Declaration of Decentralisation

DeFi Infrastructure: A New Economic Design and Consensus Protocol
Built to Empower Decentralized Businesses

Version 1.3

Imagine there are no countries . . .

For those who believe in a fully decentralised financial system without depending on government-issued currencies.

Abstract

On Jan 3rd 2009, Bitcoin set out the journey to create a decentralised financial system without government backed currencies. Today, at more than $115 billion market cap, it has become more like the digital gold reserve than a currency used for medium of exchange and financial unit of account. The volatility of exchange rates between cryptocurrencies from the virtual world with value from the physical world makes the prospect of creating a healthy blockchain economy difficult. The goal of the protocol of Meter is to complete the mission of Bitcoin and create a stateless financial infrastructure to enable the development of the cryptocurrency economy. It is a fully decentralised, permissionless public chain and Meter is the stable cryptocurrency on the chain that provides a relatively stable currency reference to values from the physical world. Meter uses the *cost of production* and the miners' arbitraging behaviour in a proof-of-work system as the key feedback to establish a long-term equilibrium price for the market. Such equilibrium price essentially anchors the unit of accounting in the Meter system to the global competition of electricity prices, which is more stable in real value than any fiat currencies in the world based on the historical data. Meter eliminates the burden on dApps developers to dynamically price their goods or services based on off-chain exchange prices, which is not only difficult to implement properly, but also extremely confusing to customers. The protocol of Meter aims to lay the foundation for a stable cryptocurrency reference that will pave the way for more sophisticated financial services and instruments like lending, insurance, options and derivatives to be built correctly.

Meter is not pegged to the U.S. dollar or any other fiat currency issued by a sovereign country. Instead, it is built on top of its own economy and its proof-of-work interactions with the physical world.

Meter is not competing with Ethereum or other public blockchains, though it is compatible with existing Ethereum dApps and can function as a side chain to most public chains. Developers can interact with and use Meter as a reference for their dApps' native public chains through Meter's cross-chain adaptors and SDKs. Each public chain runs its own consensus and scaling and implements its own incentive schemes while Meter focuses on proper monetary policy, inter-chain communications and settlements of value.

Table of Contents

1. The Problem

After speaking with hundreds of decentralised applications ("dApp") developers that are working on ICO projects and blockchain products, what the Meter team has discovered that their dApps lacked a key requirement to be successful: a stable unit of account representing an established value for dApps and users to use when interacting from the virtual world of cryptocurrency to the physical world of fiat currencies. The exchange rate volatility between cryptocurrencies and fiat makes it unlikely that people will use cryptocurrencies for transactions other than for speculation-related activities.

Take for example a landlord that wants to rent a room at 0.1 Ether per night using a dApp that provides Airbnb-like services. That landlord would not be able to reliably know the value of that 0.1 Ether in terms of a fiat currency and therefore whether renting the room is financially profitable. It may worth $100 per night when the room is posted, $70 when a traveller books the room, and $140 when the traveller later arrives. This kind of exchange rate volatility exposes both buyers and sellers to tremendous amount risk as their costs and incomes are most likely denominated in a fiat currency. Also, note that this landlord is also likely to be competing against other landlords who are renting their rooms but charging in fiat currency. Our landlord will have a harder time in attracting renters since those renters, as buyers, also face the same unit of accounting problem facing our landlord. This problem facing dApps that want to connect to the physical world is confirmed further by looking at the dApps that have achieved some commercial success. Certain dApps, like Crypto Kitties, have found success by targeting cryptocurrency users and limiting user activities to the virtual world, negating the need to connect to the physical world and exchange cryptocurrency to or from fiat currencies.

To create a robust blockchain economy, there is the need for a public blockchain with a native stable cryptocurrency that can offer a unit of account representing an established value in the physical world for all dApps. Converting cryptocurrencies into fiat currencies and vice-versa is essentially an international finance issue between the economies of the physical world with fiat currencies and virtual world with cryptographic virtual currencies.

2. A Currency Needed for the Virtual World

2.1. New Socio-Economic Structures for the Virtual World

Many of our existing socio-economic structures in the physical world were created by the constraints of working within the confines of geographic boundaries. The Internet is breaking down those constraints as people spend an increasing amount of their time online in the virtual world. People in the virtual world are naturally grouping themselves into decentralised communities based on their shared values and their perceived need and acceptance for centralised authorities like governments is weakening. These trends are likely to continue to grow. A well-designed decentralised economy and governance system that befits the virtual world, blockchain technology offers an answer to the needs of these people as its consensus scheme provides a contracting and settlement system without the risk of default. It leverages on game theory principles to form an economic consensus based on man's natural inclination to take actions in self-interest. The virtual world is developing new socio-economic structures and financial systems; cryptocurrencies and ICOs are some of the initial components of this ground-breaking transformation that is underway.

2.2.The Functions of a Currency

In this virtual world, the current blockchain economy lacks a cryptocurrency that functions as a true currency. A currency should perform three main functions, namely, being a: 1. unit of account, 2. medium of exchange, and 3. store of value.[1]

2.2.1. Unit of Account

As a *unit of account, a currency* provides a common measure of value for goods and services being exchanged. Almost all cryptocurrencies have a deflationary model with a fixed supply or limited

[1] https://en.wikipedia.org/wiki/Money

ability to expand its supply. This limitation prevents these cryptocurrencies from scaling with the GDP growth of the blockchain economy. [2]

As an example, Bitcoin is often compared to gold due to their limited supply and similarly high perceived value. Yet, an examination of gold-based (or silver-based) financial systems reveals that those systems collapsed when the underlying economy rapidly expanded and gold could not scale with it. Both gold and Bitcoin will naturally tend to increase in value due to their limited supply but it is also the same reason why neither are suitable for powering an economy.

A deflationary currency ultimately discourages production and fundamentally damages an economy. As an example, imagine you are a baker living in a world of hyper deflation. You purchase ingredients with currency during the day, bake cakes at night, and plan to sell the cakes the next day. Your plans to profit from your labour is thwarted when you discover the next day that the market price of cakes has dropped below the costs you paid for the ingredients. You realise you were better off not doing anything and should have simply held onto your currency. If someone desires to create a stable cryptocurrency that will power the entire blockchain economy, encompassing hundreds of blockchains, thousands of cryptocurrencies, and millions of dApps, products and services, the chosen currency must not be supply-limited and deflationary in nature.

2.2.2. Medium of Exchange

As a *medium of exchange*, a currency enables buyers and sellers to make informed transactional decisions, particularly between dissimilar products or services; buyers and sellers are not limited to bartering for only goods or services that both sides want. The performance and scalability of most of the popular cryptocurrencies are too limited to function as a medium of exchange for the entire blockchain economy.[3] A popular dApp or a major ICO can cripple a blockchain, like what the Ethereum network has experienced many times already. In relation to this, the scalability of major existing cryptocurrencies is further limited by their increasing transaction fees. As a

---

[2] As an example, Bitcoin is often compared to gold due to their limited supply and similarly high perceived value. Yet, an examination of gold-based (or silver-based) financial systems reveals that those systems collapsed when the underlying economy rapidly expanded and gold could not scale with it. Examples of collapses include the Ming Dynasty in China and the more recent Bretton Woods System in the Western world.

[3] Bitcoin can only handle approximately 7 transactions per second, and Ethereum transactions are only slightly better at 15 per second.

cryptocurrency's market price increases, the activity level increases which then produces higher transaction fees. Both the Bitcoin and Ethereum networks have experienced this phenomenon.

2.2.3. Store of Value

As a *store of value*, a currency ensures that the it holds an established value over time.

The concept of *value* is from the physical world based on two competing schools of thought among economists. The labour theory believes that the value of a good depends on the cost of producing it. The subjective theory believes that the value of a good emerges from our belief of the good's usefulness for the particular purpose at a particular point in time. The Meter team believes that these two theories are complementary to each other and necessary to understand how people perceive value: the labour theory's cost of production must be considered, especially in terms of analysing opportunity costs, while through employing the subjective theory, the plans of people for the usage of a good are considered and thereby an opinion on the good's usefulness is formed.

