MOVING TOWARDS INFINITY

INTRODUCTION

Cryptocurrencies have emerged as the latest brave market in the trading world. These trading markets are relatively young and thus full exploitation has not yet been achieved. The fact that some coins like Bitcoin can rise by 10% in a single day signifies the need for other stable coins to join the market. The tender age cryptocurrency in the trading world has prevented the established trading houses and only left the young companies to invest. Some years back, the market capitalization for cryptocurrency stood at $80 bn and still growing. This further signifies the availability of opportunities for young traders to venture in the market and make profit.

Bitcoin “pioneer of cryptocurrencies” has shown currency can exist outside of the current financial system. It is technologically resistant to counterfeiting via blockchain technology. However, this by itself is not inherently strong enough to spark a technological payments revolution. Rather, bitcoin is exciting and motivating entrepreneurs to build a better mousetrap.

One challenge is that bitcoin is extremely volatile and scares away many would-be users due to the fact it is accepted almost nowhere, including brick and mortar businesses and online. Financial institutions, for the most part, avoid bitcoin.

They are creating private blockchains to identify sources of funds as well as users on these systems.

WHAT IS MTI COIN

MTI coin is a 3rd generation cryptocurrency that provides secure, private, lightning fast payments and pays the user for owning it! MTI Coin is specifically designed and engineered to solve all these problems.

The fundamental principles of MTI include:

DECENTRALIZATION

MTI is owned and controlled by the people. The public ledger or “blockchain” is a decentralized, distributed ledger stored collectively on millions of computers worldwide and is governed by consensus algorithms, math and the people, not by governments, financial institutions or central banks.

PRIVACY

The consumer’s identity is as anonymous as they want it to be. The blockchain contains only cryptic numbers known as addresses for the sender and receiver of each transaction.

UNLIMITED USE

MTI can be sent immediately to and from anyone, anywhere, anytime, for anything, in any amount, with little or no fees.

CONTROLLED SUPPLY

No one can change the predetermined and published circulation schedule of a MTI. The government cannot arbitrarily create more cryptocurrency out of thin air and devalue it. MTI have many of the same characteristics as the precious metals that were once used to back a currency. They work because of their controlled and limited supply.

TRANSPARENCY

Everything is public. All technical specifications, whitepapers and source code files are published for the public to see. All cryptocurrency transactions are recorded in the blockchain for everyone to see with a publicly provided blockchain explorer.

VISION

We aim to build a future digital oriented system that is entirely focused on template developers and consumers. Through our decentralized design, we will eventually exchange rights with the general public, allowing the entire system to grow and reproduce in a sustainable way to achieve an ultimate virtual social formation without a self-centered growth.

ROAD MAP

Q3 2017

Beginning of MTI platform starts from the creation of cryptocurrency ideas and its prime functionalities. Implement to add value through these ideas.

Q4 2017

Researching and developing,Testing our hypothesis and the practicality of making it a reality.

Q1 2018

Blockchain development and release, finalization of whitepaper, Website, Listing in MNRank, Masternodes.online, Masternodes.pro. MAC, Windows and Linux Wallets release.

Q2 2018

Listing on exchanges such as Crypto-Bridge, Graviex, and CoinExchange. Android and IOS Wallet release. Will start working towards the acceptance of Accept MTI coin as a currency.

Q3 2018

Accepting MTI coin as trading currency in the Template market with a minimum of 10 online Stores.

Q4 2018

Listing in exchanges such as Cryptopia and KuCoin.
Launching “MTI Templates” website which accepts MTI as a payment for goods.

WHAT IS MTI TEMPLATE WEBSITE? TEMPLATES?

MTI Template Website is an online marketplace for digital services which will operate a group of digital marketplaces that will sell creative assets for web designers, including themes, graphics, video, audio, photography, and 3D models.

SPECIFICATIONS

Coin Name MTI Coin
Ticker MTI
Coin Type POW/POS/MN
Hashing Algorithm lyra2rev2
Block Time 150 Sec
Max Supply 72,000,000 (72 M)
Premine Coin 3,528,000 (3.528 M - 4.9% of Total)
Minimum Stake 6 Hr
Difficulty retargeting Dark Gravity wave
Instantx 5000 Coin
Last PoW Block 3,60,000
First PoS Block 201 Block
PoS Block Reward 50 Coin (reduce 18% year)
Block Size 3 MB
Coin Maturity 113 Block
MN Payment 15000 Coin

DARK GRAVITY WAVE

Dark Gravity Wave is employed by MTI from the start as a method of retargeting PoW difficulty. It uses a simple moving average that can respond to large nethash increases or drop-offs in just a few blocks. This alleviates the “stuck block effect” often caused by multipools and prevents one person adding a substantial amount of computing power from instantly solving more than a few blocks.

