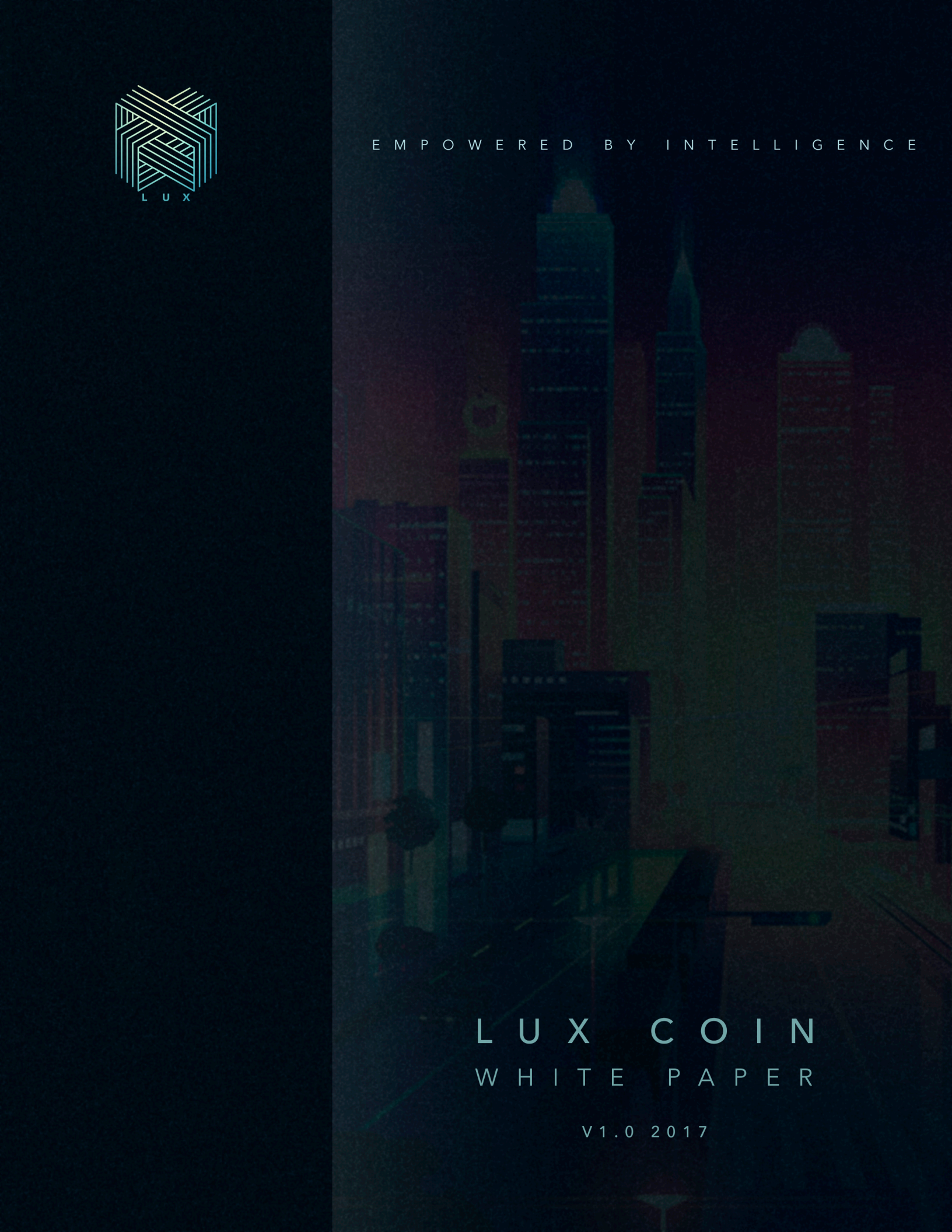

LUX COIN

WHITE PAPER

V1.0 2017

LUXCOIN – WHITE PAPER

BLOCKCHAIN TRANSACTION AT THE SPEED OF LUX

For a cryptocurrency to be truly accepted it must be unilaterally beneficial. Other cryptocurrencies take an Us vs. Big Business or Us vs. Governments approach. ***LuxCoin*** was built to help all three parties by allowing the end-user to select the level of security needed for each transaction. This is accomplished via our ground-breaking ***Phi1612*** algorithm, Parallel Masternode Networks, and ***LuxGate*** technologies. LuxCoin creates a win, win, win solution for all parties and truly decentralized global currency.