For purposes of creating a stable cryptocurrency, value is more subjective in the virtual world compared to the physical world, since the virtual world defines value from an individual user's perceived utility. For example, virtual goods such as Crypto Kitties, are valued drastically differently by different buyers and sellers. There is no standard established pricing. Therefore, to have an established value that a large group, rather than an individual, can agree upon, a linkage to the physical world to leverage an established value is needed. For this reason, most of the existing proposed cryptocurrency stable coins peg themselves to the physical world's U.S. dollar to establish a standard for their value.

2.3. Bitcoin is Not a Currency for the Virtual World

Bitcoin casts a large shadow over the cryptocurrency world for multiple reasons, but despite it symbolising cryptocurrencies in general, it fails to fully perform all three functions of a currency. It is a store of value, but it does not function well as a unit of account and as a medium of exchange.

Initially there was no perceived value for Bitcoin except for a shared ideology of paying for the consensus cost of transactions in the Bitcoin system. Capping Bitcoin's total supply combined with global instability and prolonged central bank easing policies helped Bitcoin to anchor its perceived value to gold and an almost indestructible representation of value. The price of Bitcoin has taken off ever since.

However, Bitcoin suffers from performance inefficiencies and its price is already orders of magnitude higher than what Satoshi Nakamoto had ever imagined, to the point that the original design no longer works. Bitcoin was designed as a single lane highway with fixed amount of transaction throughput. As more miners have added more mining hardware to earn Bitcoins, the cost of reaching consensus has dramatically increased. To maintain Bitcoin's initial design framework, the price of Bitcoin must continue to rise dramatically or transactions fees must rise to compensate the increased costs of production experienced by miners. In around two years, when the next Bitcoin mining reward is halved, the transaction fees will likely reach hundreds of dollars. This situation will worsen each time the mining reward is again halved. Bitcoin was never designed to be a stable cryptocurrency and its price volatility, performance inefficiencies, and limited supply preclude it from being the currency for the blockchain economy.

2.4. Decentralisation and Trustlessness

In addition to the traditional three functions of a currency, a stable cryptocurrency that will serve as the foundation of the future cryptocurrency economy must also be decentralised and trustless. Despite Bitcoin's weaknesses in terms of functioning as a currency, it excels in removing the need for one to trust a third party. It removes the counterparty risk through its decentralised consensus design. For example, in the physical world, people trust the U.S. government with respect to the U.S. dollar it issues. Implicitly, people must also trust that the U.S. government will not abuse its powers, not over-issue credit, and generally be a good steward of the dollar's monetary policy. That has not been the case always and other governments and their government-issued fiats have suffered problems. Bitcoin introduced the notion of decentralisation and trustless consensus through algorithms and game theory as a replacement to having to trust a third party. The future stable cryptocurrency should likewise be decentralised and trustless to fit in the ethos of blockchain community.

3. Meter and Stable Coins

3.1. Introducing Meter

Meter (**MTR**) is a stable cryptographic virtual currency that functions in all three capacities of a currency, particularly as a unit of account and medium of exchange. Meter creates a stable reference of value for the cryptocurrency world by linking to values from the physical world. It is built on the same decentralised, permissionless, and autonomous principals as Bitcoin and Ethereum but the currency supply is designed to automatically expand or contracts with changes to the underlying economy such as the number of dApps and fluctuations in their usage. Meter's value in effect is neither deflationary nor inflationary in the long run. The Meter team is also planning to instrument several scaling features into the protocol of Meter that will allow major dApps to scale independently without causing transaction congestion on the Meter chain.

3.2. Existing Stable Coin Proposals and Their Problems

There are several proposed stable coins already on the cryptocurrency market or in the pre-release stage, including Tether, MakerDAO, Basecoin, Fragment and a few others. None of these stable coins have a token economy other than being used as a unit of account for cryptocurrency exchanges (i.e., to drive speculation of their stable coin). Some of these stable coins require collateral to stabilise their price and most are centralised. Without exhaustively examining each stable coin, the following portion highlights some of the major characteristics and weaknesses of the existing stable coins.

Collateral-backed stable coins like MakerDAO may be decentralised but require users to front more collateral (for example, in Ethereum) than they obtain in terms of value from the stable coin received. Over-collateralisation reduces volatility but users may think twice about why they are providing more in collateral than they are receiving in the stable coin. Moreover, these stable coins are at risk to the volatility of their underlying collateral cryptocurrency which may lead to a black swan event where the user suffers a liquidation and loses both their stable coins and cryptocurrencies provided as collateral.

Other stable coins are IOU-based and centralised. Tether is such an example. Users must take on counterparty risk and trust that these stable coins are actually backed by fiat currency on a 1:1 basis as the issuing company contends. When potentially trillions of dollars are stake, it is unrealistic to bear such counterparty risk and trust that companies like Tether Limited (the company that creates Tethers) have reserves equal to the number of IOU-based stable coins in the market. Moreover, these stable coins usually prevent the free flow of capital (see below for further explanation).

Another group of stable coins follow a seigniorage shares model. They algorithmically expand and contract the supply of the stable coin much like a central bank does with fiat currencies. These stable coins are not collateralised but it is claimed that they will retain a certain value. Basecoin and Fragment are examples following this model. These stable coins issue bonds to stabilise and increase the price by removing stable coins from the marketplace. They can buy back bonds without restraint to decrease the price. These bond issuances are susceptible to getting priced lower and lower as bond traders are motivated to wait for prices to decrease. However, as price decreases, the number of stable coins removed decreases in inverse proportion, which has a cascading effect that makes removing stable coins from the marketplace more difficult for every bond price reduction.

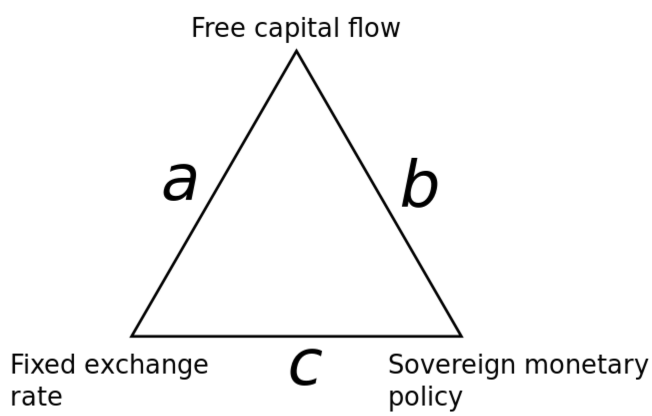
3.3. The Impossible Trinity and Adhering to Fundamental Economic Principles

Similar to the currency exchange rate among different economies in the physical world, the conversion between a stable cryptocurrency and a fiat currency is an international finance problem between two economies: the virtual and physical world. The Meter team therefore believes that compliance with the Impossible Trinity is necessary for a stable cryptocurrency to be successful. In other words, the team does not believe that fundamental economic principles can be ignored in the process creating the mechanics of a stable cryptocurrency.

Besides the noted weaknesses of the existing stable coins already on the market, all of the existing stable coins, other than Tether[4], ignore an important theory of international finance, the *Impossible Trinity*.[5] The *Impossible Trinity* states that a currency policy can only achieve simultaneously two of the following three economic goals and achieving all three simultaneously is impossible:

- Free flow of capital: the movement of capital in and out for trade and investment
- Fixed exchange rate: where the currency value is fixed against the value of another currency
- Independent monetary policy: where the monetary authority independently controls the supply of the relevant currency.

The existing stable coins *peg* to a fiat currency like the U.S. dollar. Pegging achieves a fixed exchange rate, yet those stable coins also claim to offer the free flow of capital and maintain an independent monetary policy[6]. These existing stable coins that believe that their coins can simultaneously achieve all three economic pillars of the Impossible Trinity are making a fundamental mistake of what is actually possible within the realm of international finance.



