XSUBYTE WHITEPAPER

V. 1.0

01/01/2019

Table of contents

INTRO

XsuByte is a decentralized, anonymous and p2p coin created in 2018. Based on its own Blockchain, **Xsu-Chain**, is fast, safe and user friendly: is possible send and receive the coin utilizing our wallet (available on Windows, will be released soon for Linux and for smartphone Android and iOS).

Our target is creating a decentralized ecosystem for allow people to be participant of the cryptocurrency revolution. We and our developers will create constantly dAPPs (decentralized applications) for improve users experience and for simplify everyday life.

For the people, send and receive e-money will be easy like drinking a glass of water.

For miners and participants of our ecosystem will be possible earn revenues from all activities. The mining process will be easier than ever: for the first time in the blockchain era, you'll be able to mine our coin directly from your wallet.

The Cryptocurrency

It is a DIGITAL resource that uses CRITTOGRAPHY technology to guarantee the SECURITY of data transmission. Thanks to the cryptographic system, details of the transactions are encrypted and made indecipherable.

They also define P2P (peer-to-peer) and pseudonymous currencies: p2p because they are transferred from one individual to another without the need of INTERMEDIARIES; this makes them FAST and ECONOMIC.

Completely eliminating intermediaries, everyone becomes therefore "THE BANK OF HIMSELF". You can make transactions at any time of the day and wherever you are, without having to depend on a third party.

Pseudonymous because they are not associated to people through their generality, but through a series of codes. Crypto can be stored and managed through external applications that securely contain the codes within them.

The Blockchain

BLOCKCHAIN, literally "chain of blocks", can be defined as a database where all transactions are recorded. Is a type of DLT (Distributed Ledger Technology).

What is on the blockchain is visible to all, immutable and indelible: once registered in a block, a data cannot be changed or deleted.

The blockchain is not on a single server as it can, for example, with a company database. It is found on thousands of computers and is downloadable and verifiable by anyone with the ability to connect to the network. Moreover, some of these computers can choose to update and secure the chain itself and to do so they are rewarded with new coins. They are called MINERS and their work consists mainly in verifying transactions.

All computers connected to the network, which are responsible for maintaining and distributing an updated copy of the entire chain of blocks, are called NODES. The blockchain is one of the technological innovations of the century and its adoption will radically improve our lives.

Cryptocurrency Industry

Since 2009, the year of release of the first crypto, BITCOIN, the cryptocurrency industry has grown incredibly.

Today there are more than 2000+ different cryptos and the overall market capitalization is around 150 billion dollars (source *CoinMarketCap*).

Cryptocurrencies are faster, cheaper and safer than traditional currencies. They allow you to transfer money whenever you want, wherever you are and in absolutely transparency with blockchain technology. Today, around 25,000,000 people own cryptocurrencies. This number is increasing day by day and people knowledge about this innovation is increasing with it.

We believe in cryptocurrencies and we are convinced that, gradually, they will replace the fiat currencies, controlled by governments, states and central banks.

The power and control of money is up to us, not to third parties who control us and force us to use their tools.

XsuByte: p2p, anonymous and decentralized coin

XsuByte is the coin created by people for people. It can be transferred by users with very low costs and at instant speed, allowing them to maintain their anonymity.

For transactions, to see the balance and to check the data you use an external application called WALLET.

XsuByte run on his own blockchain, **Xsu-Chain**, and every transaction will be written on it. With another app, called BLOCK EXPLORER, is possible control every transaction recorded on the blockchain.

XsuByte has a limited supply: there are only 150,000,000 of coins premined and they will be maximum 1,000,000,000 at the end of mining process.

Xsu-Chain: our blockchain

Xsu-Chain represents the heart of our work. It is based on the PoW (Proof-of-Work) consensus algorithm and uses the Cryptonight (Original) algorithm, already used by coins like Bytecoin, Electroneum, etc.

Thanks to PoW, it is possible to create a secure and trustworthy structure that guarantees users very low costs and instantaneous speed for transactions and recognizes the right reward for the work done to the miners. The role of miners is very important and it is thanks to them that it is possible to have all these advantages.

The blockchain technology is revolutionary and thanks to **XsuByte** it will be possible to exploit the full potential of this powerful innovation.

Cryptonight Algorithm (original)

CryptoNight is a proof-of-work hashing algorithm originally designed by the Bytecoin and CryptoNote developer teams. It was originally designed to accommodate CPU and GPU mining whilst at the same time being resistant to Application-Specific Integrated Circuits, or better known as, ASICs. CryptoNight as an algorithm can be thought of as something similar to SHA-256, the mining algorithm used for Bitcoin, or Scrypt, the algorithm used within the Litecoin protocol.

