Public Key Cryptography

1. Bitcoin is an open message system which is secured by Public Key Cryptography
2. In contrast to other systems which are secured by username and password Bitcoin is secured by **digital message Signature created with a unique private Key.**

Problem Solved by Private Key**:**

Bitcoin solve both the problem by a system known as Public Key Cryptography.

This system used two pieces of information to authenticate the message.

1. **Public Key is used to identify the sender and receiver and can be distributed to others**
2. **Private Key is used to create an unforgeable signature**

1. **Public and Private are key are linked through a signature algorithm, a mathematical procedure for creating identities, signing message and validating signature.**

Six Things are important about Private key:

1. A Private Key is Just a number.
2. Transactions are messaged signed with a Private Key.
3. Anyone who knows your Private Key can steal your funds.
4. A Private key generate the Public Key which generate an address.
5. Security depends on Choosing Good Private Key.
6. Private Keys are (Somewhat) Portable

1. A Private Key is Just a number.

A bitcoin Private key is simply an integer **between one and 10^77.**

**Counting 1 Trillion Private keys per second will take more than one million times the age of this universe.**

**Even worse Just enumerating these keys would consume the total energy of the Sun for 32 Years.**

**What is This number?**

This number is so large it’s difficult to understand.

5DFKNKFNKDN5FDKBKFHIWHISNDK8SDSDSF7SSMNKSSBVBVVGSBVVCBVVCVGVN

* In Bitcoin WIF (wallet Import Format) is introduce which convert this number into a compressed String.
* The result of this string is start from a number **5.**
* This compressed key can also be more compressed but this time the string will start from number **6.**

2.Transactions are messaged signed with a Private Key.

* To prevent any forgery Bitcoin requires that each transaction bear a digital signature. This digital Signature is just a number from a very large range like private key. Wallet Software generates a signature by mathematically processing a transaction together with the correct Private Key.
* Anyone with a signature and Public Key can easily authenticate the message. However, the only way to produce a valid message signature is to use the Private matches with the Published Public Key. In other word digital signature are practically impossible to forge

3.Anyone who knows your Private Key can steal your funds:

4.Private Key Generate the Public Key which generate the Address

**ECC (Elliptic Curve Cryptography)** is a method which is used to apply on **Private key** to generate the **Public Key**, on **Public Key** **multiple hashing algorithm** is applied to generate the **address** of **bitcoin**.

**Private key** is the integer whereas **Public key is a 2D coordinate composed** of two **integers.** To make a Public Key easier to process it can be transformed into a **single value.**

* One approach appends the y-coordinate to the x-coordinate. This technique produced an **uncompressed Public Key.**
* **A compressed Public Key** uses only the x-coordinate with a symmetric flag.

Notice that no **network** is **needed** at any point in the **generation of** a **private key** or the corresponding address. Every computer on the **Bitcoin network** knows about the mathematical relationship between public and **private keys**

<https://bitzuma.com/posts/six-things-bitcoin-users-should-know-about-private-keys/>

**Sweeping keys Problem?**

Multiple keys needs backup which is difficult task. For example if a user sends 1 bitcoin out of 2 and it received back 1bitcoin in its output when user takes the backup it receive empty amount in its first address so this is the issue which occur in multiple keys backup.

This issue is resolved by HD Wallet(**Hierarchical determinist**ic )

HD wallet have a master key which is linked by all private keys. When a user a want a backup of private keys he just has to take the backup of master key which will recover all the private keys.