[4] Tether is an exception to violating the Impossible Trinity since it explicitly forsakes an independent monetary policy by claiming 1:1 ratio of Tethers to US dollars held in reserve. It also restricts the free flow of capital. If Tether Limited received 100 million U.S. dollars in the past and then a sell off of Bitcoin prompted Bitcoin sellers to exchange 200 million U.S. dollars' worth of Bitcoins into Tether, the peg between Tether and U.S. dollar would immediately break. This is why Tether Limited restricts the conversion between Tether and U.S. dollars.

[5] https://en.wikipedia.org/wiki/Impossible_trinity

[6] For example, by issuing bonds to contract or expand the currency supply.

Figure 1: The Impossible Trinity states that only one side of the triangle representing two of the three possible monetary policy goals can be achieved at any given time and successfully implementing all three policies simultaneously is impossible.

3.4. Summary

To summarise to this point, the Meter team has reviewed how a stable cryptocurrency must perform the three functions of a currency. As part of the store of value function, the stable cryptocurrency must be transparently connected to the physical world. Moreover, adopting from the Bitcoin protocol, the stable cryptocurrency must be decentralised and trustless. Finally, the stable cryptocurrency must not violate fundamental economic principles such as the Impossible Trinity without risking its credibility among the cryptocurrency community and those it may interact with from the physical world.

Based on these criteria, the Meter team has concluded that the existing stable coins do not meet the requirements outlined and have designed the protocol of Meter to satisfy all those requirements.

With respect to the three functions of a currency, Meter has an uncapped supply, is neither deflationary nor inflationary, and its relatively stable price design helps it satisfy the *unit of account* and, relatedly, the *store of value* functions. Its infrastructure supporting multiple blockchains enables it to be a *medium of exchange* with high throughput and efficient transaction times. Meter employs a proof-of-work consensus validated main chain that is decentralised among miners doing proof-of-work computations. Therefore, Meter users avoid bearing counterparty risk and are not required to trust a third party for the Meter blockchain to operate. Finally, since Meter is not pegged to at fiat currency, such as the U.S. dollar, it can still offer the free flow of capital and operate an independent monetary policy without violating the Impossible Trinity.

Meter does not peg itself to a fiat currency from the physical world (there is no legal guarantee) and, as mentioned, the market price of Meter should be linked to the physical world[7]. Data produced by our proof-of-work model from the physical world is critical in the determination of the market price of Meter, and hence value, to build community trust and enable the virtual world

[7] As an attribute of how value should be derived by linking back to the physical world's concepts of the cost of production and the perceived utility of the good produced.

to start building a robust cryptocurrency ecosystem. In the next Section 4, the analysis of the design of Meter is explained, starting with the design principles behind Meter.

4. The Meter Design

4.1. Meter's Design Principle

4.1.1. Computing Power Linking the Physical and Virtual Worlds

The Meter team perceives the current blockchain landscape and its need for a stable cryptocurrency to interactions between the physical and virtual worlds. The physical world uses fiat currencies and the virtual world should have a stable cryptocurrency to which thousands of other cryptocurrencies are pegged. The physical world exports computing power to the virtual world to maintain blockchain consensus for that stable cryptocurrency. The virtual world in return exports virtual goods[8] and services to the physical world. The virtual world must have a healthy internal consumption rate (i.e., its own domestic economy) to make its stable cryptocurrency resistant to large fluctuations of export demand (which price changes precipitate during bear or bull markets in the virtual world). Computing power therefore provides a critical link between the physical and virtual worlds and the miners putting the computing power to work are the merchants and traders between these two worlds.

4.1.2. Marginal Cost of Production Tracks the Market Price of Bitcoin

In a proof-of-work system like Bitcoin and Ethereum, that computing power is performed through the process of "mining", in which the cost for the computing power is paid in fiat currencies and the revenue is received in cryptocurrencies. The process and technical review of Bitcoin mining is described in-depth elsewhere (e.g. Kroll Et al. 2013; Sapirshtein et al 2016; Nakamoto 2008). The cost of mining can be divided into a fixed cost in semiconductors and a variable cost in energy consumption. The semiconductor factor also impacts the energy efficiency in mining measured as GigaHash/Second/Watt.[9] On the revenue side, the incentive for mining is the block reward and

[8] Other cryptocurrencies could be considered virtual goods.

[9] For Bitcoin, the hashrate is based on the SHA-256 algorithm, while Ethereum is based on Ethash, which is more memory bandwidth intensive.

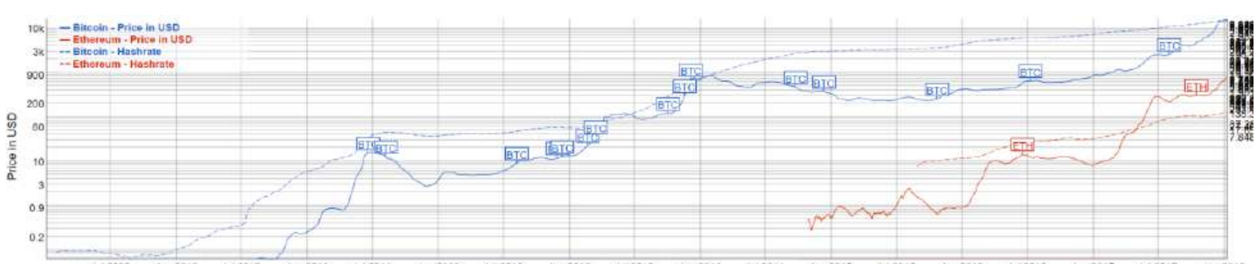
other related transaction fees. Each miner, either independently or collaboratively as a mining pool, is racing to be the first to solve a cryptographic puzzle for a specific block. The miner that first solves the puzzle receives the block reward and puts the block on the blockchain. The incentive to obtain the reward while racing against other miners to solve the puzzle makes mining a highly competitive activity.

The competitive nature of mining drives the activity towards the equilibrium state.[10] Based on microeconomics theory, the equilibrium state in this competitive mining scenario should be:

$$MR = MC$$

The marginal revenue (“MR”) of production should be equal to its marginal cost (“MC”), which should also be equal to the selling price (also known as the *competitive price*).[11] Competition will drive miners, as self-interested actors, to the equilibrium state, resulting in the competitive price, which is otherwise the market price. In the following analysis, Historical data will be used to determine whether the average marginal cost of production for miners is a strongly correlating proxy for the market price.

The cost of electricity constitutes the bulk of the miners’ marginal cost. If the average worldwide electricity rate is estimated as USD $0.135 per KWh[12], the price of Bitcoin and Ethereum should correlate well with their respective electricity consumption rates. Assuming the energy efficacy of mining equipment is relatively stable, energy consumption can be proxied from the blockchain network hash rate. So, the network hash rate proxies energy consumption, which should approximate the marginal cost of mining and the competitive price. The following graph of Bitcoin and Ethereum market prices shows such a correlation to their respective network hash rate:



[10] https://en.wikipedia.org/wiki/Economic_equilibrium
[11] MR = MC also indicates that profit is maximised at peak efficiency.
[12] https://en.wikipedia.org/wiki/Electricity_pricing

Figure 2: This *Bitcoin and Ethereum Price vs Network Hash Rate* chart shows that the network hash rates for Bitcoin and Ethereum correlated with their respective market prices supporting the hypothesis that energy consumption, proxied from the network hash rate, largely approximated the marginal cost and, hence, the competitive price.

Rigorous studies (Hayes 2016, 2017) using Bitcoin network data show that the marginal cost of Bitcoin production can be estimated if the energy cost of mining and the daily mining production are calculated first. The energy cost of mining can be expressed as:

$$E_{day} = (\frac{\rho}{1000})(\frac{\$}{kWh} \cdot W_{per} \cdot GH/s \cdot hr_{day})$$

Where E_{day} is the daily energy cost to mine, ρ is the hash power employed (*GH/s*) by the miner, *$/kWh* is the dollar price per kilowatt-hour, and *Wper GH/s* is the energy efficiency of the hardware and hr_{day} is the number of hours in a day.

