PAPERCOIN WHITEPAPER

V. 0.005

INTRODUCTION CRYPTOCURRENCIES

Cryptocurrencies are changing traditional finance and payment methods. The cryptocurrencies guarantee transparency and anonymity in the international transactions.

Most cryptocurrencies are designed to gradually introduce new currency units, putting a cap on the amount of money that will be in circulation. This is done both to imitate the scarcity (and value) of precious metals, and to avoid hyperinflation.

Over thirty different specifications and protocols have been defined which are mostly similar or derived from Bitcoin. Since 2009, after the advent of Bitcoin, many cryptocurrencies have been issued, immediately called altcoin (alternative coin, or alternative coins to the original one), which differ in some aspects, and use blockchain and technologies other than Bitcoin. Altcoins rely on features that Bitcoin does not possess according to the altcoin developers. Cryptocurrencies can be like ordinary currencies managed by financial institutions or accumulated and saved as cash.

Transactions made with cryptocurrencies offer a good level of privacy, thanks to the pseudonymic nature of the users. The level of privacy varies depending on the protocol used, and is total for those cryptocurrencies (such as Monero, Dash, Zcash) that use the "zero knowledge" validation system, thanks to which no information of the parties is exchanged.

they use peer-to-peer technologies (p2p) on networks whose nodes are made up of users' computers, potentially located all over the globe. On these computers special programs are executed that perform functions of purses. There is currently no central authority that controls them. The transactions and the release take place collectively on the network, therefore there is no "centralized" management. These unique properties of their kind cannot be performed by traditional payment systems. The decentralized control of each cryptocurrency works through a generalized accounting technology (DLT) generally a blockchain, which serves as a database of public financial transactions.

INTRODUCTION BLOCKCHAIN

The blockchain is a very powerful and cheap technology. The blockchain technology has not yet been fully clarified from a legal and legislative point of view, but governments are trying to move towards a progressive update: in 2017, for example, the state of Nevada, United States, has approved a law for the complete liberalization of the blockchain.

As for the Blockchain, it was recognized within the Italian legal system with Law 12 of 11 February 2019, within which the legal value of any information recorded on it was also recognized. In the same Law reference is made to smart contracts, while no further definition of cryptocurrency is recognized.

INTRODUCTION PAPERCOIN

Papercoin the cryptocurrency for paper and tobacco articles.

Papercoin is a cryptocurrency for buying tobacco and smoking items.
The idea is to create an international payment system through the blockchain, an inviolable and completely decentralized technology. Papercoin was issued on WAVES blockchain
Papercoin was created to be adopted by sellers and buyers of tobacco and smokers' items worldwide.
The WAVES blockchain is new, innovative, fast and with low transaction costs.
The asset ID of Papercoin is: DeYSvxFZW7tqowT3YK57SskTNBvLHway7ErP9aedk2r3
Cryptocurrencies are the future of payments and finance, every company in the future will have its crypto or token to facilitate payments. By buying tobacco items with Papercoin it will be possible to receive the item directly at home in a few days, transactions will always be traceable on the blockchain and secure, fast and encrypted payments. The Papercoin project tries to solve all international payment problems and tries to facilitate the exchange of services anywhere in the world.
Papercoin will be a partner of all those who want to buy and sell tobacco and all smoking products.

Asset ID: DeYSvxFZW7tqowT3YK57SskTNBvLHway7ErP9aedk2r3 **Asset Name: Papercoin** **Ticker: PAPER** **Total Supply: 55,782,893,421.28759003**
Total Burned: 55,427,040,132 Date: 07/04/2019 **Circulating supply: 355,853,292** **Decimals: 8** **Not Re-Issuable**
Issuer: 3PAQYBQvu5yvG53xgUcr2ZythKLMUhnxDcu **Issue Date: 2019-02-25 19:03:26** **Blockchain: WAVES** **Issued in Waves block: 1,412,586**

ABOUT CRYPTOCURRENCIES

A cryptocurrency is a digital - assets designed to work as a medium of exchange using cryptography to secure the transactions on a ledger that is typically publicly viewable. A community guarantees the authenticity of the transactions in addition to the creation of additional units of the currency

what problems do cryptocurrencies try to solve?

