Title 1: Zoom into Cryptowallets

Title 2: A Quick Dive into Cryptowallets

**Title 3: Cryptowallets Explained**

**Cryptowallets are a vital element of the cryptocurrency economics and ecosystem. Without them, even the most basic crypto transactions simply wouldn’t be possible. In this article, we introduce the idea of cryptowallets and explain what they are and how they function.**

**What are cryptowallets?**

Cryptowallets are either digital tools or physical devices that allow you to store, trade and manage cryptocurrencies by interacting with a blockchain. Cryptowallets do not hold any cryptocurrency as such. Instead, they contain the addresses of public and private keys that prove your ownership of a digital currency and allow you to make crypto transactions. Metaphorically speaking, a public key address can be compared to a traditional account number and a private key to a PIN code or security password.

**The Keys to the Kingdom**

To understand the mechanism of cryptowallets, we first need to get to grips with public and private keys. A public key is a long alphanumeric code consisting of letters and numbers that enable you to receive cryptocurrencies into your account. This is a unique personal address that can be compared to an account number that is shared between two people that perform a transaction. A public key can be safely shared between a payer and a receiver. Different types of cryptocurrencies have different formats.  A public address can be easily acquired when a wallet is being set up. A bitcoin public address will look like something this:

***Example: 1BdVxAKqVwSAomk3T8MQSMoADL1PRtXcUL***

Private keys are cryptographic codes that secure transactions guaranteeing that only the desired recipient can access the contents that have been sent. They constitute a vital component in cryptocurrency security. Private keys are randomly generated and very long. It is very important that you keep private keys secret and store them safely, as they constitute the only way to access your crypto funds.

Even though a public address is known to everyone, your wallet cannot be accessed and your funds cannot be spent by anyone who does not have the corresponding private key. Because of this unique two factor authentication, cryptowallets can be considered secure.

**How do cryptowallets work?**

As we just established, cryptowallets use two keys – public and private – to securely carry out the transfer of funds. Public keys are derived from a private key – a kind of a passcode for accessing the crypto assets stored at the corresponding public address, which acts as your pseudonymous identity for sending and receiving the crypto assets. In general, the crypto assets are stored at different public addresses and are visible in the open distributed ledger. If you own the private key, you own the crypto assets stored at that public address. It means that anyone who gets custody of the private key gets access to the funds at the same time.  In other words, you get to have your own bank, take responsibility for your assets and safely manage them.

**Wall to Wall Wallets**

**Hot & Cold Wallets**

Hot wallets are cryptocurrency wallets that are always connected to the internet. They are easy to set up and access. Cold wallets, on the other hand, are cryptocurrency wallets that are not connected to the internet. You can find a comprehensive list of the different types of hot and cold wallets below.

**Hot Wallets:**

**Web-based Wallet**

The simplest and quickest way to deposit, store and transfer crypto assets is via a web-based wallet. They can be chosen from a number of websites. Web-based wallets are the least secure method of storing your money and can be vulnerable to hackers. If the website hosting them is compromised, then you could lose all your money. You must pay attention to safety measures to avoid losing money to hackers, for example by using two-factor authentication.

**Mobile Wallet**

Mobile wallets are installed on phones in the form of mobile apps. They are very convenient because transactions can be performed instantly. However, phones can easily be misplaced or damaged, which is a downside in terms of security.

**Desktop Wallet**

A desktop wallet is installed on a computer and gives you complete control over transactions. Its biggest drawback is the threat posed by computer viruses.

**Cold Wallets:**

**Paper Wallet**

A paper wallet is an analog version of wallets that include printed keys and QR codes. They should be kept in a secure place. It is also advisable to keep more than one copy of a wallet to avoid permanent loss of data if it is damaged.

**Hardware Wallet**

A hardware wallet is similar to a USB flashdrive. It ensures the highest security standards and allows a significant amount of digital assets to be stored. Most hardware wallets require you to push a physical button in order to confirm a transaction. This makes it impossible for hackers to access your private key and your coins.