The following equation calculates the daily Bitcoin production:

$$\frac{BTC}{Day} = \left((\beta + Tx)\rho \cdot \frac{sec_{hr}}{\delta \cdot 2^{32}}\right) hr_{day}$$

BTC/Day is the expected level of daily Bitcoin production, β is the block reward (currently at 12.5 BTC/block), *Tx* is the average transaction fee/block, ρ is the hashing power employed by a miner, and δ is the difficulty defined in Bitcoin (expressed in units of *GH/block*). The constant $sec_{hr}$is the number of seconds in an hour, $hr_{day}$the number of hours in a day. To maintain a relatively constant block time, δ has to scale with the total Hashing power in the Bitcoin network.

After the daily energy costs to mine and the daily number of Bitcoin mined is calculated, the competitive price for Bitcoin can then be proxied as:

$$P = \frac{E_{day}}{BTC/Day}$$

- P = competitive price
- E_{day}= daily energy cost of mining
- *BTC/Day* = daily Bitcoin produced

After adjusting for the energy efficiency of the network based on the differing efficiency levels of generations of mining hardware and their deployment dates, Hayes 2017 compared the competitive price results from the above formula against Bitcoin's actual market price to derive the following chart:

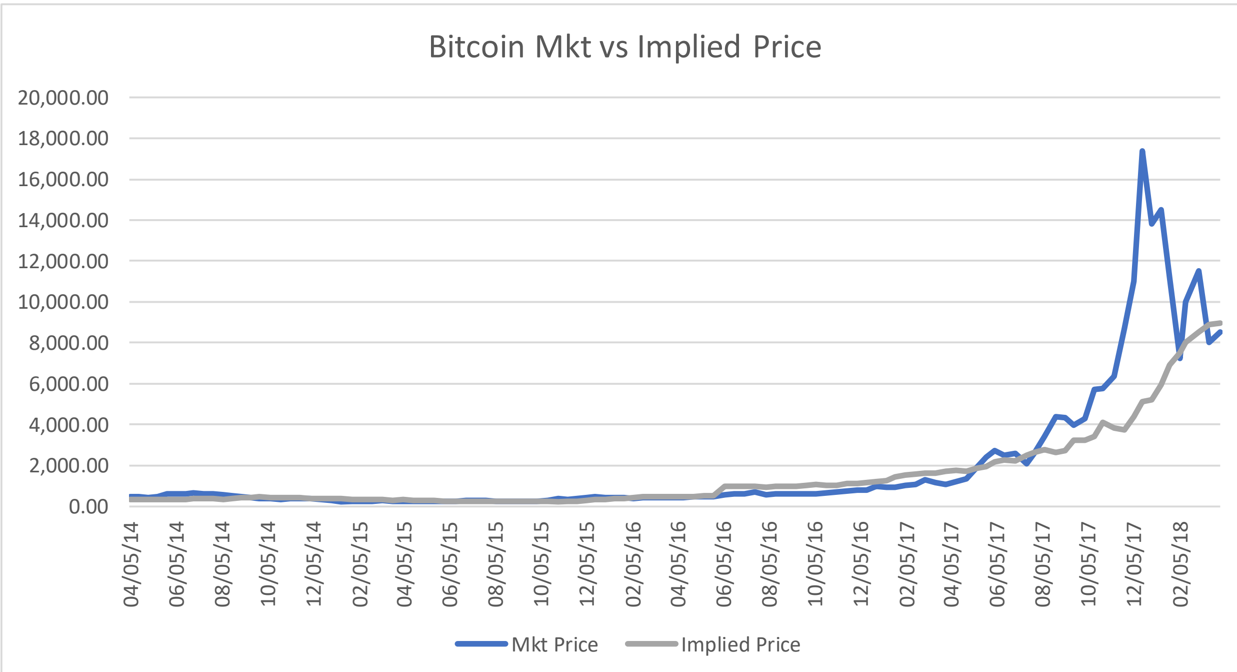


Figure 3: The implied price (i.e., competitive price) based on energy consumed for mining Bitcoins correlated strongly with the actual market price of Bitcoin from Hayes' study.

An ordinary least square regression[13] showed R^2=84.5%, which means that nearly 85% of the Bitcoin market price could be predicted by the competitive price formula (which itself was heavily influenced by Bitcoin's cost of production).[14]

[13] https://en.wikipedia.org/wiki/Ordinary_least_squares

[14] A greater deviation appears after July 2017, which likely reflects the series of Bitcoin forking events that caused market uncertainties in the second half of 2017. These forks likely caused short term misaligned expectations between the market and the miners resulting in the increased deviation.

4.2. A Stable Cryptocurrency with Long Term Equilibrium

It has been shown that it is possible to calculate Bitcoin's competitive price, which tracks closely to its actual market price, by calculating the marginal costs of mining. The protocol of Meter is designed similarly, as a proof-of-work-based cryptocurrency except that the marginal cost of mining should be stable that will tend towards a stable competitive price.

As the energy efficiency improves with the release of better mining hardware, corresponding adjustments will be made to account for those improvements. Moreover, for a relatively long period of time, the marginal cost can be proxied by the total hash rate of the network against the production volume. If the production of cryptocurrency scales with the hash rate of the network, the competitive price for the cryptocurrency should be relatively stable. Miners are profit driven, so if they observe a rise in the price of Meter, they will deploy more computing power to mine Meter. If the price of Meter drops, their margins will shrink and miners may move their computing power to other cryptocurrencies. In both scenarios, whether miners add or stop adding Meters to the market and thereby cause the price to decrease or increase respectively, the invisible hand of the market will keep the Meter price stable. Fundamentally, such a scheme anchors the cost of production for each Meter to the global competitive electricity price. The following chart shows the industrial electricity price in the US, which is among the lowest in the world in the past fifty years. The nominal price (measured in USD cents) went up almost five times while the real price (adjusted for inflation based on the current USD purchasing power) essentially stayed the same. In terms of comparable purchasing power, the electricity price has been more stable than any fiat currencies in the world in the long run.

