**What is Encryption, Wallet, Private and Public Keys.**

PS: I will be commonly using ethers in below explanation of wallets. Ether is not the only form of crypto money, but there are others like Bitcoin, Litecoin and many others. I am sticking to Ether for simplicity sake.

Like you carry a physical wallet with multiple credit /debit cards in it. Apply similar analogy to crypto wallet. It’s a piece of software which can hold multiple Externally Owned Accounts (EOA). Like each credit/debit card in your wallet is unique in number carrying its own money, similarly, each EOA is unique in number and can be filled with varying amounts. You can use these accounts to perform transactions, send ethers or receive ethers. Remember in previous article (Article 3) inherent accounts owned by Ganache (local blockchain) carried fake ethers to enable us deploy SC because deploying SC is a transaction and transaction in Ethereum world comes with a cost? Deployment of SC is one form of transaction. Other form of transactions can be buying of your daily needs.

In real crypto world to carry out real transactions EOA need a place to park themselves. That’s where wallet comes. Wallet is one stop shop to manage cryptos (Bitcoin, Ethereum, Litecoin etc. etc.)

Another analogy is with Bank. Bank provides unique account number, saving or checking when you open an account. Bank keeps track of your credit/debit transactions. Similarly, when you open a crypto account a bunch of hexadecimal numbers are generated in pair of private and public keys. Public key is what you use to send transactions or provide to others for receiving money. Public key is visible to anyone. Your claim to your public key is through a private key. Anyone can send cryptos to your public account, but to claim this ethers/money private key is needed to unlock an account. Let me give you another analogy so that idea gets cemented and you get an intuition. Your email ids are public and anyone can send an email to you, but only you can open an email through password. In case anyone else knows password, they can see all your Inbox.

Loose private key, you lose all ethers/money. There is no way to recover funds. So, keep private key very private. Your private key is sometimes called mnemonic phrase.

**What is Encryption**

Private/Public keys are nothing, but encrypted version of your plaintext messages. The word encryption comes from Greeks word Krypto’s. The art of encryption is as old as art of communication. At one point of time writing message simply in readable form was enough. As civilizations developed need came to securely transport message from one end to another. Example Romans used Caesar cipher, Caesar code or shift cipher developed by Julius Caesar. It’s was one of the simplest and widely used encryption techniques. It’s a technique in which each letter in the plaintext is replaced by a letter with some fixed number of positions. Example T will be replaced by W in case right shift of 3 is used. C will be replaced by F.

Plaintext: what in the world encryption means

CipherText: zkdw lq wkh zruog hqfubswlrq phdqv

Word Cipher comes from Arabic word sifr, meaning empty or zero.

Encryption is widely used in internet to protect user information being sent between browser and a server. This information may include password, payment or any other personnel information. Let me show you know how to create a simple wallet. Let me little bit explain about Private and Public keys.

Algorithm of deriving Private and Public key is based on Elliptic Curve Cryptography (ECC). Sounds heavy? Let me try to explain at a very high level. The long keys (Private/Public) in Hex format can be generated through multiple ways. The first modern algorithm in the area of public cryptography was developed in 1977 in which Private/Public keys were generated through the multiplication of Prime numbers. This method is called RSA named after 3 men who developed this algorithm: Ron Rivest, Adi Shamir and Leonard Adleman. RSA was a breakthrough technology as first-time asymmetric encryption was developed without worrying about securely transporting secret code. I explained above asymmetric concept. RSA was first step in public key cryptography. RSA is good, but it’s quite calculation intensive and requires a 1,024-bit key to achieve an algorithm. Enter ECC. ECC generates key through properties of elliptic curve equation instead of product of very large prime numbers. ECC can generate 164-bit key with the same level of RSA encryption, but with lower computing power. ECC is getting adapted very fast. Bitcoin as first implementation of Blockchain implemented ECC. Other cryptos followed same model. A small device (Ex: Cell Phone) can make use of ECC due to economical computation performance of ECC. Quite number of IoT devices are adapting to ECC to generate a secure communication.

Read a lot about Public and Private key until you get an intuition. It took me some time to understand, but once meaning is grasped you will be able to connect many dots. One [article](https://medium.com/@vrypan/explaining-public-key-cryptography-to-non-geeks-f0994b3c2d5) I really liked. There are tons of small videos on You tube. They will help you in getting a concept.

**MyEtherWallet (MEW)**

There are multiple sites you can create a wallet. Let me show you one of such Wallet [MyEtherWallet](https://www.myetherwallet.com). Follow below steps

1. Site will pop first few information messages about MyEtherWallet and in Blockchain in general. You can choose to read or press X to close
2. Click “New Wallet” which is a first menu option on top left corner
3. Create New Wallet screen appears. Enter a password.
4. Press button Create New Wallet
5. Download and save KeyStore file in next screen. File name is long starting with UTC--. Contents of this file can be viewed in notepad
6. Once file is downloaded **I understand. Continue** will activate allowing you to go to next screen
7. Next screen will show Save Your Private Key. This is your secret key which lets you control your account i.e. Public Key.
8. Print Paper Wallet button in green print reveals your Public and Private keys