The problem bitcoin is trying to solve is an important one faced by many people across the world. By controlling money, vast power is wielded in today's world. The enormous amount of money in circulation is primarily controlled by bankers and they wield the powers of inflation and currency debasing as methods of increasing and controlling product prices throughout the economy. Centralized and institutional control of currency is the problem the cryptocurrencies is trying to solve.

the virtual value like many other cryptocurrencies, gives power to the people using the cryptocurrency as they do not require authorities in a centralized system to do business and make purchases. By being peer to peer (P2P) and decentralized it lets people trade without having the rules of the transaction dictated by third parties. Cryptocurrency enables users to act anonymously and this removes power traditionally held by financial institutions.

ABOUT BLOCKCHAIN

Initially the blockchain may seem difficult to understand; in reality it is very simple. The blockchain represents another type of transaction logging database: when a transaction occurs, it is copied to all of computers in a participating network. This process is sometimes called distributed ledger. The data is stored in "blocks", which have two important features:

- Content: represents a list of instructions and digital resources, the amounts and addresses of the parts of these transactions.

- Heading: consisting of metadata (for example, the unique block reference number, a link to the previous block and the time the block was created. Knowing the last block, you can access all the previous blocks that are connected to each other through a chain (blockchain) .The more the network grows, the more difficult it becomes for the malicious actors to pass the verification processes carried out by the community.

ABOUT PAPERCOIN

Papercoin the cryptocurrency for paper and tobacco articles. Papercoin is a decentralized cryptocurrency based on the WAVES blockchain. Papercoin can be used as a store of value and can be exchanged with other cryptocurrencies and trade on exchanges. Papercoin guarantees completely anonymous, public and traceable transactions on the WAVES blockchain. the Papercoin project aims to bring tobacco, cigarettes and smoking products to blockchain sales. Papercoin can facilitate transactions worldwide, thanks to the speed of the transaction (6 confirmations) in 1 second. Papercoin is a good, safe and cheap currency. Papercoin promises financial sovereignty to those Papercoins that are not controlled by any centralized institution. Banks and governments do not have control over it.

GET PAPERCOIN

Papercoin are earned on the exchanges on which it is listed, with airdrop events and with the Papercoin bot.

Join out Papercoin community

- Papercoin Airdrop 🛬💎💎💰💰💎💎🛬 Telegram bot @papercoin_bot
- Papercoin telegram group
- Papercoin faucet
- Twitter
- Instagram
- Linkedin

WHAT IS PAPERCOIN

Papercoin is a cryptocurrency that tries to simplify transactions around the world in an easy, secure and fast way, guaranteeing a high level of privacy. Papercoin's vision (PAPER) is to make decentralized payments for the purchase of services and items worldwide easier.

FAST. SAFE. ANONYMOUS. TRACEABLE.

Papercoin is a decentralized payment system based on the waves blockchain for safe transactions.
A secure and anonymous crypto-asset. built with a focus on democracy and privacy.

TRANSACTION FEES

Commissions for Papercoin and other crypto-asset transactions on the WAVES blockchain are very low (0.001 waves) The commissions are fixed, so they do not depend on the amount sent. The commission payment on the blockchain serves as a reward for the miners who extract WAVs using the LPoS algorithm. If there are many minerals active on the WAVES blockchain, the decentralized system becomes faster, more reliable and safer.

WAVES BLOCKCHAIN

Open-source blockchain platform for cutting-edge dApp: provides tools to create WEB3 solutions. The blockchain platform launch campaign declared the collection of $ 16 million, making it one of the largest in terms of funds raised through crowdfunding. In June 2017, the Waves platform reported the integration of the dollar payment gateway into the Lite client; this allows the users of the portfolio to reinstate the account in US dollars.

The Waves platform is analogous to the cryptocurrency of the Kickstarter crowdfunding platform. The platform allows each user to issue a cryptographic token for less than a minute and to raise funds through a crowdfunding campaign. Users can interact with the platform using the Chrome browser or download the complete app and start it from your PC.

DEX Decentralized Exchange

Waves opened DEX, the first decentralized exchange in history, which allows users to exchange any pair of tokens without obtaining a transaction through an intermediate currency.

Just a few milliseconds to approve the transaction.

An important feature of DEX, is to work faster and more safely than traditional cryptocurrency exchanges. The work of the exchange is paid by the corresponding nodes, which are linked to the buyer by the seller for a commission, and then it corrects the transaction in the Waves blockchain.

