WHITEPAPER 1.0

Boostx, Lead Developer BoxyCoin

Author Note: No Grant or Funding has been sought for the BoxyCoin Project.

ABSTRACT

Bitcoin and Litecoin are highly regarded as the first successful digital currency systems. Bitcoin involves miners continuously attempting to solve computational puzzles that have no inherent value. These challenges offer no real intrinsic utility other than to provide equation confirmations, though the value of power used to solve them could be viewed as a monetary worth[1]. BoxyCoin is a cryptographic currency, similar to Bitcoin and Litecoin, with a few major differences. BoxyCoin is a de-centralized cryptocurrency built on ARTAX Technology. The ARTAX backbone of the network offers increased security, reliability and proprietary storage integration unlike no other. BoxyCoin is intended to be the leading coin, incorporating ARTAX technology and Encryption Cache Persistence (ECP), the first of its kind. BoxyCoin will look to incorporate it's technology as it grows into the greater cryptography landscape, to help other currencies wherever possible by broadcasting the technology open-source as it is tested.

Unlike second wave 'Proof of Stake' crypto coins, BoxyCoin utilizes the orthodox 'Proof of Work' protocol incorporating hard-coded persistence scaling. This means there is a fixed available supply, which is important in determining Boxy's value and sustaining a limited market. Every coin held is a representation of a stake in the Boxy movement and a portion of ARTAX technology.

INTENTIONS

BoxyCoin has not undertaken an Initial Coin Offering and does not require any external funding for Development. BoxyCoin is steered by four ambitious developers who met in the crypto-sphere, co-incidentally trying to solve issues with the scaling of bitcoin nodes. The Developers did not undertake any initial advertising campaign or ramp up, they are more concerned with improving the code and letting it speak for itself.

UNIQUE DIFFERENCES

The difference quite simply is the ARTAX vision and associated code. All crypto-currency including Bitcoin, to date have scaling issues, issues with blockchain sizes, transaction sizes and security. ARTAX looks to resolve these issues by way of Encryption Cache Persistence (ECP). ARTAX nodes will use BoxyCoin as a precedent for scaling through one variable spectrum and streamlining one de-centralized storage interface for the coins node backend. The intention is to eventually have other teams forking BOXY and ARTAX into newer, greater things and improvising ARTAX and the storage resolutions into the cryptography landscape.

Unlike Bitcoin and its proposed alternatives, BoxyCoin was essentially birthed in two parts;

(a) BoxyCoin the community currency.

Sustenance in self without “legal tender” laws. To create money that will last beyond generations, and not money that will be losing its value or controlled by a few. To create a currency that will be recognized beyond political affiliations, geographical boarders, or nationalities. BoxyCoin is a truly democratic form of money. It represents an alternative way of thinking about saving, economic freedom, and privacy in financial transactions. Anyone can save and exchange value in a completely transparent way without having to trust each other or any central authority.

(b) The ARTAX Technology Backend.

ARTAX is the driving force behind BoxyCoin, working in the background to enhance node scaling, ECP and mounting the blockchain over the smallest of devices. ARTAX technology is to harness storage as small as a portable phone to be able to carry a compressed version of the chain, exchange and documents. The projection is that, should the local or wider network fail for any reason, this compressed chain can then be synchronized and pushed over many devices, faster and securer than ever thought possible. One variable spectrum that has no central authority should be available for clasping whenever required. A de-centralized storage GUI should be accessible for viewing allotments in the chain.

A typical feature of ‘Encryption Cache Persistence’ (ECP) is the allowance for peer and node information to be translated by way of Bamby Compression and scaled over all nodes and wallets in one seamless integration. This is an expansion on the idea of the blockcipher-based cryptographic compression, one that is set to revolutionize the way blockchains are used. The intention is to be able to carry the blockchain in a compressed formula, isolated from its surrounding environment. This can then be mobilized on smaller, portable devices and piggy-backed on any compatible application.

Successfully running a BoxyCoin wallet or ARTAX node verifies the chain and its contents, providing localized access and encryption to the network. As ARTAX grows, calculations and parameterizations based on realistic hardware constraints will be tested to demonstrate the practicality of BoxyCoin and it’s ARTAX counter-part. Having the ECDH key-pair running harmoniously with ARTAX will be a significant milestone for the team.

WHAT IS AN ELLIPTIC-CURVE DIFFIE-HELLMAN (ECDH)?

ECDH is a Key-agreement protocol which means that ECDH defines how keys should be generated and exchanged between parties. How to actually encrypt data using these keys is up to the people that use it[2]. Traditionally, cryptography has dealt with the secure exchange of information between two parties over an insecure channel.