DARKSEND

Darksend is an improved and extended version of the CoinJoin. In addition to the core concept of CoinJoin, we employ a series of improvements such as decentralization, strong anonymity by using a chaining approach, denominations and passive aheadoftime mixing. The greatest challenge when improving privacy and fungibility of a cryptocurrency is doing it in a way that does not obscure the entire blockchain. In Bitcoin based crypto currencies, one can tell which outputs are unspent and which are not, commonly called UTXO, which stands for unspent transaction output. This results in a public ledger that allows any user to act as guarantor of the integrity of transactions.

The Bitcoin protocol is designed to function without the participation of trusted counterparties, in their absence, it is

critical that auditing capabilities remain readily accessible to the users through the public blockchain. Our goal is to improve privacy and fungibility without losing these key elements that we believe make a successful currency. By having a decentralized mixing service within the currency we gain the ability to keep the currency itself perfectly fungible. Fungibility is an attribute of money, that dictates that all units of a currency should remain equal.

When you receive money within a currency, it shouldn't come with any history from the previous users of the currency or the users should have an easy way to disassociate themselves from that history, thus keeping all coins equal. At the same time, any user should be able to act as an auditor to guarantee the financial integrity of the public ledger without compromising others privacy. To improve the fungibility and keep the integrity of the public blockchain, we propose using an aheadoftime decentralized trustless mixing strategy. To be effective at keeping the currency fungible, this service is directly built into the currency, easy to use and safe for the average user.

CONSENSUS

POW

The PoW consensus mechanism, as designed by Satoshi Nakamoto, is currently the soundest method of blockchain security. It solves the Double Spend problem and creates a secure network, capable of transferring financial value. Furthermore, competition among miners and The Longest Chain Rule create fairness on the blockchain. The Longest Chain Rule provides a high level of defense against two of the most dangerous methods of blockchain destruction—The 51% Attack and The Genesis Attack—assuming a strong overall hash rate on the network.

New PoW blockchains can opt to compete directly with Bitcoin's hash rate, and some level of competition is good for the ethical values and innovative power of the cryptocurrency industry. However, it is not necessary, cost-effective, nor eco-friendly that every new blockchain innovation requiring security should attempt to compete directly with Bitcoin. Not only is this unsustainable, but it is also unreliable, as it depends on the arbitrary choices of the decentralized network of miners around the world.

Algorhytm - Lyra2rev2

Lyra was a password-based system that used cryptographic algorithms to decode a sequential system. This is also referred

to as a key derivation function or KDF. It was the creation a group of students from Escola Politecnica da Universidade de Sao Paulo. Lyra was great but then Lyra2 came into existence. The same group from Escola Politecnica da Universidade de Sao Paulo later came up with an improvement on the old system. This program was pretty similar to its predecessor on the surface. Again this was a PHS with cryptographic functions that were also purely sequential in style.

It is an impressive design that creates a pseudorandom output for key encryption algorithms or an authentication string. The memory is a matrix; that stays intact through the entire password hashing process. This matrix came about through the operations of the sponge and remains sequential, never resetting to zero.

Lyra2 saw its release as a public domain option with two extensions: Lyra2-Δ and Lyra2p. The former gives users greater control over the use of the algorithm's bandwidth. The latter opens up parallelism capabilities on the user's platform, something not possible with the first Lyra model.

Despite This, The New Lyra Model Had Some Strength Over The Previous Version The original Lyra model was a great example of key encryption algorithms. The idea of this sequential system, rather than one that could be easily paralleled, was that it was much safer. Hackers with the

toughest custom hardware and multiple processing cores couldn't get through this model.

The system was tough, smart and complex. However, there was the benefit of ease-of-use, as it was easy to bring into an existing system. Another important benefit of this system was the fact that it offered a higher memory usage.

The advantage here is that increases the cost of attacks without increasing the processing time. There was a lot to love with Lyra. However, even the best model can be significantly bettered.

Lyra2REv2" (RE – Reduced Efficiency), a NIST5 based chained algorithm with customizable parameters useful for thwarting future ASIC (Application Specific Integrated Circuit) threats.

Lyra2RE is a chained algorithm consisting of five different hash functions: Keccak, Skein, Groestl, Blake and Lyra2. Lyra2 (nRows=8, nCols=8, TimeCost=1) Keccak-256 Blake-256 Groestl-256 Skein-256

Leveraging industry proven hashing algorithms, we were able to create the most secure, robust, enduring chained algorithm to date that is both easier on GPUs and resistant to ASICs. At this time we have decided not to implement an "N factor" schedule as it is nearly impossible to predict the

future. However, Lyra2RE will give us the flexibility to make changes whenever that becomes necessary. Due to the chained nature of the algorithm, GPU miners will be inherently hard to optimize, meaning that power draw and heat can be reduced. This has been a desired feature for some time with Scrypt-N coins seeing dropping hashrates due to high energy consumption. Lyra2 is strictly sequential in nature, using a "cryptographic sponge" at its core. This means that parallelization of the algorithm will be practically impossible with each step relying on the previous step having already been computed. Unlike Scrypt-N, time cost and memory cost are separated, giving us independent control over both parameters.