Technical Specifications

The platform works through the leasing participation test mechanism, replacing the Proof of stake consent. LPoS is released on MainNet; it gives the possibility to any user of transfer their technical skills for mining and receive awards while increasing the network security. For this reason, classic cryptography is used with a public key. Tokens can be converted either into fiat or cryptocurrency, or into tokens of others projects.

ALGORITHMS ON BLOCKCHAIN

Any blockchain requires a mechanism that allows you to decide which block chain is valid, and to guarantee that there are no double costs (for example sending the same money to different parties and in separate chains). There are different methods to achieve this goal.

The waves use the so-called Proof-of-Stake consensus algorithm. Below we will describe and compare it with the widely used Proof-of-Work algorithm which used for example Bitcoin. Since each Blockchain is a system of decentralized "nodes" (or computers that confirm the transactions that occur on the network and maintain decentralized consent throughout the system), it is important for these nodes, also called "miners" in the Proof system. of-Work or "validators" in the Proof-of-Stake system, to be encouraged to continue to confirm the various transactions. The way in which nodes ("miners" or "validators") confirm transactions and how these nodes are encouraged to do so - is the main difference between Proof-of-Work and Proof-of-Stake. Proof-of-Stake represents a different methodology for validating transactions and achieving distributed consent. The purpose is the same as the proof of work, but the process to reach the goal is different. In PoW the number of mining blocks is proportionate to the amount of hardware and energy resources that have been invested. On the contrary, in PoSa the person can extract or validate block transactions based on the amount of coins he holds. Consequently, unlike the Proof-of-Work, the creator of a new block is selected randomly, with a greater amount of betting which increases the probability of inserting a block in the chain.

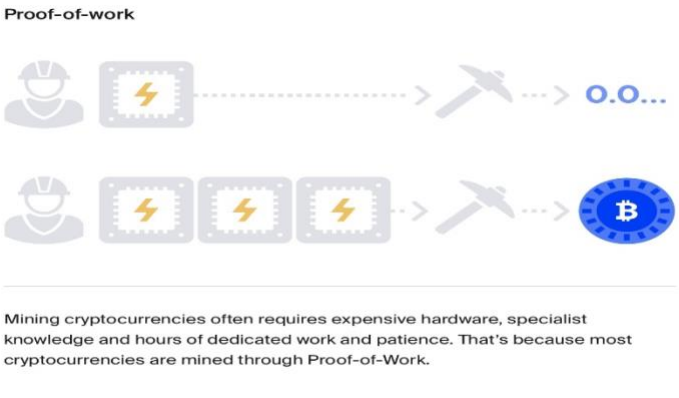
Usually, in the PoS system, there is no block premium, so the miners take the transaction fees. For this reason, miners are often called block forgers or generators.

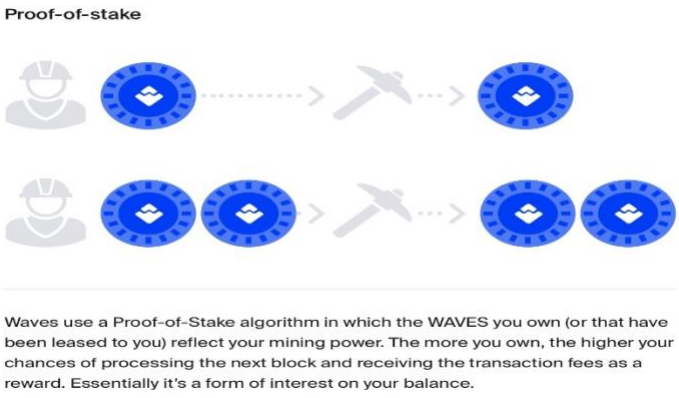
With a PoS, the attacker should get 51% of the cryptocurrency to execute a 51% attack. The stake test avoids this "tragedy" making it disadvantageous for a miner with a 51% stake in a cryptocurrency to attack the network. Given that it would be difficult and expensive to accumulate 51% of a reputable digital currency, a miner with 51% of the currency would have no interest in attacking a network of which he holds the majority. If the value of the cryptocurrency decreases, the value of its holdings also decreases, and therefore the owner of the majority stake would have more incentive to maintain a secure network.

