynchronous, meaning the higher the TPS, the longer it takes the information to arrive from one node to another. This time lapse or propagation delay also known as 'Network Latency' may increase the probability of Orphan Blocks, and as a result, the higher the propagation delay, the higher the probability of attacks.. of course this won't be the case for Setheum.

With a cannonade of high-profile hacks of exchanges and manipulated vulnerabilities in source code, it's evident that many crypto projects had chosen to focus on decentralization and scalability, leaving security behind. Blockchain ecosystems, for all their upsides, hinge on the strength of the underlying source code - like anything else, it must be carefully examined. Due to the transparent nature of the source code and the potentially lucrative benefits one can receive from conducting a successful attack, blockchains have become prime targets for hackers. Promising blockchain use cases have faced setbacks that stifled their growth, such as the notorious DAO attack, which was the result of improper source code security. While scalability focuses on the upside, security prevents the downside - something just as important, but all too often forgotten.

The Equilemma

While most are still worrying about the Trilemma, I care more about the Equilemma, the difficulty to balance blockchain architectures on the trilemma scale, if solved will provide unprecedented levels of reliability and vast opportunities to bolster technological innovation and blockchain's mass adoption, the blockchain is in constant development and innovation, there are a lot of issues it needs to get into, and a lot of projects out there take on some of the issues one more important than the other, but we need a blockchain that encompasses all these attributes and provides an equilibrium between the conflicting forces while also terminating harmful trade-offs in the attributes it possess.

The Equilemma is by definition the state of imbalance between forces or mechanisms often perceived as alternatives that seem to only be in partial equilibrium or absolute conflict, leaving the equanimity undiscovered yet it exists. It is the conceived lemma of equilibrium that is feasibly not the way it seems, therefore not a lemma at all.

I argue that any lemma is a 'yet-to-be-discovered equilemma' until proven impossible to be in equilibrium. It is basically the disequilibrium challenges facing blockchain technology today.

Firstly, it's important to note that the Trilemma is just a model to conceptualize the various challenges facing blockchain technology. There is no law stating that the three (3) aspects cannot be achieved, so the concept is theoretically flawed. But to date, teams have worked on different approaches in an attempt to maximize decentralization, scalability, and security. I believe that the equilemma may actually be better conceptualized in a hierarchical pyramid, where the base layer is the fundamental layer that upholds all others: And like many others believe, it should be Security. Without security, decentralization may be corrupted and scalability may be short-lived. Security will create the underpinning for both decentralization and scalability to flourish. Decentralization eliminates censorship and



resonates security. Scalability prevents, but security is the key to improving scalability and upholding decentralization, therefore security is uncompromisable.

The blockchain world has long awaited the full-fledged entry of established enterprises into using blockchain technologies, often citing a lack of scalability as the primary hindrance. While a lack of scalability may certainly be a factor, a lack of reliable security would certainly be a heavy contributor to this reluctance, and of course a lack of economic stability is also been what established enterprises always point to as one of the major factors that hinder their adoption of cryptocurrencies, even the public point this out, and therefore none of these should be neglected. Setheum addresses them all, as I have studied that the equilemma is one of the major factors that prevents blockchain technology from reaching mass adoption and economic diversity.

Regardless of the shape of the equilemma, it's agreed upon that it's difficult but not impossible for any blockchain system to effectively achieve decentralization, scalability, and security.

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.

Diaprivacy: Termed "*Differential Auditable Privacy*", is a formal cryptographical framework for guaranteeing privacy protection when auditing, analyzing or releasing statistical data. Diaprivacy is basically the mechanism that ensures the privacy of a subject while allowing it to be auditable. Diaprivacy, also known as "*Zero Knowledge Proof*" will allow users in financial services - for instance (can be applied to any industry) to prove one aspect of compliance without having to reveal the underlying details.

Imagine an investment firm being able to prove that it's taking the correct management fee, without needing to reveal details about it's trades, investments or investor identities, this can be extended to Identity and Reputation Solutions that offer User Data privacy via Selective Disclosure Credentials like Insurance for instance.



Imagine CocaCola being able to prove to regulators that its top secret coke formula is safe and complying to regulations, without having to reveal what the top secret formula is.

Imagine an immigration officer being able to prove if a traveller is a citizen of a banned country or the person themselves being banned or not, without having to know which country he belongs to or for what reason he was individually banned.

Diaprivacy allows you to do statistical analysis without compromising the privacy of the data set. More specifically, it allows you to query a database while making certain guarantees about the privacy of the other records contained within the database. Generally, research policies require researchers to protect privacy as a principle that is fundamental to safeguarding the dignity and welfare of their subjects. Researchers are accordingly responsible for implementing privacy-protective measures and effectively conveying the extent of protection afforded to their subjects.

Imagine you're being able to clear a court case by proving the validity of a will and the truth of a statement on the will without having to reveal the will itself.

Imagine you're being able to prove the structure or compliance of an aggregate without having to reveal the aggregate itself.

Imagine you're being able to truthfully prove why you didn't conform to a subpoena, and the urgency or value of the reason, without revealing what the reason is. That is the job of Diaprivacy.

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 its 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 stable currency on top 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 (SetheumFiscal 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 its 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, ie; 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 propaduction. 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 in , and the 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  **USD(SettUSD)** or  **SAR(SettSAR)**, and can swap that back into the basic  token via the Atomic Shifter Tunnel(to be explained in the next subtopic). These tokens minted by SETT, are called "**Prototokens**", because they 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  **100USD** (100SettUSD) or its equivalent of  **SAR** (SettSAR), or any one of the over one hundred (100) available  prototokens.