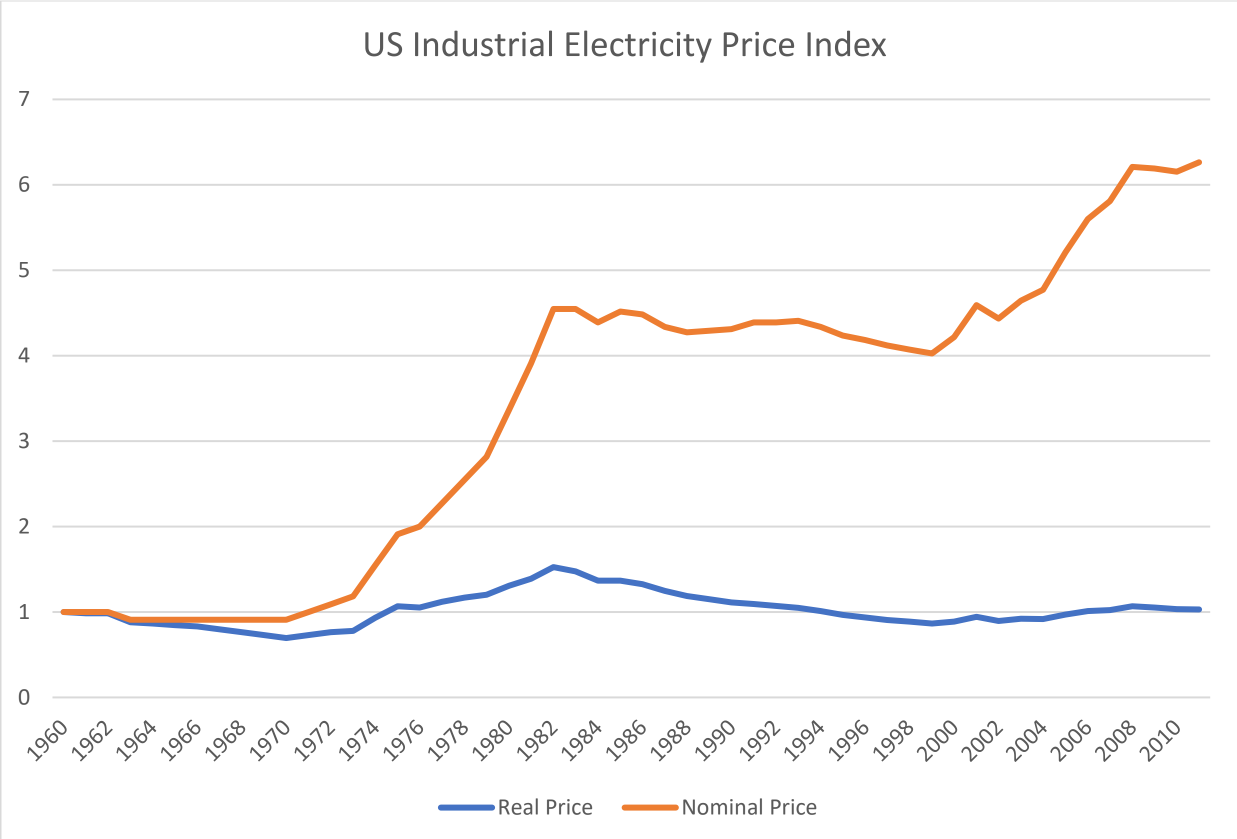


Figure 4: Historical industrial electricity price in the US, which is among the lowest in the world.

4.3 Governance

The Meter team believes that it will be the first to create a real currency in the crypto world with a long-term equilibrium value. However short-term volatilities are expected especially when the Meter economy is still young. Additional monetary policies will be needed to absorb such volatilities. Such monetary policies will require continuously tuning and evolving the protocol. Proper governance mechanics will be one tool to do so and will be crucial for ensuring the community's stability and success. The protocol of Meter therefore is also issuing a separate governance token for the community (**MTRG**). It is planned that for major changes to the monetary policy, MTR production and new features added to the main chain may require voting to be initiated by MTRG (and subject always to prevailing regulatory requirements).[15] Most importantly, MTRG is a key part of Meter's innovative hybrid consensus protocol which makes

[15] In addition, since Meter has a root chain and side chain structure (see Section 4.6), any new proposals could be tested on the side chain first. Once it is fully tested and understood by the community, the changes could be merged to the main chain through a vote.

Meter greener, hundreds time faster than traditional proof of work based blockchains. It also does not suffer the typical problems in proof of stake blockchains like “nothing at stake”, “long range attacks”, and “weak subjectivity”. For the avoidance of doubt, ultimately community members are not connected with the Foundation (or its affiliates) in any manner, and the assets and funds of the Foundation (or its affiliates) remain under the control of the relevant Board of Directors who shall exercise independent judgement and apply them to achieve the Foundation's objects. The right to vote does not entitle MTR or MTRG holders to vote on the operation and management of the Foundation (or its affiliates) or their assets, and does not constitute any equity interest in the Foundation (or its affiliates).

4.4 Proof of Value Consensus with Instant Finality

4.4.1 Proof of Value Consensus is a Proof of Work and Proof of Stake Hybrid System

For a cryptocurrency based on proof of work, the network hash rates can be very unstable. Mining pools have tried to game other proof-of-work cryptocurrencies by causing the network hash rates to fluctuate significantly. Bitcoin Cash, Fedoracoin and other proof-of-work based cryptocurrencies suffered such attacks resulting sometimes in the networks waiting hours or days for the next block to be solved. Most recently, Bitcoin Gold and Verge experienced double spending attacks from hackers who were able to lease and control more than 51% of the hashing power during a few hours window. Based on the information provided by crypto51, it only takes a little over ten thousand dollars to perform a one hour 51% attack to several cryptocurrencies with greater than one billion USD market cap[16]. The Meter system would be particularly vulnerable to such attacks, if it completely relies on proof of work as its security mechanism. The Meter team therefore have introduced a hybrid proof of stake and proof of work consensus. In Meter system, there are miners who are in charge of creating currencies and validators who are in charge of maintaining the public ledger and bookkeeping. The proof of work miners do not directly process transactions but create the necessary randomness and the notion of time in the system to improve decentralisation and resilience to attacks. Such division of work mirrors the physical world where there are miners for gold or silver and bankers for keeping the financial system. They collaborate to make the financial system more stable, secure and scalable.

[16] https://www.crypto51.app/

The stakes for the validators are a combination of MTRG and MTR. The details of the composition will be explained in the monetary policy section.

4.4.2 Proof of Value Consensus Protocol in a Nutshell

The consensus protocol of Meter is a variant of Hotstuff (Yin 2019) and pBFT consensus. The consensus mechanism itself can be paired with any method of Sybil resistance (proof of work or proof of stake) to create an open participation model. In the Meter system, proof of stake is chosen for Sybil resistance for the purpose of providing an additional layer of security as well as checks and balancing in the economic incentive design. It allows users to agree on a log of transactions and achieve the following goals:

Consistency. If a transaction A is confirmed by the protocol, any future transactions confirmed by the protocol will appear in the log that already contains A. This holds even for isolated users that are disconnected from the network (for example, by Eclipse attack).

Liveness. The protocol of Meter should make progress under the assumption that more than 2/3 majority of the participating validators (elected through proof of stakes delegation process) are honest and the network is in "strong synchrony" (meaning that most honest users can send and receive messages from other honest users within a known time bound). It will maintain security when the network is in "weak synchrony" (temporarily overtaken by adversary) until the network is back to synchronous mode.

The consensus protocol is a variant of Byzantine Agreement. On the high level, it consists of the following steps:

1. *Random beacon generation.* Decentralised randomness is the core of a truly decentralised blockchain system. Bitcoin implicitly create the randomness through the global race involving miners searching for the hash solution to the puzzle. Proof of stake systems lack such schemes and have to explicitly create one. For example, Dfinity consensus protocol (Hanke 2018) leverages the BLS signature schemes and Algorand (Gilad 2017) relies on verifiable random functions (VRFs) for generating random numbers, which are used for creating the committees in the later steps.

The proof of work miners in Meter function as the random number generator. They work on a side chain with a purely proof of work basis called the Committee Election Relay (CER). The CER regularly splits and merges with the main chain to trigger the committee re-election and ensures the liveness of the main chain (the period between each split and merge is called an Epoch). The transactions on CER includes the block rewards for each miner (which will be confirmed on the main chain) and the Merkle root of all the transactions on the main chain during the split period. There could potentially be multiple CER forks running among the miners, only the miners on the longest CER confirmed by the next main chain block receive their corresponding block rewards. The block periods on the main chain and CER are different. Initially the block period on the main chain is to be set as 10 seconds, while the CER chain block period set as 2 minutes. Due to the nature of proof of work mining, the block periods on CER follow an exponential distribution. CER and the main chain should have a merge whenever there are more than 30 blocks on CER to trigger a committee re-election and data synchronisation with the main chain. The design choice of 30 blocks is mainly to reduce of the volatility of the committee re-election period and wider distribution of block rewards.

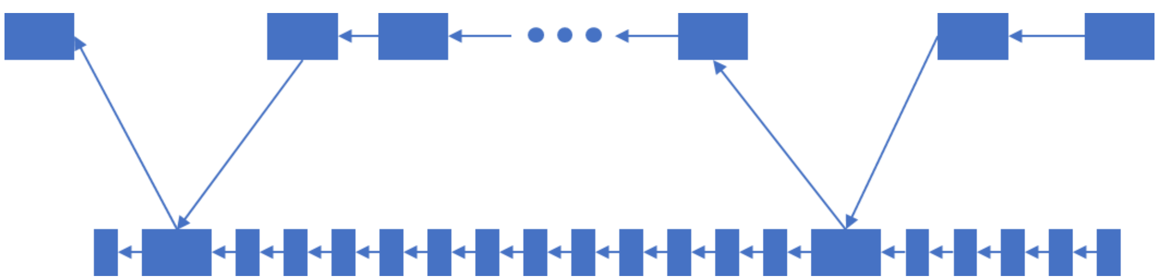


Figure 5: Meter's Proof of Stake and Proof of work chain cross reference each other.