PoS has some constraints to avoid certain types of attacks, now we see them in detail:

• The minimum amount of WAVES to be generated is 1000 WAVES

• When a scale is increased, the generation scale will be increased after 1000 blocks





LPoS ALGORITHM ON WAVES BLOCKCHAIN

LPoS is an improved version of Proof-of-Stake. Normally in the Proof-of-Stake system, each node that holds a certain amount of cryptocurrency can add the block following the blockchain but in the LPoS system, (and more specifically on the Waves platform), users can rent their balance at full nodes . With LPoS, the user will be able to rent WAVES from the wallet to several contractors who can pay a percentage reward. The larger the amount that is leased to a complete node, the higher the chances that that complete node will be selected to produce the next block. If that node is selected, the lessee will receive a percentage of the transaction fee that is taken from the complete node.

In the case of leased Proof-of-Stake, users have two choices: executing a complete node or leasing their stake to a complete node with the receipt of prizes. This system allows anyone to participate in the maintenance of the Waves network.

The user can also rent his WAVES through leasing on any computer or mobile device equipped with an Internet browser, since Waves provides a lite client solution that rents his balance to store the entire Blockchain or to make the wallet work.

ANONYMITY

Cryptocurrencies have gained enormous popularity due to many factors. Two important ones among those are the features of privacy and anonymity that cryptocurrency networks offer which allow a user to keep their identities as well as their transactions concealed. Amid mounting concerns about data privacy, the world of cryptocurrencies is also becoming worried about threats to user privacy.

PRIVACY

The purpose of cryptocurrencies is to maintain the privacy of those who purchase them; no government

or bank can access cryptocurrencies in portfolios. The portfolios are controlled exclusively by those who own the

access keys.

In a society where our privacy is constantly threatened, it is essential to maintain the privacy of the transaction. Many have received cryptocurrencies as privacy,

coins or payment methods in its early years. It was believed to be one of the great promises of this

technology: anonymity. Transactions are recorded and made public, but are only connected

with an electronic address. This means that you preserve your privacy until the pseudonym

it's not connected to you.

SAFETY

It's called cryptocurrency because it uses encryption to verify transactions. This means that advanced encryption is involved in storing and transmitting cryptocurrency data between portfolios and public records. The goal of cryptography is to provide protection.

There are various types of cryptocurrency portfolios available, with different levels of security, including devices, software for different operating systems or browsers, and offline portfolios.

A cryptocurrency is composed of an encrypted data string indicating a currency unit. It is monitored and organized by a peer-to-peer network called blockchain, which also acts as a secure ledger for transactions, for example the purchase, sale and transfer. Unlike physical money, cryptocurrencies are decentralized, which means that they are not issued by governments or other financial institutions.

They are created (and protected) by cryptographic algorithms that are maintained and confirmed in a process called mining; a computer network or specialized hardware how application-specific integrated circuits (ASICs) process and validate transactions. The the process encourages the miners who manage the cryptocurrency network.

VALUE RESERVE

Cryptocurrencies are an excellent store of value, which is why they are compared to precious metals.

Value reserve means an activity (tangible or intangible) that tends to preserve its value over time; for this reason it can be kept for future use without the danger that it will "deteriorate". The reserve value cannot be absent in payment instruments, given that the use of a payment instrument assumes that his temporary detention does not cause him to lose value in terms of purchasing power.

WHAT IS AN EXCHANGE

A cryptocurrency exchange or digital currency exchange (DCE) is an exchange where it is possible buy or sell cryptocurrency. We can exchange it using electronic currency units, Fiat currencies or other digital resources. Dollars, pounds, euros, yuan and yen, for example, are fiat, that is, currencies that governments declare as legal tender.

Digital resources are any resource which exists electronically, such as domain names, files, digital currency or virtual property.

Modern technological solutions, such as cryptography, ensure that transactions are extremely secure. Encryption allows you to create and decrypt the code.

Generally a cryptocurrency exchange works 24/24 h 7/7 days. One of the most important features is that they remain anonymous. No one knows who the buyers and sellers in cryptocurrency are.

On cryptocurrency exchanges, you can make instant transactions.

A cryptocurrency exchange could be seen as an online entity that exchanges money and digital currencies electronically transferred.

It could also be seen as a physical business that exchanges digital currencies and uses traditional payment methods.