CryptoNight was envisaged as an egalitarian hashing algorithm because it can be computed by CPUs and GPUs, but is impractical for use by ASICs. The CryptoNight algorithm does this by:

- Requiring access to memory
- Latency dependence

Requiring access to memory – Traditional ASICs are suited to hashing algorithms such as SHA-256 because it does not require the device to access memory in order to submit a result. Instead, the ASIC is limited simply by the number of calculations that it can perform per second.

This is to the disadvantage of CPUs and GPUs which do have memory functions built in, therefore, inherently limiting the number of computations that they can perform. Furthermore, each time memory is accessed, the CryptoNight requires 2 MB of memory. This is problematic for some ASICs as they do not have memory functions built into them, therefore, CryptoNight is said to be memory-hard.

Latency dependence – Latency refers to the length of time it takes for a calculation to be issued and for the result to be returned. For example, if a calculation of 2+2 were to be issued, and it takes 3 seconds for the result of 4 to be returned, then the latency is 3 seconds. Furthermore, dependence refers to the notion that a second calculation cannot be performed until the result of the first has be returned, i.e. there is a dependence on the first calculation in order for the second calculation to be performed. In the context of the CryptoNight algorithm, every new solution that is proposed by a device, is dependent on all previously proposed solutions.

CryptoNote

CryptoNote was originally implemented in the CryptoNoteCoin protocol, a cryptocurrency designed for the sole function of showcasing the CryptoNote technology. CryptoNoteCoin itself has no commercial value; the genesis block was relaunched every so often in order to prevent value from accruing.

Cryptocurrencies such as Bytecoin (the very first fork of the CryptoNote) and Monero chose to fork from CryptoNote due to the anonymity technology that the protocol has to offer. Examples of these technologies include:

- Ring signatures
- Stealth Addresses
- Adaptive Limits

Ring signatures – Ring signatures are a type of digital signature for which a group of possible signers are merged together to produce a distinctive signature that can authorize a transaction. A ring signature is composed of the actual signer, who is then combined with non-signers to form a ring. The actual signer and non-signers in this ring are all considered to be equal and valid. ring signature technology helps the sender mask the origin of a transaction by ensuring that all inputs are indistinguishable from each other.

Stealth Addresses – Stealth addresses grant additional security to the recipient of a digital currency by requiring the sender to create a random one-time address for a given transaction. When multiple transactions sending funds to a stealth address are conducted, instead of the transactions appearing on the blockchain as multiple payments to the same address, what will be recorded will in fact be multiple outgoing payments to different addresses.

Adaptive Limits – This refers to the continuous recalculation of different aspects of the CryptoNote protocol, such as its mining difficulty and block size. The difficulty is determined by summing the total work performed by nodes over the last 720 blocks and dividing it by the time taken to reach 720 blocks. In addition, the block size is calculated by taking the average block size of, for example the past 100 blocks, and multiplying it by 2. Therefore, if the average block size of the past 100 blocks had been 1 MB, the new block size would be calculated as being 2 MB.

To conclude, CryptoNight is a proof-of-work algorithm that was originally implemented in the CryptoNote protocol which has since been forked by projects such as Monero and Bytecoin. The CryptoNight algorithm functions by requiring access to memory, as well as placing an emphasis on latency dependence.

The CryptoNote protocol offers cryptographic technologies such as ring signatures, stealth addresses and adaptive limits.

More information on CryptoNote and CryptoNight can be found on the CryptoNote website and the CryptoNote whitepaper.

XsuByte Ecosystem

The main goal of **XsuByte** is to create a real functional and efficient ecosystem. It will allow users to develop dApps (decentralized applications), to interact with each other (messaging programs, social networks, etc.), to share content (video platforms, images, files, etc.), to gain through their activities within the ecosystem, to send and receive money (desktop and mobile wallet) and to keep their resources safe.

To achieve this important goal, we decided to create a fundraiser (ICO) to allow users to participate in advance in our ecosystem and take advantage of exclusive benefits.

XsuByte Coin Sale

In January 2019 will start our coin sale that will allow users to buy **XsuByte coins** (**XSU**).

Below you will find the main information related to our currency.