2. *Block proposer committee selection and ranking.* The block proposer committee is elected from the proof of stake delegates pool. Let the individual delegates be labelled 1, 2, … ∈ U. N is the size the of the committee, N<U. When N is large enough (for example a few hundred), the probability for more than 2/3 of the delegates to be honest becomes extremely high. The random beacon β generated from step 1 (based on the longest CER as confirmed by the existing committee) could be used for re-electing part or the entire committee from all the delegates. In the initial phase, when the Meter network is still relatively small, the

committee will likely to be all the qualified delegates of the stake holders. At this stage, the main application for β will be ranking the order of committee for block proposals. β functions as the seed for a cryptographic sort, which ranks committee members from 1 to N. The highest ranked committee member will announce the start of a new Epoch. Delegates can be elected in and out of the committee at the starting of the Epoch.

3. *Block proposal.* Each committee member proposes a new block in rounds based on their ranking order. A valid block proposal B in round r should be:

   $H(B_r) = confirmed(B_{r-1})$ $\quad$ *$confirmed(B_{r-1})$ is the last confirmed block*

   Data in B_r is valid

   Assuming B_{r-1} is confirmed, if the committee member in charge of round r fails to propose a block or obtain confirmation of a block within the BlockTimeOut, the committee member in charge of r+1 will start proposing based on confirmed(B_{r-1}).

4. *Block confirmation.* As soon as a committee member receives a block proposal. It starts signing the proposal and broadcasting the signature. It always listens to signature messages from its peers. As soon as the accumulated signature for B_r reaches >2/3 quorum, Br is confirmed with a confirmation signature confirmed(B_r). Any messages for round r and earlier will be refused once confirmed(B_r)

Such consensus algorithm does not require the network to be in strong synchrony all the time and will survive sovereign grade network attack and partitions. For example, if more than 1/3 of the committee members goes offline due to network partition, the block production will halt. However, the proof of work miners will continue to work in their respective network islands. As soon as the network connection restores, the longest proof of work chain will trigger a committee reshuffle and a new Epoch. The Meter team believes that such behaviour is safer for regular consumers than the random behaviour in the traditional proof of work system like Bitcoin, in which although the transactions seem to be still moving forward and confirmed based on the network islands surrounding a user, they could be completely erased by a longer chain after the network partitions merge back. The Byzantine Agreement style fast consensus scheme ensures short latency (under 5 seconds block time), high throughput (around 1000 transactions per second at launch and scales to billions of transactions per second through sharding, side chain and multi-layer consensus) and instant finality (impossible to fork and reverse transactions by proposing a longer blockchain).

4.4.3 Comparison of Proof of Value Consensus with PoW and PoS Consensus

One of the major criticisms towards consensus protocols based on proof of work is the wastage of energy. It is reported that the electricity consumed by Bitcoin mining each year may amount to more than that of Ireland. [17] Such a wastage of energy was a direct result of Bitcoin's incentive design rather than the proof of work concept itself. As analysed previously, the profit chasing behaviour of miners causes the total network hash rate of Bitcoin to follow Bitcoin's market price closely. As the total reserve for Bitcoin is fixed at 21M Bitcoins. Bitcoin's network hash rate essentially scales with the total market cap of Bitcoin. The higher the market cap of Bitcoin, the more energy Bitcoin wastes to operate and maintain its ledger.

Meter will be the greenest proof of work cryptocurrency as its network hash rate only responds the demand for additional currency in the system rather than the price of the currency. In other words, the network energy consumption scales with the increment of market cap rather than the total market cap of Meter. The Meter team has estimated that with the size and the growth rate of US domestic economy, the annual energy cost for mining Meter will be very similar to the combined annual budget of US Mint and Bureau of Engraving and Printing.

Proof of work typically provides the following benefits to a consensus scheme:

1. Sybil resilience
2. Randomness
3. Notion of time
4. Permissionless to Access Currency

The hybrid consensus of Meter leverages on proof of stake for 1 and still relies on proof of work for the rest. Performance and instant finality wise, it is on par with the most advanced proof of stake consensus algorithm. In addition, it does not suffer from the common flaws in proof of stake systems:

1. The rich become richer. In proof of stake systems, only existing coin holders can participate in mining, the earnings from mining is usually proportional to the amount of coins they hold instead of their efforts in the real world. Therefore, it is difficult the change

[17] https://www.telegraph.co.uk/technology/2018/05/18/bitcoin-now-uses-much-electricity-ireland-energy-demands-not/

the wealth distribution. In Meter system, mining is completely permissionless. You do not have to hold a single coin to start mining on the CER chain and obtaining MTR. The proof of stake validators will be mainly supported by transaction fees and a small portion of their mining incentives from the Reserve (Reserve will be explained in later sections) in Meter, and occasional dilution of MTRG. In order to receive more MTR in the system of Meter, the best way is to participate in mining.

2. Nothing at Stake. Voting on a particular version of a proof of stake blockchain requires no resources and therefore has no opportunity costs. Unlike Proof of Work, where miners must choose which chain to point their mining power at, to the exclusion of other chains, proof of stake validators can stake their coins on every version of a Proof of Stake blockchain that exists to maximise the amount of mining returns. The instant finality design in the Byzantine Agreement consensus of Meter does not allow forking as long as no more than 2/3 of the validators are adversaries.
3. Long range attack. The original, small group of stakeholders can collude to go back and 'revive' an early version of the chain with a completely new history of transaction records. In the protocol of Meter, the Proof of Work based CER chain introduces the notation of time in the protocol. The Merkle root of all the transactions in each Epoch is recorded in the CER chain. To recreate the chain not only requires more than 2/3 of the staking token delegates but also recreating the entire CER chain history, which fundamentally takes the same amount of the time as creating the original chain. In addition, the new chain would not contain the same amount of Meters (or wealth) as the original chain.
4. Weak Subjectivity. When a node joins the network the first time, it has to rely on a trusted source to find out the hash of the valid chain, which completely undermines the trustless nature of a public blockchain. In the system of Meter, the node simply looks for the longest CER chain, which contains the information of the active committee.

In summary, by combining the benefits of both proof of work and proof of stake, the consensus protocol of Meter is green, high performance yet secure and permissionless.

4.4.4 Meter token

The native digital cryptographically-secured utility token of Meter (**MTR**) is a major component of the ecosystem, and is designed to be used solely as the primary token on the network.

Fundamentally, MTR comprises a chain of digital signatures on the Meter blockchain. The cryptographic protocol of Meter enables an owner of MTR to transfer ownership of MTR to another by digitally signing a hash of the previous transaction, and adding these to the end of the chain of digital signatures. A payee may verify the signatures to verify the chain of ownership.

MTR is a non-refundable functional utility token which will be used as the unit of exchange between participants on Meter. The goal of introducing MTR is to provide a convenient and secure mode of payment and settlement between participants who interact within the ecosystem on Meter. MTR does not in any way represent any shareholding, participation, right, title, or interest in the Foundation, the Distributor its affiliates, or any other company, enterprise or undertaking, nor will MTR entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Singapore or any relevant jurisdiction. MTR may only be utilised on Meter, and ownership of MTR carries no rights, express or implied, other than the right to use MTR as a means to enable usage of and interaction with Meter.

As discussed herein, the validation and verification of additional blocks / information on the blockchain would require computing services and resources, thus providers of these services / resources would require payment for the consumption of these resources (i.e. "mining" on the Meter network) to maintain network integrity, and MTR will be used as the economic incentive to encourage the provision of these computing resources. MTR is an integral and indispensable part of Meter, because without MTR, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the entire ecosystem on Meter. Users of Meter and/or holders of MTR which did not actively participate will not receive any MTR incentives.