In other words, suppose Alice wishes to send a message to Bob, but an adversary Eve intercepts every message that either person sends. How can Alice send a message which can be deciphered by Bob but not by Eve? The classical solution to this problem is for Alice and Bob to meet ahead of time and share a piece of information called a key. With the key, a message can be either encrypted or decrypted. Without the appropriate key, neither encryption nor decryption can be performed. Suppose that $E(\cdot)$ is the pair's encryption function and $D(\cdot)$ is the pair's decryption function. Then if Alice wishes to communicate a secret message m to Bob, she sends him the encrypted value $E(m)$. Bob then applies his decryption function to obtain $D(E(m)) = m$. On the other hand, since Eve does not have access to the key that Alice and Bob use, she cannot extract any information about m even if she intercepts $E(m)$. However, this method requires that Alice and Bob meet ahead of time in order to decide on a key. Public-key cryptography allows us to forgo this requirement. More specifically, with public-key cryptography, our adversary Eve is unable to extract any information about a message m even if she has access to both an encryption function $E(\cdot)$ and an encrypted message $E(m)$. However, the message can still be decrypted by a user with access to a separate decryption function $D(\cdot)$. If Alice wishes to send a message to Bob using public-key cryptography, the pair uses the following procedure:

- Bob randomly selects an encryption function E and corresponding decryption function D such that $D(E(m)) = m$. He sends the encryption function $E(\cdot)$ to Alice.
- Alice sends the encrypted message $E(m)$ to Bob.
- Bob decrypts the message by calculating $D(E(m)) = m$. Since Eve knows only the encryption function $E(\cdot)$ and the value $E(m)$, she is unable to collect any further information about m[3][4].

MINING

Billions of dollars have been spent by various individuals and companies to build application specific integrated circuit (ASIC) computers for mining. These devices rendered GPUs and CPUs almost obsolete in the mining process. As a result, the vast majority of Bitcoin and Litecoin transactions are processed by massive data centers.

The Scrypt Algorithm and it's higher memory requirements was utilized by Tenebrix and Litecoin to try and deter ASIC integration. BoxyCoin has the opposite position on ASICs, whereby they are encouraged to service the network and rewarded appropriately for doing so. ASICS are an important part of facilitating the network (though not completely necessary) and producing the hash necessary to verify the ECP where required. Various confirmations will be re-purposed for admission and verification for when a wallet or node is added to the network to ensure integrity of chain.

The basic identity of BoxyCoin and ARTAX is to utilize the hash rather than squander it. The objective is to show that BoxyCoin; Proof of Work resources can be purposed for other, more useful tasks, therefore refuting the claim that mining can only be used to secure the network.

The belief, with consideration to the current crypto terrain and the vast addition of currency is that ASICS will become more competitive. Unlike other Scrypt based coins, BoxyCoin will happily receive and use this to its advantage. The position of BoxyCoin is to encourage new techniques for the better repurposing of blockchain storage and the harvesting of resources other than stand-alone mining. Utilizing stale and orphan blocks will be one of the first things ARTAX aims to address. An estimated 2% of produced blocks are stale in the Bitcoin chain. The ARTAX view is not that mining is a waste of energy but that the current resources are being inadequately managed, resources that have not yet been used to their full potential.

TESTING AND CONCLUSION

The BoxyCoin staging plan is to provide rewards for the testing of ARTAX - payable in BOXY. ARTAX is the underlying technology we would like to make its way into every coin. Testing of Multi-Signature capabilities and integration with the existing Electrum servers will be the first step[5][6]. Bounties and rewards are not just limited to testing but will also cover coin improvement. Introducing a BoxyCoin reward guarantees our development team reliable and fair results in ARTAX testing, it also provides a position for the coin holder to take up a stake in a technology that will change the future of the blockchain as we know it. By way of active participants testing the software also triggers currency flow and adoption by people who are genuinely interested in the technology. The expectation is not for this coin to grow by itself but to expand with ARTAX and encourage other people to clone and improve on the vision. The expectation is that BOXY will be used as legitimate currency and an incentive to solve blockchain scaling problems worldwide by way of lateral medium.

REFERENCES

[1] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. R from https://bitcoin.org/bitcoin. pdf

[2] What is an Elliptic-curve Diffie-Hellman (ECDH)?

Retrieved from https://en.wikipedia.org/wiki/Elliptic-curve_Diffie–Hellman

[3] Cryptography and Secure Two-Party Computation Gabriel Bender August 21, 2006

http://www.math.uchicago.edu/~may/VIGRE/VIGRE2006/PAPERS/Bender.pdf

[4] O. Goldreich, S. Micali, and A. Wigderson. How to play ANY

mental game. Annual ACM Symposium on Theory of Computing.

Proceedings of the nineteenth annual ACM conference on

Theory of Computing. Pages 218-229. http://portal.acm.org/.
http://portal.acm.org/citation.cfm?coll=GUIDE&dl=GUIDE&id=28420

[5] Multisignature - Bitcoin Wiki. (n.d.). Retrieved August 8, 2017, from https://en.bitcoin.it/wiki/Multisignature

[6] Voegtlin, T . (n.d.). Welcome to the Electrum Documentation! ? Electrum 2.5 documentation.

Retrieved August 8, 2017, from http://docs.electrum.org/en/latest/