What is purpose of Key store file and password? Use case of key store file is to safeguard your private key. When you need to unlock your account for the purpose of transaction (send or receiving ethers), key store file is needed. Private key is deduced from key store file and lets you sign the transactions. Read [this](https://medium.com/@julien.maffre/what-is-an-ethereum-keystore-file-86c8c5917b97) article to gain more insights in Key store file

Few quick important points about Private & Public keys

**Public and Private key are 256 binary digits shown as 64 Hexadecimal digits**

**Public key is derived from Private key. One cannot reverse Public key and derive Private key. In case that would have been possible than whole meaning of private key is meaningless. That’s why it’s a one-way function. A simple analogy is egg once broken its yolk cannot be put back into the egg.**

**Pairing of Private and Public key is asymmetric encryption. Example:**

1. **Bob sends money to Alice and encrypt using its private key and Alice Public key**
2. **Alice decrypts message with its own private key. Alice is able to decrypt because initial encrypted message contains Alice Public key. Had Public key would have belonged to someone else, Alice wouldn’t have been able to decrypt**

One of the advantages of Myetherwallet is you don’t have to download complete Ethereum node which can take long time and occupy space in your computer. There is an official Ethereum Wallet like [Mist](https://www.cryptocompare.com/wallets/ethereum-wallet-dapp/) which needs to be created on top of local Ethereum node. This means you will have to download full node. Private key can be ported between MyEtherWallet and Mist Browser. Remember Private key you stored in KeyStore file? KeyStore is an encrypted version of your Private key.

Advantage of Mist is it’s also a Dapp browser and a multisignature. In other words, it’s a wallet with multiple accounts, multiple owners and with multiple private keys. Risk of loosing money in a multisig wallet is much less than a wallet with single private key. [Here](https://coinsutra.com/best-multi-signature-bitcoin-wallets/) is nice explanation of multisig wallet.

DApp stands for distributed applications. To interact with an Ethereum smart contracts through front end apps, web 3.0 protocol is needed. MetaMask provides Web 3.0. It’s a Chrome browser extension developed by google. MetaMask is not only Wallet, but also when installed injects web 3.0 in Chrome so that front end Dapps can be designed and tested. In previous article (Link) I showed Web3 module usage for deployment of Smart contract, but that required reference to web3 module. For a novice user who does not understand web3 and just want to send/receive ethers, MetaMask comes into play. MetaMask can let user either plainly transact ethers or interact with Smart Contract through Chrome Browser. In summary MetaMask is a bridge between your browser and Ethereum blockchain.

MetaMask belongs to Hierarchical Deterministic (HD) wallet family. What is HD?

You remember in above MEW steps a private key was generated and its encrypted version gets stored in a KeyStore file. In case you need to have another account, a similar process is needed in MEW for generation of private key which in turns create another paper wallet or KeyStore file. When complexity of transactions increases where you may need to store them in multiple account having multiple private keys or KeyStore files is a cumbersome. Here comes HD wallets to make life easy. In HD wallets private keys are determined (Hence deterministic) behind the scenes through a seed key. This seed key is composed of 12 or 24 words. Seed is also called Mnemonic code. This seed is itself a private key. From this Key multiple private key are determined in a hierarchical (Hence hierarchical) manner. Loosing seed is not an option just like any other private key. This seed is initially generated by wallet. I have made up below seed in bold just to show how it appears.

This is a

Seed example just

To show you

how seed looks

Here is nice [article](https://coinsutra.com/hd-wallets-deterministic-wallet/) about HD. You will see a real Seed generation during account setup in MetaMask.

I can show step by step installation and account setup for MetaMask, but it is so simple that I can just refer to tons of material on web. Here is an [article](https://medium.com/cryptostrikers/getting-started-how-to-install-metamask-4a2d9c18b4cc) on how to install and setup MetaMask. Moreover, you can always install/uninstall MetaMask with no hassles.

In case you are developing and testing Dapps, MetaMask can interact with local blockchain (Ganache) environment, Rinkeby testnet or real Ethereum network.

**MetaMask Security**

MetaMask is locked by default. During the course of transaction, MetaMask needs to be unlocked. This may expose to a possible phishing attack as MetaMask stores private key in a browser local storage. In case multiple tabs are open hacker can steal your private key by popping a page informing you that transaction did not go through. This may force you to unlock MetaMask by entering your password. Hacker have now access to your wallet. Best way to do transaction in MetaMask is to do through a single tab. So, is MetaMask secure? Anxiously yes. It is as secure as users are. In case you are trying to download a movie from an illegal web site and MetaMask is unlocked than you are responsible for the safety of your Ethers.

Different wallets developed just make life easy in terms of generating and managing accounts. One can generate its own private keys using various ways. That requires some technical skills. Here is one [article](https://medium.freecodecamp.org/how-to-generate-your-very-own-bitcoin-private-key-7ad0f4936e6c) I liked.

There are hardware wallets too. They are like USB, removable storage devices. They are also called cold storage because they keep your private key offline. One should always store cryptos in different wallets. In case one gets hacked or stored then at least you will have a backup. In next article I will show how to deploy to Rinkeby testnet using HD wallet and Infura API.