In particular, you understand and accept that MTR:

(a) is non-refundable and cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by the Foundation, the Distributor or any affiliate;

(b) does not represent or confer on the token holder any right of any form with respect to the Foundation, the Distributor (or any of its affiliates), or its revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property), or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to Meter, the Foundation, the Distributor and/or their service providers;

(c) is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;

(d) is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument or any other kind of financial instrument or investment;

(e) is not a loan to the Foundation, the Distributor or any of its affiliates, is not intended to represent a debt owed by the Foundation, the Distributor or any of its affiliates, and there is no expectation of profit; and

(f) does not provide the token holder with any ownership or other interest in the Foundation, the Distributor or any of its affiliates.

To the extent a secondary market or exchange for trading MTR does develop, it would be run and operated wholly independently of the Company (or its affiliates), the sale of MTR and Meter. The Company will not create such secondary markets nor will it act as an exchange for MTR.

4.4.5 Governance token

The governance token on Meter (**MTRG**) is the main staking token to qualify as a validator for maintaining the blockchain ledger. It is also used to gather proposals and votes for major changes to the monetary policy. New features or changes to the main chain may require voting to be initiated by MTRG (and subject always to prevailing regulatory requirements).

MTRG cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by the Company or any affiliate, does not represent any shareholding, participation, right, title, or interest in the Company or any other company, enterprise or undertaking, is not for speculative investment, and (although MTRG may eventually be traded on virtual currency exchanges), there is no guarantee or representation of value or liquidity for MTRG, is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument or any other kind of financial instrument or investment, and MTRG is not intended to constitute securities in Singapore or any relevant jurisdiction, and will not entitle token holders to any promise of dividends, revenue, fees, profits or investment returns.

To the extent a secondary market or exchange for trading MTRG does develop, it would be run and operated wholly independently of the Company (or its affiliates), any sale of MTRG and Meter. The Company will not create such secondary markets nor will it act as an exchange for MTRG.

4.5 Monetary Policy

4.5.1 Minor Price Fluctuations and Block Rewards

There will be price fluctuations in the market due to short term supply and demand misalignment. When this occurs, miners, who are profit driven, will move more mining equipment to the network when the market price of MTR goes up and remove mining equipment when the market price goes down. Their actions will cause the Meter block reward to elastically change in response, which will bring the price back to its equilibrium or competitive state. During normal conditions, block rewards should be the main revenue source for miners and income from transaction fees should be minimal. During a significant prolonged downward price movement, the value of block rewards towards miners may become negligible. Transaction fees will be the main source of income for supporting the network and they are likely to go up. Facing similar conditions to being in an inflationary environment, the ecosystem of Meter would experience an increase in labour costs.

4.5.2 Large Price Fluctuations and Monetary Policy Intervention

The protocol of Meter does not have a centralised government, but it retains the concept of possessing a *reserve* to absorb any significant shocks to Meter's price stability ("Reserve"). The Reserve is a stream of future income which could be used to attract currency holders to exchange the liquidity of Meter. In the consensus protocol of Meter, a portion of the MTRG auction proceeds and all of the transaction fees go first to the reserve and then to the block validators. MTRG is typically used as the tokens for proof of stake purposes. However, when the system has to reduce the circulation of Meter, it will start allowing Meter to be used as stakes as well. A portion of the block reward goes to the Meter stakes and the rest goes to the MTRG stakes. By adjusting the ratio of Meter and governance reward ratio, the system will use the market forces to remove different amount of MTR from circulation. The exact amount of MTR put into the staking process is completely decided by the market.

In the protocol of Meter, the block validators essentially function as commercial banks, while the Reserve managed through MTRG functions as the central bank. The central bank impacts the monetary system by adjusting the interest rate.

4.6 Bootstrapping the Meter System

The MTR is the basic currency and unit of account for the Meter financial system. All the transactions fees, gas for computations have to be measured and paid by MTR. One of the most important use of the MTR token when the network launches, will be to obtain the governance token MTRG to participating in safeguarding and growing the Meter system. The system will automatically generate Dutch auctions for the MTRG tokens based on predetermined intervals (daily as an example). The only way to participate the auction is to use MTR as the bidding currency. At the end of the Dutch auctions, all the participants in the time period would receive the same price for MTRG. Majority of the MTR tokens from the auction proceeds will be saved into the Reserve while a portion will be allocated to the validators and the future growth of the Meter ecosystem. In the future, we will implement features to allow MTRG token holders borrowing from their pro rata shares of MTR tokens from Reserve.

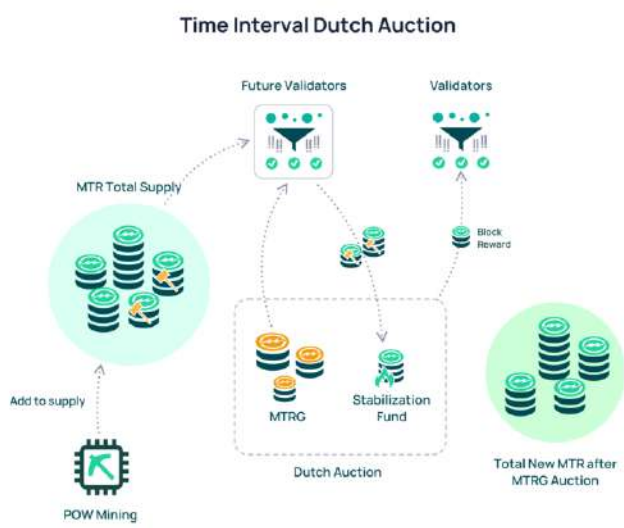


Figure 6: Meter's side chain / parallel chain architecture ensures scalability and throughput efficiency to power the entire cryptocurrency economy.

4.7 Meter Protocol's Cross Chain Architecture

Meter is designed as a fully open system with a main chain, side chain, and parallel chain architecture. The main chain uses proof-of-work to support the Meter stable virtual currency, monetary policy and transaction settlement records. It also serves the medium for inter-chain communications. The side chains originate from the main chain but can join the main chain's consensus or have their own independent consensus mechanism. The Meter team is actively researching the compatibility of major initiatives from other public chains, such as sharding, with the monetary policy of Meter. Additionally, high-performance consensus protocols like delegated proof-of-stake, direct acylic graph, parallel chains and other features can be implemented on side chains to increase transaction throughput or usher in more complicated services like storage and software-defined networks.

Although Meter is a public chain, it is not intended to compete with Ethereum and other public chains. Instead, it provides a stable financial system to these public chains through Meter's parallel chain infrastructure. A parallel chain is a completely independent blockchain that communicates with Meter through inter-chain communications. The Meter team is currently building connectors and SDKs for Ethereum, EOS, Bitcoin and other major public chains to facilitate such communications. From these public chain's perspective, Meter essentially functions as a layer 2 side chain to them.

