Mechanics of Bitcoin (2)

Cryptographic Keys, Addresses, Wallet

Prof. James Won-Ki Hong

Distributed Processing and Network Management (DPNM) Lab.
Dept. of Computer Science and Engineering
POSTECH
Pohang, Korea

http://dpnm.postech.ac.kr
jwkhong@postech.ac.kr

Table of Contents

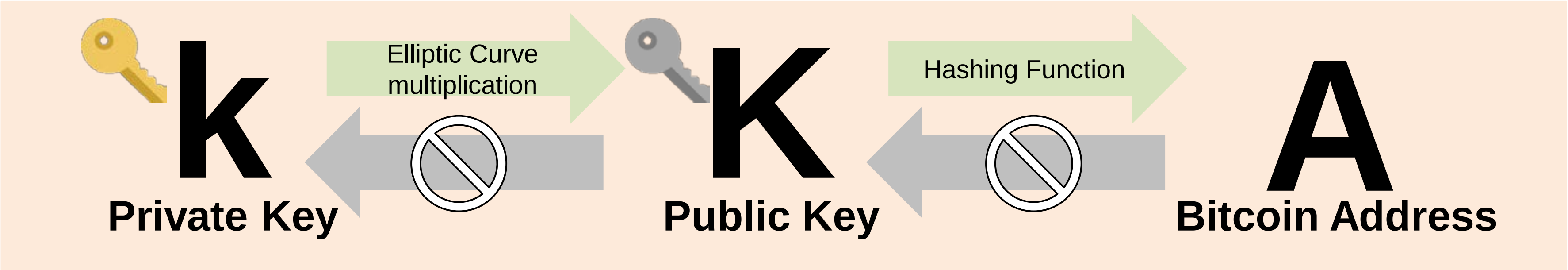
- Cryptographic Keys & Bitcoin Address
- Wallet

Relationship between Keys & Bitcoin Address (1/4)

- **Digital Keys**

	Public Key	Private Key
Similarity	Bank Account	Secret PIN number
Usage	Receive Bitcoin	Transfer Bitcoin
How to generate	Elliptic Curve Cryptography	Random Digit Extraction

- **Bitcoin Address**
  - An object to receive a bitcoin
  - In most cases, Bitcoin address is generated from the Public Key
- **Relationship between Keys and Address**



Relationship between Keys & Bitcoin Address (2/4)