WHAT IS A WALLET

Cash is stored in a physical portfolio and for the cryptocurrency the pè analogous system is used. The wallets store the private keys you need to access an address. They are present in different forms, designed for different types of devices. You can also use card storage to avoid having them on your computer. Of course, protecting and backing up your wallets is very important.

A cryptocurrency wallet is a software program that keeps public and private keys, interacts with various blockchains to allow users to send and receive digital currency and monitor their balance.

A cryptocurrency wallet, similar to a bank account, contains a pair of cryptographic keys. The public key allows other portfolios to make payments to the portfolio address, while the private one allows you to spend cryptocurrency from that address.

In addition, portfolios can be digital apps or hardware. If the private key is not stored with the user, it is stored remotely and transactions are authorized by a third party.

Key derivation
Deterministic wallet

With a deterministic portfolio it is possible to use a single key to generate an entire tree of key pairs. In this case the single key acts as the root of the tree.

The generated mnemonic phrase or the word seed it simply represents a more readable way for humans. Those words, in this order, will always generate the same root key.

A sentence can consist of 24 words or 12. That single root key does not replace all the other private keys, but rather is generally used. All addresses usually have different private keys, but they can all be restored from that single root key. The private keys of each address can be calculated starting from the root key.

That root key, in turn, can be recalculated by inserting the word seed. The mnemonic phrase represents the backup of the portfolio. With the backup you can restore the portfolio also on another software.

PAPERCOIN WALLET

Papercoin is supported on the WAVES wallet available for WINDOWS, iOS, ANDROID, MAC

With the WAVES wallet you can send and receive Papercoin and other cryptocurrencies, you can exchange FIAT currencies with other cryptocurrencies and you can vote safely and anonymously.

WAVES WALLET CLIENT

The Waves Wallet is the official wallet for the Waves Platform. It comes as a Chrome Extension and can be easily installed and used to perform most actions in the Waves Platofrm as well as for Windows, Linux and Mac OS. Currently in development, the Waves Platform will allow users to issue, transfer and trade assets.

The wallet has a built-in decentralized exchange platform that can be used to exchange assets, cryptocurrencies and fiat tokens.

Multi-currency

Supports a range of fiat and cryptocurrencies, including USD, EURO, TRY, BTC, ETH, LTC, PAPER, ZEC, BCH, BSV, DASH and XMR, all of which can be deposited, stored, traded and withdrawn

Multi-platform

Can be used on Windows, Mac OS, Linux, iOS and Android devices.

Secure

All traffic and private keys are encrypted and stored only on your device. Face ID, Touch ID and Fingerprint scanning are supported

TRANSACTIONS TIMES

Waves explained that if the size of a block in the bitcoin network is increased by four times, "only 90% of participants will have time to download it before creating a new one.

In particular, NG allows blockchains to minimize latency and maximize throughput.

NG is basically a modification of the protocol and allows an increase in the number of transactions per block without increasing the number of forks.

The information to start generating the next block is sent quickly to all the nodes after the generation of the previous one. Only after this step will the miner send the transactions that will fill the block to the network, sending them in different tranches (or microblocks).

Platforms

	Consensus Mechanism	**Block Time Target**	**Actual TPS max**
Ardor	POS	1 minute	800
Bitcoin	POW	1o minutes	2,000
Bitshares	DPOS	2 seconds	100,000
Ethereum	POW	15 seconds	2,000
Heat Ledger	POS/POP	25 seconds	1,000
Steem	POW	2 seconds	1,000
Waves	DPOS/LPOS	1-30 seconds	1,000

PAPERCOIN WHITEPAPER DISCLAIMER

The Papercoin whitepaper has no legal value

This whitepaper has not been viewed by any legal institution

The Papercoin whitepaper is for informational purposes only

This document is not an invitation to invest in cryptocurrencies

The Papercoin team reserves the right to disclose this whitepaper for informational purposes only

ROADMAP

COMING SOON...

CONCLUSION

The mission of Papercoin is to become a partner of the stores that sell items for smokers. Our vision is to implement sales and shipments of physical and online smoking stores on the blockchain of WAVES.

We will try to bring Papercoin to a level of utility even in real life.

We offer Papercoin as an alternative payment method to FIAT currencies, a fast, secure, anonymous, cheap and decentralized payment system

NOTE

This whitepaper is at version 0.005 The Papercoin team reserves the right to update / modify the whitepaper and its related content