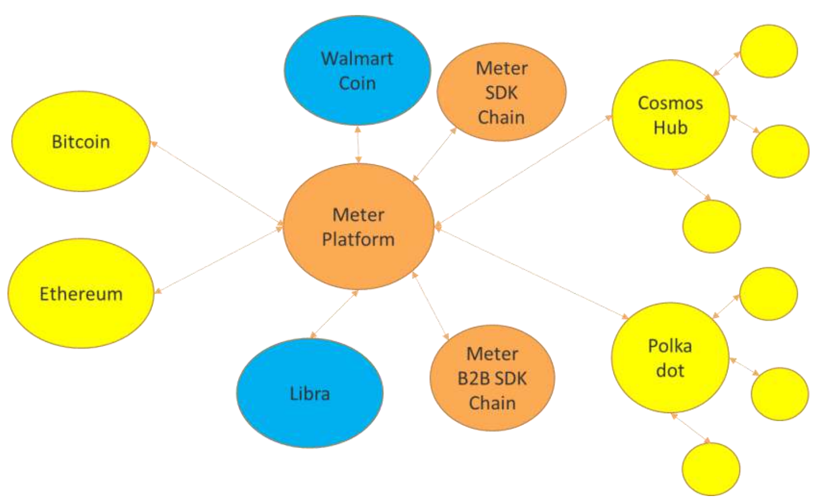


Figure 7: Meter functions as layer 2 for other public chains to connect different value silos in crypto

For example, a dApp developer building a payment service like Paypal or Venmo on a high-performance side chain could issue a payment token that is pegged to Meter and also offer a staking token -- a native token for the dApp that is used for purposes[18] other than those related to payment. Therefore, completely different token economies, incentive matrixes and development road maps can be maintained on side chains (and parallel chains). In this example, every dApp payment token is backed by MTR in a smart contract, with the protocol of Meter providing the interface and final settlement for the dApp payment token when pegged to MTR.[19]

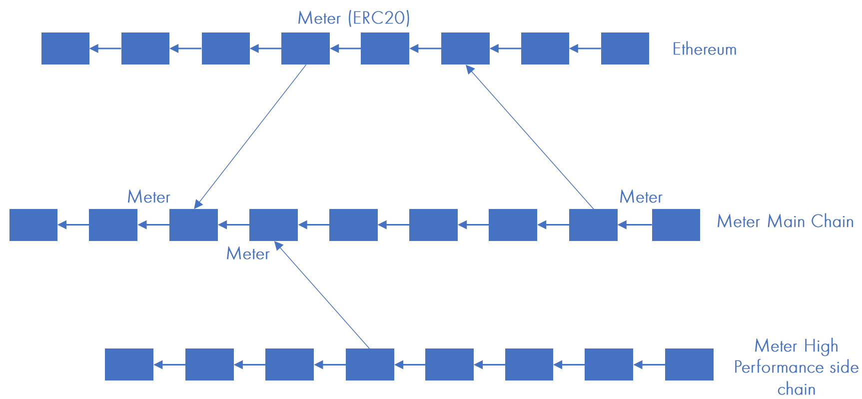


Figure 8: Meter's side chain / parallel chain architecture ensures scalability and throughput efficiency to power the entire cryptocurrency economy.

4.8 Meter at Launch Will be Ready to Power Ethereum

The Meter virtual machine ("VM") is fully compatible with the Ethereum VM and the Ethereum developer tools and ecosystem can be easily migrated to Meter. In addition, adaptors will be provided for the easy transfer of Ethereum and ERC20 tokens between the Meter main chain and Ethereum.

5 Conclusion

The Meter team introduced Meter, a proof-of-work-based stable cryptocurrency with its value fundamentally linked to values in the physical world. Proof-of-work is the fairest method for

[18] Those other purposes could include building a ranking system for reputation, trust, popularity, helpfulness, etc., or other behaviors that the dApp wants to encourage among its users.
[19] The Meter team plans to first support Ethereum VM (EVM).

mining new cryptocurrencies and the most secure way to protect a fully decentralised, permission-less public blockchain.

The historical data of Bitcoin was reviewed to show that its value could be proxied from the marginal cost of production. Meter similarly uses energy consumption from the physical world as a unit of account to reliably proxy its market price. It provides a relatively stable unit of account for the cryptocurrency economy and reduces the extremely volatile exchange rates that dApp developers to date have had to face. The protocol of Meter further absorbs short term supply demand volatility by continuously removing MTR tokens from circulation through MTRG token auctions. Although a stable value is a necessary requirement for developers, they are free to leverage other public chains for performance, development environment, eco-system, and other considerations. Meter provides cross chain communication and value transfer mechanisms to help developers anchor their currency with the stable value in Meter across multiple public chains. Meter is a decentralised financial infrastructure for connecting values not only among different blockchains in the virtual world, but also with the physical world. People must be able to use cryptocurrencies to transact with the physical world's good and services to build a larger thriving cryptocurrency economy.

6 Risks

You acknowledge and agree that there are numerous risks associated with purchasing MTR, holding MTR, and using MTR for participation in Meter. In the worst scenario, this could lead to the loss of all or part of the MTR which had been purchased. **IF YOU DECIDE TO PURCHASE MTR, YOU EXPRESSLY ACKNOWLEDGE, ACCEPT AND ASSUME THE FOLLOWING RISKS:**

6.1 Uncertain Regulations and Enforcement Actions

The regulatory status of MTR and distributed ledger technology is unclear or unsettled in many jurisdictions. The regulation of virtual currencies has become a primary target of regulation in all major countries in the world. It is impossible to predict how, when or whether regulatory agencies may apply existing regulations or create new regulations with respect to such technology and its applications, including MTR and/or Meter. Regulatory actions could negatively impact MTR and/or Meter in various ways. The Foundation, the Distributor (or its affiliates) may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. After consulting with a wide range of legal advisors and continuous analysis of the development and legal structure of virtual currencies, a cautious approach will be applied towards the sale of MTR. Therefore, for the token sale, the sale strategy may be constantly adjusted in order to avoid relevant legal risks as much as possible. For the token sale, the Foundation and the Distributor are working with Tzedek Law LLC, a boutique corporate law firm in Singapore with a good reputation in the blockchain space.

6.2 Inadequate disclosure of information

As at the date hereof, Meter is still under development and its design concepts, consensus mechanisms, algorithms, codes, and other technical details and parameters may be constantly and frequently updated and changed. Although this white paper contains the most current information relating to Meter, it is not absolutely complete and may still be adjusted and updated by the Meter team from time to time. The Meter team has no ability and obligation to keep holders of MTR informed of every detail (including development progress and expected milestones) regarding the project to develop Meter, hence insufficient information disclosure is inevitable and reasonable.

6.3 Failure to develop

There is the risk that the development of Meter will not be executed or implemented as planned, for a variety of reasons, including without limitation the event of a decline in the prices of any digital asset, virtual currency or MTR, unforeseen technical difficulties, and shortage of development funds for activities.

6.4 Security weaknesses

Hackers or other malicious groups or organisations may attempt to interfere with MTR and/or Meter in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or a member of the Foundation, the Distributor or its affiliates may intentionally or unintentionally introduce weaknesses into the core infrastructure of MTR and/or Meter, which could negatively affect MTR and/or Meter.

Further, the future of cryptography and security innovations are highly unpredictable and advances in cryptography, or technical advances (including without limitation development of quantum computing), could present unknown risks to MTR and/or Meter by rendering ineffective the cryptographic consensus mechanism that underpins that blockchain protocol.

6.5 Other risks

In addition, the potential risks briefly mentioned above are not exhaustive and there are other risks (as more particularly set out in the Terms and Conditions) associated with your purchase, holding and use of MTR, including those that the Foundation or the Distributor cannot anticipate. Such risks may further materialise as unanticipated variations or combinations of the aforementioned risks. You should conduct full due diligence on the Foundation, the Distributor, its affiliates and the Meter team, as well as understand the overall framework, mission and vision for Meter prior to purchasing MTR.

7 References

Nakamoto, Satoshi, 2008. Bitcoin: a peer-to-peer electronic cash system.

Kroll, J.A et al, 2013. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries, Proceedings of WEIS

Sapirshtein A. et al, 2016. Optimal Selfish Ming Strategies in Bitcoin. International Conference on Financial Cryptography and Data Security (pp. 515-532)

Hayes AS. 2016. Cryptocurrency Value Formation: An Empirical Study Leading to a Cost of Production Model for Valuing Bitcoin. Telematics and Informatics 2016 May 13

Hayes AS. 2017. Bitcoin Price and Its Marginal Cost of Production: Support for a Fundamental Value

Hanke T 2018. Dfinity Technology Overview Series Consensus System Rev .1

Yossi G 2017 Algorand: Scaling Byzantine Agreements for Cryptocurrencies

Castro M 1999 Practical Byzantine Fault Tolerance

Yin M 2019 HotStuff: BFT Consensus in the Lens of Blockchain

* Special thanks to Maofan Yin and Kevin Sekniqi who provided numerous feedbacks and support for implementing the Meter Hybrid consensus.