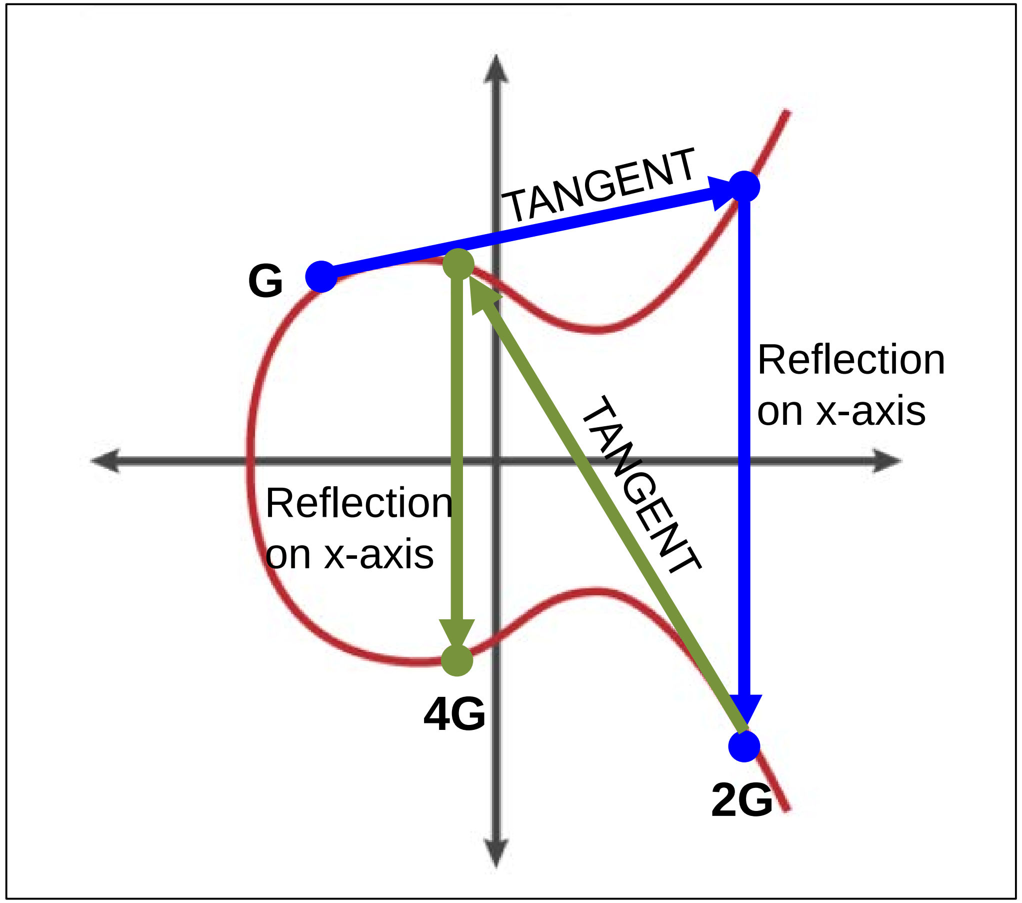
Generating Private Key

- Random Digit Extraction
  - Randomly selects a number between 1 and 2^256
- Encode with Base58Check
  - Express a long string of numbers in a condensed way
  - Base58: text-based binary encoding format developed for use in Bitcoin and other cryptocurrencies
  - Use Capital letter, small letter and number except 0(number), O(capital letter of o), l(small letter of L), I(capital letter of i)
  - Checksum: prevents the wallet software from accepting the incorrectly entered Bitcoin address as a valid destination

Relationship between Keys & Bitcoin Address (3/4)

