BLOCKCHAIN TUTORIAL 15

Convert public, private key pairs to addresses

BLOCKCHAIN TUTORIAL 15

Convert public, private key pairs to addresses

CONVERT PUB, PRIV KEY PAIRS TO ADDRESSES

- Social Security numbers or bank account numbers are just identification numbers and have no other function but to identify individuals for the purposes of Social Security or banking.

- A public key however has a corresponding private key which are mathematical linked to each other. These keys are used to create a transaction between parties by encrypting and decrypting data with these keys.

- The randomly generated **private key** and the calculated **public key** are converted into a **private address** and **public address**.

- More information about private and public keys, see the Elliptic Curve Key Pair Generation video, part 11 of the Blockchain tutorial series.

CONVERT PUB, PRIV KEY PAIRS TO ADDRESSES

- There can be many reasons why a public and private key pair are converted into differently looking public and private addresses, for example:
  - implement checksum digits in addresses to detect mistyping of the addresses.
  - implement version number in addresses to differentiate between similar blockchain implementations (Bitcoin, Litecoin) or environments (Bitcoin, Bitcoin-Testnet).
  - apply base-58 encoding to addresses to avoid mistyping of the addresses.
  - apply hash algorithm to addresses to reduce the address sizes.
- In a later video I will demonstrate how to create a Bitcoin private and public address starting from a randomly generated number.