ASICs have been far easier to develop for Scrypt-N than they will be for Lyra2RE because increasing the N-factor of Scrypt simply involves doing more iterations of the algorithm.

Under Lyra2, whilst increasing the time cost only involves more iteration, increasing the memory requirement means that any potential ASIC device would have to physically be designed with more memory for each thread. In the future, if ASICs ever were developed for Lyra2RE, we would simply have to fork to a higher memory requirement and those ASICs would no longer properly function. Many crypto-currencies claim to have ASIC-resistant algorithms, but many of them are only so because no ASIC has been made for them yet. As

we see recent Monero example. By contrast, Lyra2RE aims to be ASIC-resistant at heart, allowing for less disruption to miners in the future due to our ability to change algorithm parameters rather than change algorithm all together. It will also free up development time to focus on new features without having to worry about constantly implementing new algorithms every time there is an ASIC threat.

POS

The proof of stake was created as an alternative to the proof of work (PoW), to tackle inherent issues in the latter. When a transaction is initiated, the transaction data is fitted into a block with a maximum capacity of 1 megabyte, and then duplicated across multiple computers or nodes on the network.

The nodes are the administrative body of the blockchain and verify the legitimacy of the transactions in each block. To carry out the verification step, the nodes or miners would need to solve a computational puzzle, known as the proof of work problem. The first miner to decrypt each block transaction problem gets rewarded with coin. Once a block of transactions has been verified, it is added to the blockchain, a public transparent ledger.

Mining requires a great deal of computing power to run different cryptographic calculations to unlock the

computational challenges. The computing power translates into a high amount of electricity and power needed for the proof of work. In 2015, it was estimated that one Bitcoin transaction required the amount of electricity needed to power up 1.57 American households per day. To foot the electricity bill, miners would usually sell their awarded coins for fiat money, which would lead to a downward movement in the price of the cryptocurrency.

The proof of stake (PoS) seeks to address this issue by attributing mining power to the proportion of coins held by a miner. This way, instead of utilizing energy to answer PoW puzzles, a PoS miner is limited to mining a percentage of transactions that is reflective of his or her ownership stake. For instance, a miner who owns 3% of the Bitcoin available can theoretically mine only 3% of the blocks.

MASTERNODE

Masternodes are computers that run a wallet 24 hours a day, keeping the network steady and secure by locking transactions with InstantSend, coordinating mixing of coins, and voting on budget funding. Masternodes are owned by different people in MTI Coin's community and they only require a 15000 MTI Coin collateral, a dedicated IP address, and continuous uptime. Masternode owners get half of the block reward distributed in a fair random manner between all the active masternodes.

Investing in Masternode coins gives you the ability of not only being an investor, but part of the decision makers in shaping the coin advancement. Owning own gives a voice to an investor and makes it more than just money. This is done through submitting proposals.

The foundation of Masternodes is stable and has long term values at the core of the infrastructure.The founding investors have committed their money for a long term making it stable and increases trust among investors. Investors get capital gains by just running the Masternode services.

On top of that, investors are paid in that coin as rewards from each block found. The availability of a stronger community guarantees the long-term sustainability of the crypto project.

This in turn ensures that energy is focused on the project's long-term future instead of pump and dump cycles.

MTI Masternode community is to manage and run the proposals that helps in stabilizing and increasing the value of a currency if the governance system is introduced. In Masternodes, the proposals can be made by any person unlike other coins who charge a proposal fee and this makes Masternode a favorite among investors. After proposals are submitted, a vote is made by master node holders and proposal is voted in.

REWARD TABLE

BLOCK	POS	MN	POW	TOTAL
1 to 50				3.528M
51to 200	No POS	No POS	25	
201 to 15000	1%	99%	20	
15001 to 30000	5%	95%	15	
10001 to 49000	10%	90%	12	
40001 to 90000	15%	85%	8	
90001- 360000	20%	80%	5	
360001 to End	25%	75%	0	

To Run multiple masternodes from single, Single IP system

CONCLUSIONS

MTI Coin is just born yet has made a lot of progress. Tremendous steps have also been made in throughput, network stability and marketing. MTI will be listed on more exchanges soon. Each day MTI closes to consensus swap from POW to POS. In a Proof-of-Stake system, the coin holders get paid transaction fees for validating transactions. Therefore, Proof-of-Stake creates a clear and unambiguous economic incentive to hold coins for the long term.Essentially, a POS blockchain can be thought of as a decentralized Visa / Mastercard with all the additional distributed ledger functionality supported by the specific implementations. This is important, because a Proof-of-Stake coin value can be supported by traditional value arbitrage investing. A POS coin in a functioning network cannot be valued for too long below the present value of the cash flows generated by the network, similarly to any other cash flow producing asset—thus generating stability and dampening volatility, which in turn means POS coins should be better store of value than their POW competitors.