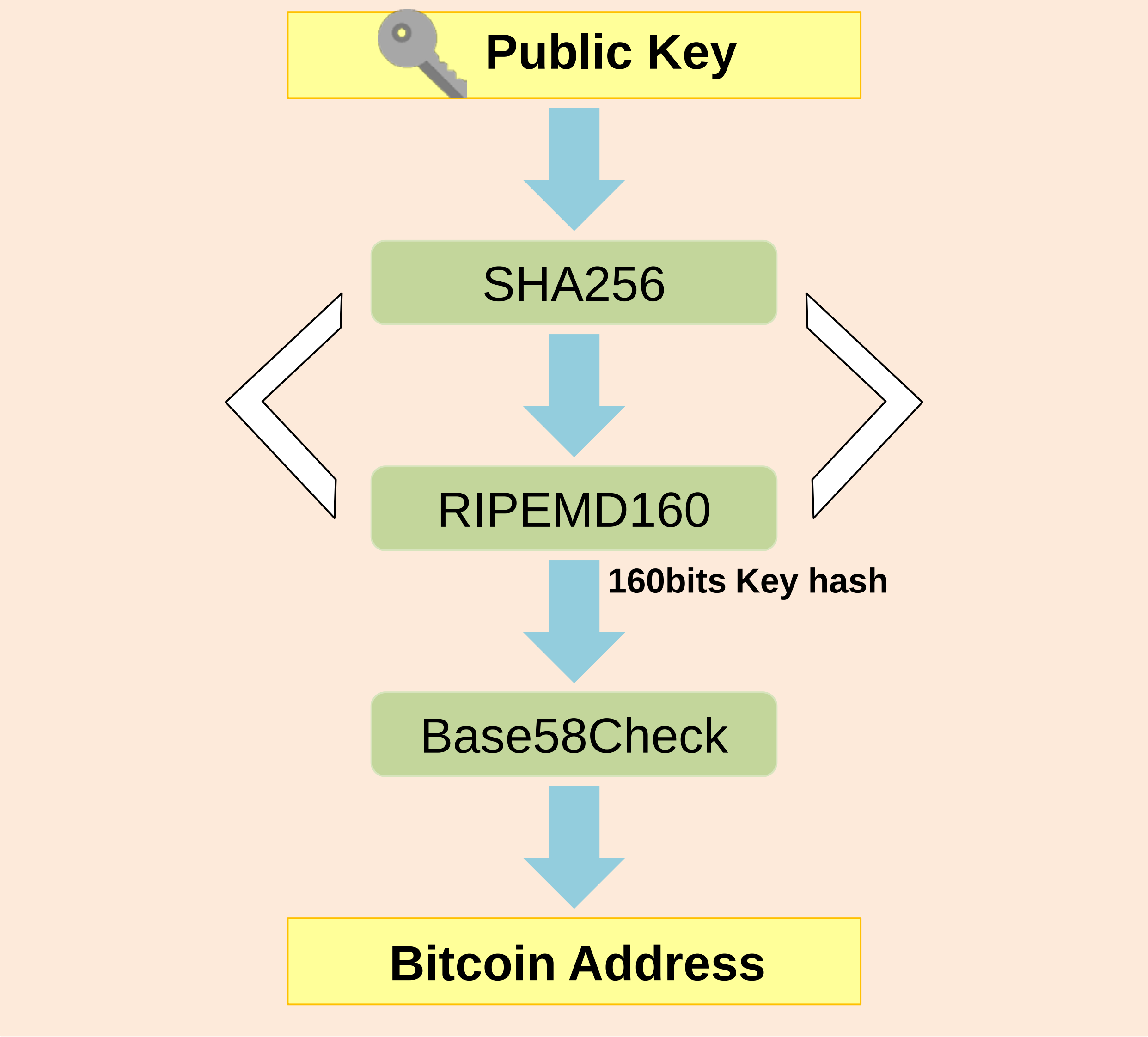
Generating Public Key

- Elliptic Curve Cryptography
- K = k * G
  - k: Private key
  - G: Generation point
  - K: Public key
- K = (x, y)
- Irreversibility
  - It's infeasible to switch to a private key using public key



Relationship between Keys & Bitcoin Address (4/4)

- **Public Key to generate Bitcoin Address**



Wallet (1/3)

What is a Wallet?

- Simple data base which stores pairs of Private key and Public key

Basic functionality of Wallet

1. Generate Private key
2. Generate Public key from Private key
3. Generate Address using Public key
4. Transfer Coins
5. Broadcast transaction to Blockchain network