HISTORY OF BITCOIN

At LUX, we believe in a no-nonsense approach to business. We assume that if you are reading our white paper, you have a pretty good idea of Bitcoin's history and the invention of the blockchain. If you don't, here's the link to Bitcoin on Wikipedia https://en.wikipedia.org/wiki/Bitcoin. Since the inception of Bitcoin there have been many changes and adaptations to blockchain technology, but the innovation of its decentralized structure has continued to be foundational. We believe LuxCoin has some additional improvements to offer to the following areas.

1. ***Speed of Transactions*** – Many crypto currencies have a slow transaction time, and it is not uncommon for transactions to take an hour or more.
2. ***Incentives to support the network*** – Many crypto currencies use Proof-of-Work (PoW) protocol only. Because of this, the needed network nodes are created only by people currently mining, making transactions, or exchanges trading that currency.
3. ***Level of Security/ Privacy*** – These two terms may seem synonymous, but they are not. According to Wikipedia, Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable or valuable asset, such as a person, dwelling, community, item, nation, or organization.[i] Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. [ii] In order to have Security you first need Privacy. LuxCoin not only gives you both, it lets you choose the level of each you need for every transaction.

WHYLUXISBETTER

The word LUX is LIGHT in Latin. By offering a faster, more profitable, more secure and private transaction solution for individuals, institutions, and governments, ***LuxCoin*** sheds a new light on cryptocurrency. ***LuxCoin*** utilizes a new ***GPU Phi1612*** algorithm built from: Skein, JH, Cubehash, Fugue, Streebog, and Echo. ***PHI1612*** presents the most efficient ASIC resistant GPU mining algorithm, with faster hash rates and reduction of power by 10%. In addition to the new algorithm, ***LuxCoin*** is built with LUX transaction protocol for near-instant transactions.

GET REWARDS

LuxCoin has three distinct ways for Miners and ***LuxCoin*** owners to be rewarded: Proof-of-Work (PoW), Proof-of-Stake(PoS), and Masternodes.

Proof-of-work (PoW) by Bitcoinwiki, is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof-of-work can be a random process with low probability so that on average a lot of trial and error is required before a valid proof of work is generated.

Total Blocks = 6M

Block Size = 4MB

Instamine protection was activated for the first 500 blocks

Block Rewards = 10 LUX

Block Time = 60 seconds

Transaction Confirmations = 10 Blocks

Minimum Transaction Fee = 0.0001

Proof-of-stake (PoS) according to Wikipedia, is a type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus. In PoS-based cryptocurrencies, the creator of the next block is chosen via various combinations of random selection and wealth or age (i.e. the stake).

LuxCoin PoS 2.0 is a Static reward system, not a Dynamic one. A Dynamic system rewards a percentage based on the amount of coins a user holds in their wallet, which can cause those that hold less, to wait days or even weeks for rewards.

LuxCoin PoS 2.0 system rewards a static 1 LUX to all individuals staking, regardless of the amount of coins held in the wallet. Those that hold more coins are rewarded more often. This allows for all individuals staking to be rewarded, without long waiting times due to large weight of others. This means having your wallet open and staking is a great way to increase your coins. A ***LuxCoin*** achieves maturity for PoS after being in an online unlocked wallet for 36hrs. The PoS reward is set to 50% of the block reward.

However, for the first 100,000 blocks the reward is set for 100% of the block reward. The result is that the current PoS reward is 2 LUX to those staking.

PoS 2.0 Static Reward: from block 1 to 100,000 = 2 LUX, after block 100,000 = 1 LUX

Minimum stake age 36h

No Maximum PoS age

MASTERNODES

LUX Masternodes. Any computer mining LUX or staking LUX is considered a node, or connection to the blockchain network. The more nodes the stronger the network. A Masternode is a 24/7/365 dedicated server connected to the blockchain network which adds an additional layer of stability and two additional levels of functionality to the network. The additional functions are 1. Near-instant transactions and 2. ***LuxSend.*** ***LuxSend*** is a form of coin-mixing that provides an additional layer of privacy. To run a Masternode, a user is required to have 16,120 LUX in a wallet.

Masternode owners earn rewards for supporting the network and providing the additional services. These rewards are called Proof-of-Service rewards. The Proof-of-Service payment comes from 40% of the proof of stake and are randomly paid to the Masternode owners. Currently the masternode system is being rewarded .8 LUX and the PoS is being rewarded 1.2 LUX for every Block found.

SECURITY AND PRIVACY

LuxCoin has the capacity for Parallel Masternode networks, providing a public network and a private network running simultaneously on the LuxCoin Blockchain and connected to each other through the ***LuxGate***. This is a new and revolutionary concept in Blockchain technology.