COIN NAME: XsuByte

SYMBOL: XSU

PREMINED SUPPLY: 150,000,000.00 XSU

TOTAL SUPPLY: 1,000,000,000.00 XSU

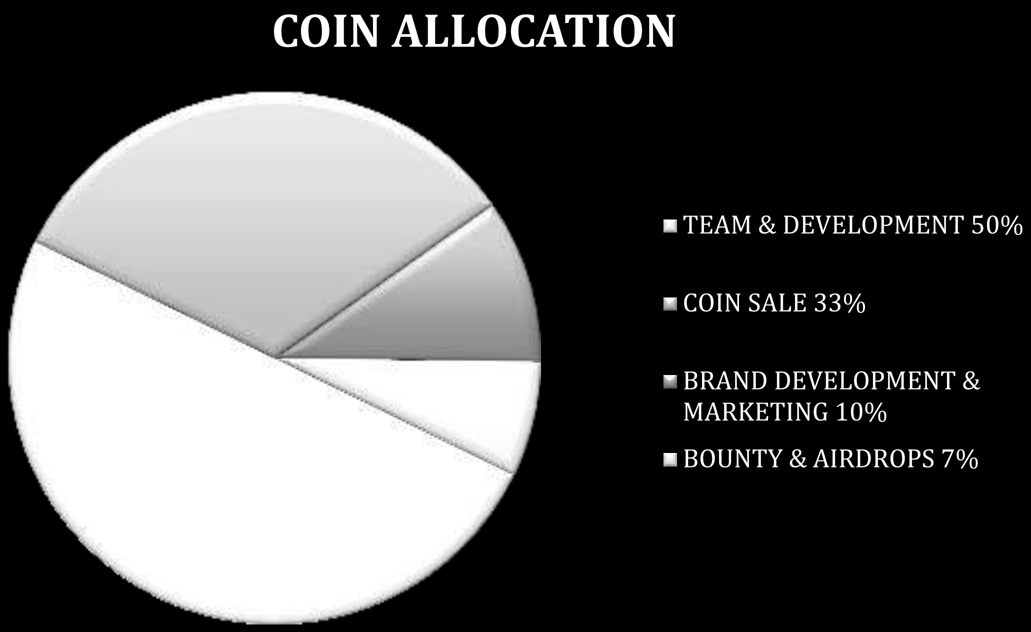
COIN SALE SUPPLY: 50,000,000.00 XSU

PRICE: 0,00001 BTC

SOFTCAP: 75 BTC

HARDCAP: 500 BTC

Crypto Economy



PREMINED SUPPLY: 150,000,000.00 XSU

TEAM & DEVELOPMENT: 75,000,000.00 XSU

COIN SALE: 50,000,000.00 XSU

BRAND DEVELOPMENT & MARKETING: 15,000,000.00 XSU

BOUNTY & AIRDROPS: 10,000,000.00 XSU

DESTINATION OF FUNDS

The funds raised will be used to develop our project, to create the first dApps and to publicize our brand.

Another very important goal will be to be able to list XsuByte on the most important exchanges.

For the moment we cannot provide further information on the development of our project. Follow our social channels to stay tuned for news.

TEAM

FRANCESCO PAPA – CEO, FOUNDER

Programmer

Francesco, a web programmer for 15 years, has worked for several companies in Italy and abroad, in 2010 he entered the crypto field acquiring notions related to mining and expanding his knowledge on blockchain, structure, mechanics etc.

In 2013 begins the development of the first web platforms based on cryptocurrencies, in 2016 begins the programming of the same web services aimed at mobile technology, in 2017 begins a project dedicated to its cryptocurrency and a totally decentralized and anonymous blockchain and then to 2018 with the creation of XsuByte.

ALESSIO FERRARO – CO-FOUNDER

Author, Crypto Trainer & Consultant, Content Writer, Community Manager.

Alessio is a reference in the Italian crypto community. Author of the book "SOGNANDO LA LUNA: MY TRIP IN THE CRYPTOWORLD", a text in which he narrates his adventure in the world of cryptocurrencies and explains to readers all the basics related to these digital innovations.

Founder of Bitcoin4me.it, an Italian portal dedicated to dissemination and teaching about the main tools used in the blockchain world (wallet, exchanges, block explorers, etc.).

Ambassador & Advisor for different realities.

With Francesco & Andrea, in the end of 2018, he starts to project the XsuByte blockchain.

ANDREA DE CICCO – CO-FOUNDER

Web developer, software and mobile applications.

Andrea becomes part of the world of computer science during his studies in Economics and Marketing, applied to the world of the web, open his mind to new business horizons.

After working for an Italian Startup, two years ago, he decided to leave his job to concentrate on cutting-edge new technologies, Blockchain and cryptocurrencies.

From here begins its journey towards the development of XsuByte.

USEFUL LINKS

Website: www.xsubyte.org

Telegram Official Group: t.me/xsubyteofficial

Discord Channel: discord.gg/FFNTcb8

Facebook Page: facebook.com/xsubyte

Twitter: twitter.com/xsubyte

BitcoinTalk thread:

Reddit: