WORTHLESS COIN

IN WORTHLESS WE TRUST

This presentation has the scope to educate and introduce some key terms and notions related to the Worthless Coin Project and decentralized peer-to-peer cryptocurrency systems in general.

These set of notes and the material contained therein do not constitute investment advice. You should always consult your financial advisor prior to investing in cryptocurrencies. The Worthless Coin Project accepts no responsibilities for any damages direct or consequential deriving from the use of this document and its content.

WORTHLESS COIN

Introduction To Cryptocurrencies and The Blockchain

Cryptocurrency is a decentralized (Peer-to-Peer, P-2-P) digital currency that combines an online (public) ledger - called the blockchain - with strong cryptography to secure and validate online transactions. In this set-up, decentralized means that there is no need for a central server or trusted parties (hence no need of financial intermediaries). In decentralized payment systems users hold the crypto keys to their coins and transact directly with each other, with the help of a P-2-P network which prevents double-spending and counterfeiting.

Advantages of the Blockchain

1. Cryptocurrencies provide a platform for two parties to easily transfer funds without the involvement of any third party (such as banks and/or credit card companies).
2. Thanks to the blockchain, cryptocurrencies cannot be counterfeited, double-sent or reversed arbitrarily by the sender. Furthermore, transaction anonymity and privacy are granted by the sophisticated workings of the blockchain technology.
3. Transferring cryptocurrencies only incurs in low processing fees, allowing the user to potentially save on charges incurred when adopting more conventional payment methods.
4. Thanks to its increasing popularity, there are numerous websites that accept cryptocurrency payments, as well as websites where users can convert cryptocurrencies into major (commonly accepted) currencies (€, $, £, etc.).

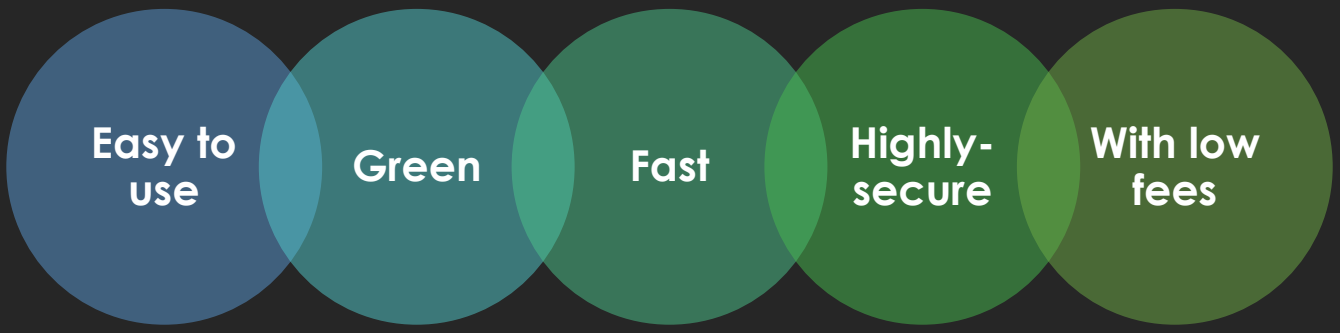
The block chain is a shared **public ledger** on which the entire network relies on. All confirmed transactions (coins sent/received) are included in the block chain. Transactions are **permanently recorded** in files called blocks. New transactions are constantly being processed and **validated** by miners into new blocks which are then added to the end of the chain. The more deeply embedded in the chain each block is, the **more secure** and **confirmed** these transactions become.

In order to **verify transactions** and append blocks to the blockchain, miners need to solve **complicated mathematical functions**. However, once the solution is found, it is easily verifiable by the network. This is the process of "mining", where "miners" compete to find the correct answer.

WORTHLESS COIN

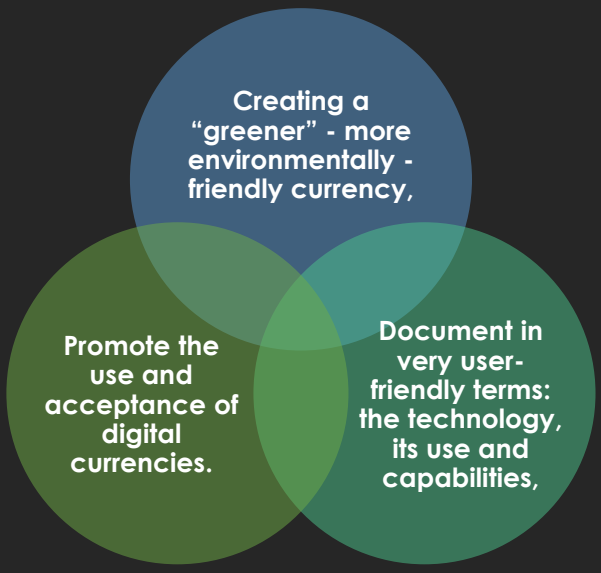
Introduction to Worthless Coin

Worthless Coin is a new **decentralized electronic cash system**. It aims to be a new digital currency that is:



MAX COIN SUPPLY	1 Billion WRTC
CURRENT SUPPLY	100 Million WRTC
BLOCK REWARD	500 WRTC
BLOCK TIME	60 SECS
SYMBOL	WRTC
CONSENSOUS PROTOCOL	P-O-W (scheduled to move to P-O-S)
ALGORITHM	SHA-256

Worthless Coin is based on the same technology as bitcoin; however, these are two different, **independent** blockchains.
The objective is to carry out some **tweaks** to existing cryptocurrency characteristics with the objective to:



Worthless Coin was created as a joke. The name reflects the common adjective given to cryptocurrency, aka "worthless coins". The project started as an educative project, without however posing any limitations to its scope.