In addition to ***LuxSend***, the Coin-mixing service provided by the LUX Masternode network, which is an improvement on the CoinJoin concept first proposed by Gregory Maxwell [v] there is an additional Security and Privacy option within the wallet called Stealth Address. A receiver can create a Stealth Address with the click of a button in the wallet. The wallet generates an untraceable link to the receiver's wallet, therefore blocking the sender, or a third party from seeing the balance in the wallet.

SECURITY PRIVACY

Threat Levels and Choice of Security One of the foundational concepts of ***LuxCoin*** is the ability for users to choose their own level of security and privacy, known as Threat Levels.

Threat Level 1 – Regular blockchain transaction between trusted or known individuals. Both wallet addresses are visible on the blockchain.

Threat Level 2 – Regular blockchain transaction where the sending address is visible, but the receiving wallet is hidden via Stealth addressing.

Threat Level 3 – Regular blockchain transaction sending address is hidden via LuxSend and receiving wallet is visible on the blockchain.

Threat Level 4 – Regular blockchain transaction where the sending address is hidden via LuxSend and the receiving wallet is hidden via Stealth addressing.

Once activated, the Parallel Masternode network and ***LuxGate*** will add more choices of security with two additional layers of encryption onto transactions on the private network, or transactions that pass through a LuxGate.

PARALLEL MASTERNODE NETWORK

Parallel Masternode Network (PMN) is a second, separate network running on the ***LuxCoin*** blockchain. It uses the ***SAM Protocol*** [vi] ***and i2pd Technology*** [vii] to doubly enhance its encryption. Unlike the masternodes on public network, the masternodes on the parallel network will be reserved for verified institutions. Banks, businesses, and governments will be vetted before they can purchase a Parellel Masternode. Individual users will have access to the i2pd parallel network, but they will not be able to own a Masternode on that network. One of the key security features of the i2pd Parellel network is that all ip addresses connected to the network will be encrypted, and the network will auto change the ip address similar to a Virtual Private Network (vpn). The wallets of users on the i2pd network are not visible on the blockchain explorer. ***LuxGate*** is a unique connection between the two parallel networks, allowing users to send LUX between the two networks. Users can also choose which of the two networks for their wallet to reside upon, based on their personal security/privacy needs, The ***LuxGate*** allows the user to switch back and forth between networks as needed with the click of a button.

USE CASE IN ADDITION TO A CURRENCY

As mentioned in the Parallel Masternode section, the intent is to only sell PMN to vetted institutions and governments. In addition to the added security, they will have access to the closed source ***LuxCore*** Software. The intent of the ***LuxCore*** software is to provide a faster, cheaper, and more secure alternative to the current Swift banking system.

UPCOMING WALLET UPGRADES

Trading Wallet Stake your coins and trade them too! Exchanges are not the safest place for your LUX, and when your LUX are on the exchange you will not receive the PoS reward. The LUX trading wallet allows you to trade your coins directly from your wallet.

Multisignature Transactions Transaction between two wallets that require more than one key to authorize the transaction. This gives users yet another level of security while using LuxCoin.

Examples of ways to us Multisignature Transactions work:

- 1-of-2 Signatures can authorize the transaction. A couple may share a joint LUX account and have two separate signatures. Either of the two is sufficient to authorize a transaction.
- 2-of-2 Signatures: A couple share a joint account, but both parties' signatures are required to authorize a transaction, thus preventing one party from spending the LUX without the approval of the other.
- The number of Signatures can be as large as needed to protect the account and allow for sufficient oversight.

CONCLUSION

This whitepaper is intended to give users of LuxCoin a general overview of its planned solutions to overcoming the shortfalls of other blockchain cryptocurrencies. LuxCoin is uniquely suited to quickly become a leading cryptocurrency as well as a Software as a Service (SaaS) company to serve institutions and governments.

i Security definition. 28 October 2017. https://en.wikipedia.org/wiki/Security

ii Privacy definition 28 October 2017. https://en.wikipedia.org/wiki/Privacy

iii Proof-of-Work definition. 28 October 2017. https://en.bitcoin.it/wiki/Proof_of_work

iv Proof-of-Stake definition. 28 October 2017. https://en.wikipedia.org/wiki/Proof-of-stake

v Maxwell, Gregory. CoinJoin: Bitcoin Privacy for the Real World. 22 August 2013. Retrieved 28 October 2017 https://bitcointalk.org/index.php?topic=279249

vi Project Sam website. 28 October 2017. http://project-sam.awardspace.com/overview.htm

vii I2pd website. 28 October 2017. https://i2pd.readthedocs.io/en/latest/

WWW.LUXCOIN.TECH