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 longrun 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 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.


So when we talked about 'Alice' swapping or minting  **100USD**, 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.

The main purpose of this is to provide the discounts on DApps That use it and, even wallets that are built on it will give users access to this massive reward, where if a user deposits Sett in that wallet Dapp, their account gets some more Sett when the value increases and more sett is minted.



This type of wallet can choose to have a reserve that stakes Dinar, and then distribute the rewards it gets from newly minted Sett to the users as a SignUp bonus or something like that, whatever they wish.

Similarly, Dapps can finally be free of charge for as long as the the DApp has a reserve that stakes and is built on the Setheum network, it can use the rewards of  it receives to pay its transaction fees, so this way DApps can be tested on the mainnet without having to pay from their initial capital. Even ICOs can benefit from this model. This opens up a lot more opportunities than I can actually imagine. And we will support the Developers of Such DApps on the Setheum blockchain. We will create a Blockchain Fund to invest and offer grants to innovative DApps and Blockchains built on the Setheum Network, I personally am interested in the projects i just highlighted, I am willing to share ideas with the most innovative and charismatic developers, game designers, engineers, mathematicians, cryptographers, and students who are planning to propose intelligent projects on the Setheum Network.

Same way, an ecommerce site/platform can harness this beauty of Setheum to attract more users/customers with amazing discounts, the site can even have the type of reserve like that of the wallet I suggest, to direct discounts in whatever manner they wish. And these prototokens are also tradable like all other tokens on the Setheum Network and atomic swap between SettPrototokens and 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  Prototoken, and vice versa. This takes place in a tunnel called the “Atomic Shifter” between the SERP and SettPay in Setheum Finance. So without SettPay, Sett Prototokens will not be minted from SETT, let alone distributed.

Halal Loans Protocol(Zero-Interest Loans on Setheum)

Similarly, Flash loans - called “Halal loans” on Setheum, are available, the reserve allocates a portion of the minted SETT to the “Halal Loans Protocol”. And when contraction is needed, this Halal loans protocol is the first to be visited by the SERP, and then the validators absorb less contraction in the process, if and only if the Halal Loans Protocol has absorbed enough to a limit. The Halal Loans protocol provides what we know as flash loans, and it costs only the transaction fees and a profit of 2.58% allocated to the SettPay protocol for SettPay users. This can be used to trade arbitrage for profit without spending a dime of interest or collateral, just with the transaction fees.. And 2.58% of the profit is deducted, not 2.5% of the total loan, but that of the profit alone, so it's a small fee but when many loans are given, so much profit will be shared to the Setheum Network.

Shards

Every shard in Setheum has an abstract STF (State Transition Function) based on WASM (WebAssembly). Each shard can expose a custom interface, as long as the logic compiles to Wasm and the shard provides an "execute block" function to Setheum validators. Setheum will have a development framework that allows full spectrum composability with a suite of modules that can be configured, composed, and extended to develop a chain's STF.

XCMP(Cross-Chain Message Protocol)



Cross-chain transactions are resolved using a simple queuing mechanism based around a Merkle tree to ensure fidelity. It is the task of the Relay Chain validators to move transactions on the output queue of one parachain into the input queue of the destination parachain.

- Cross-chain messages will *not* go on to the Relay Chain.
- Cross-chain messages will be constrained to a maximum size in bytes.
- Parachains are allowed to block messages from other parachains, in which case the dispatching parachain would be aware of this block.
- Collator nodes are responsible for routing messages between chains.
- Collators produce a list of “output” messages and will receive the “input” messages from other parachains.
- On each block, parachains are expected to route messages from some subset of all other parachains.
- When a collator produces a new block to hand off to a validator, it will collect the latest “input” queue information and process it.
- Validators will check a proof that the new candidate for the next parachain block includes the processing of the expected “input” messages to that parachain.

Code Execution - WASM (WebAssembly)

WebAssembly, shortened to simply *Wasm*, is a binary instruction format for a stack-based virtual machine. Wasm is designed as a portable target for compilation of high-level languages like C/C++/Java/JavaScript/Rust etc., enabling deployment of client and server applications on the web.

We consider Setheum to be the 5th generation of blockchains - focussed on mass adoption and industrial diversity. Entire blockchains can run as applications on Setheum. For this, we need a better virtual machine than the EVM, and especially we need something that is more efficient and diverse.

We chose WebAssembly (Wasm). This is a virtual machine specification that is intended to match the semantics of physical machines in the real world today, making it efficiently executable on modern hardware. It's also built to be easily verifiable, not necessarily for logical correctness but for memory safety.

For example, there are no random `gotos`, you have to specify an actual function to call or block to break out of. It's also intended to have no undefined behaviour. This means you can natively compile the VM code to native code without having to insert expensive runtime checks.

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).

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 parachain's block and test its validity. The random parachain-validator assignments and secondary checks performed by randomly selected validators make it impossible for the small set of validators on each parachain 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 WWII.



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/aVUqXulcpZ4>
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-info-graphic>
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-info-graphic>
17. Differential privacy: an introduction for statistical agencies
https://gss.civilservice.gov.uk/wp-content/uploads/2018/12/12-12-18_FINAL_Privitar_Kobi_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.>