WORTHLESS COIN

Main Properties Of Worthless Coin

The main properties of Worthless are the same as other existing cryptocurrencies (e.g., Bitcoin), with few **useful additions**:

Time Efficient

- With a high transaction speed, Worthless Coin is available anytime, anywhere. Users can transfer Worthless Coins in real time across the globe.

Safe and Anonymous

- Worthless Coins allows you to send and receive secure and anonymous payments. Privacy and anonymity is ensured thanks to the blockchain technology and cryptography.

Decentralized

- The worthless coin is controlled by the community, hence there is no need for third parties. The network validates and executes transactions. This puts the users in power and at the center of the system.

POS consensus – "greener currency"

- In a Proof-of-Stake (PoS) protocol it is possible to mine or validate the block transactions according to how many coins are held (stake). The more coins are owned, the higher the mining power. Proof of Stake is less energy expensive because it removes the high-powered computing need of Proof-of-Work (PoW) from the consensus algorithm.

User friendly cryptocurrency

- Currently, cryptocurrencies are difficult for the average user to understand and use. The objective is to render the use and understanding of worthless coin accessible to a wider audience.

WORTHLESS COIN

Proof-of-Stake vs Proof-Of-Work Consensus

POW	POS
▪ Proof-of-work (p-o-w) is a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle to prevent anybody from gaming the system.	▪ Validate block transactions based on the number of coins a miner holds (more coins held mean more mining power).
▪ The probability of solving a block is a positive function of the computational power of a miner.	▪ A miner is chosen depending on existing share of coins held (aka stake) in a deterministic way.
▪ A reward is given to the first miner who solves the block.	▪ Miners are rewarded with transaction fees for validating a block, however they lose a part of the stake if they verify fraudulent transactions.
▪ Adding a malicious block requires a hacker to have 51% of the total network computational power (possible in the long run when reward decrease so does the number of miners, leaving a small pool of miners in power).	▪ Adding a malicious block requires a higher to hold a stake of 51% of the total coins (unlikely because its expensive and unlikely that a majority stakeholder attacks is own coin).

A Highly Documented and User-friendly Cryptocurrency

- The use and working of cryptocurrency and blockchain are **still obscure** to most of the world population;
- Worthless Coins aims at being one of the most **user-friendly** cryptocurrencies – focusing on fostering the **understanding** of its uses and **workings** to a wide audience;
- User-friendliness will be guaranteed by the provision of **step-by-step guides** and **video tutorials**;
- Effectively rendering the use and applicability of the currency **within everyone's reach**.

WORTHLESS COIN

The Worthless Coin Wallet

- A **transaction** is a transfer of value between Worthless Coin wallets that gets included in the block chain.
- Worthless Coin wallets keep a secret piece of data called a **private key** or **seed**, which is used to sign transactions, providing a **mathematical proof** that they have come from the owner of the wallet.
- The **signature** also prevents the transaction from being altered by anybody once it has been issued.

Cryptocurrency Wallet Terms

Public Key
- Your wallet's public address is used to receive coins to your wallet.

Private Key
- A digital signature that proves you own the coins

Keystore File
- An encrypted version of your Private Keys

Mnemonic Phrase (Seed)
- List of words that store all the information needed to recover funds in a wallet.

WORTHLESS COIN

How To Get Started With Worthless Coin

Choose your wallet according to your OS

- A wallet is used for holding your Worthless Coins directly on your computer/smartphone.

Configure your wallet

- After downloading, you can configure your wallet according to our guide.

Get some Worthless coins

- There are numerous way to get Worthless Coins. You can receive them, trade for them, get tipped, "mine" them, and more.

You need to synchronize with the blockchain to use Worthless Coin. A worthless coin is a "full" wallet. It syncs by downloading it, providing a solid-working Worthless Coin wallet. Worthless Coin supports wallets in the following Operating Systems:

- Windows User
- Linux
- macOS
- Android **Under development**

Community Support

The worthless coin is currently not endorsed by anyone nor any other project. The hope is that the community will recognize the efforts and that this will result in endorsements by individuals and other projects in the future.

For endorsements, collaborations and exchange of ideas please get in touch at: info@worthless-coin.co.uk

WORTHLESS COIN

Conclusion

In conclusion, Worthless coin is a cryptocurrency using its own independent public ledger that is highly secured and has low transaction fees. Although completely independent from Bitcoin, the blockchain uses the same highly secure and powerful SHA-256 algorithm. However, unlike Bitcoin, Worthless Coin employs a POS (Proof of Stake) protocol to reach network consensus. In blockchain networks, POS protocols are a set of consensus mechanisms for blockchains that work based on selecting validators in proportion to their quantity of cryptocurrency holdings, effectively making it a "greener" - less energy intensive alternative to POW (Proof of Work).

Finally, thanks to the wide provided documentation, numerous videos and teaching material, Worthless Coin aims at being a user-friendly cryptocurrency widely understood and exchanged worldwide.