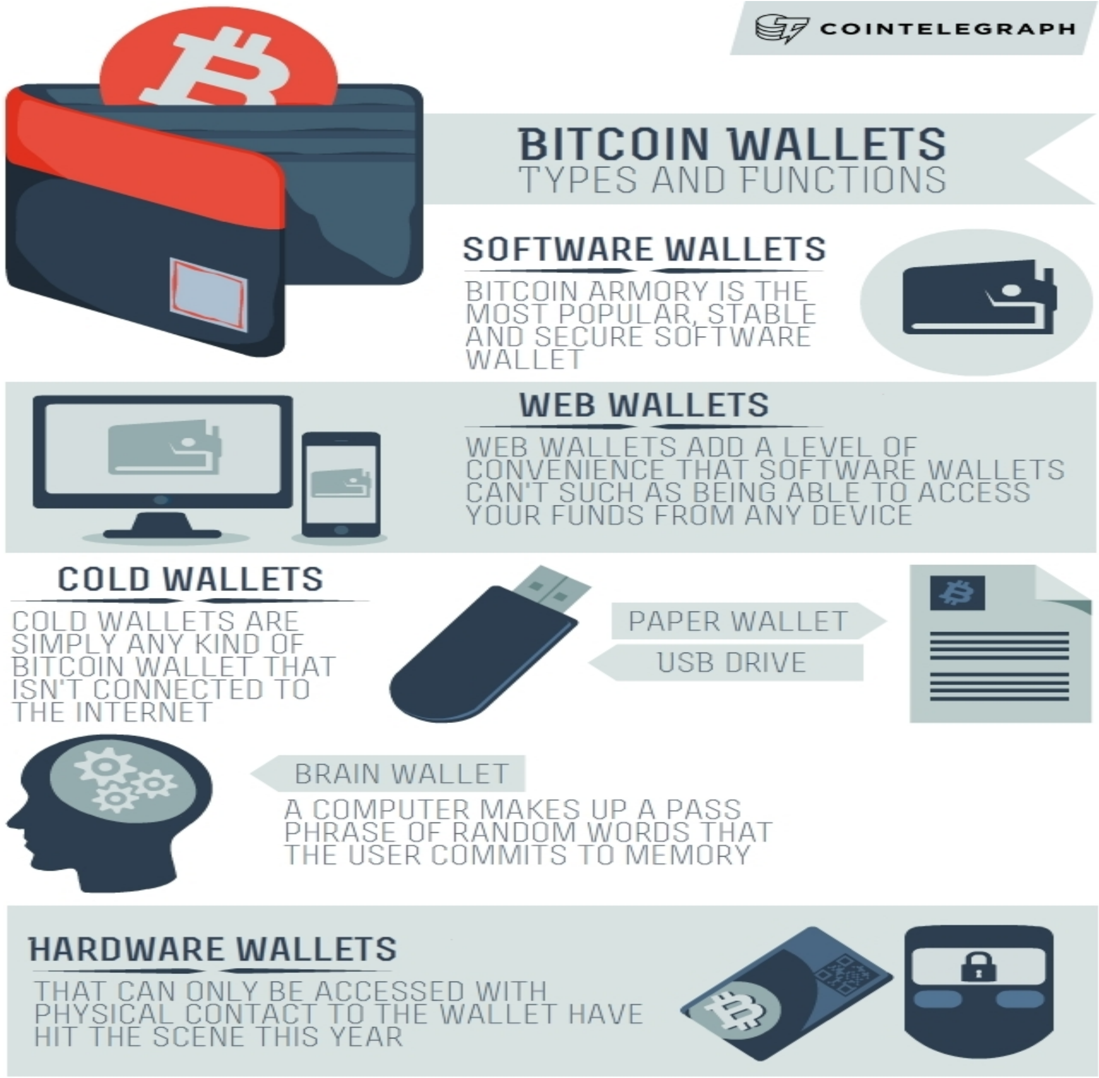
Wallet (2/3)

Types of Wallet (1)

- **Nondeterministic (randomness) Wallet**
  - Contain randomly created Keys
  - Just a Bunch of Keys
  - Complex to manage, back up or retrieve data
  - Wallet should be backed up frequently
- **Deterministic (seed) Wallet**
  - Contain private keys from common seed using one-way hash functions
  - Only back up them once at a specific time
  - Even among different kinds of wallets, all of the users' keys can move easily
- **Hierarchical Deterministic (HD) Wallet**
  - Contain keys generated from a tree structure
  - A tree structure can be used to represent organic meaning, such as when a particular branch consisting of sub-keys for receiving money is used
  - Users can generate a public key without accessing a private key

Wallets (3/3)

- **Types of Wallet (2)**



COINTELEGRAPH

BITCOIN WALLETS
TYPES AND FUNCTIONS

SOFTWARE WALLETS

BITCOIN ARMORY IS THE MOST POPULAR, STABLE AND SECURE SOFTWARE WALLET

WEB WALLETS

WEB WALLETS ADD A LEVEL OF CONVENIENCE THAT SOFTWARE WALLETS CAN'T SUCH AS BEING ABLE TO ACCESS YOUR FUNDS FROM ANY DEVICE

COLD WALLETS

COLD WALLETS ARE SIMPLY ANY KIND OF BITCOIN WALLET THAT ISN'T CONNECTED TO THE INTERNET

PAPER WALLET

USB DRIVE

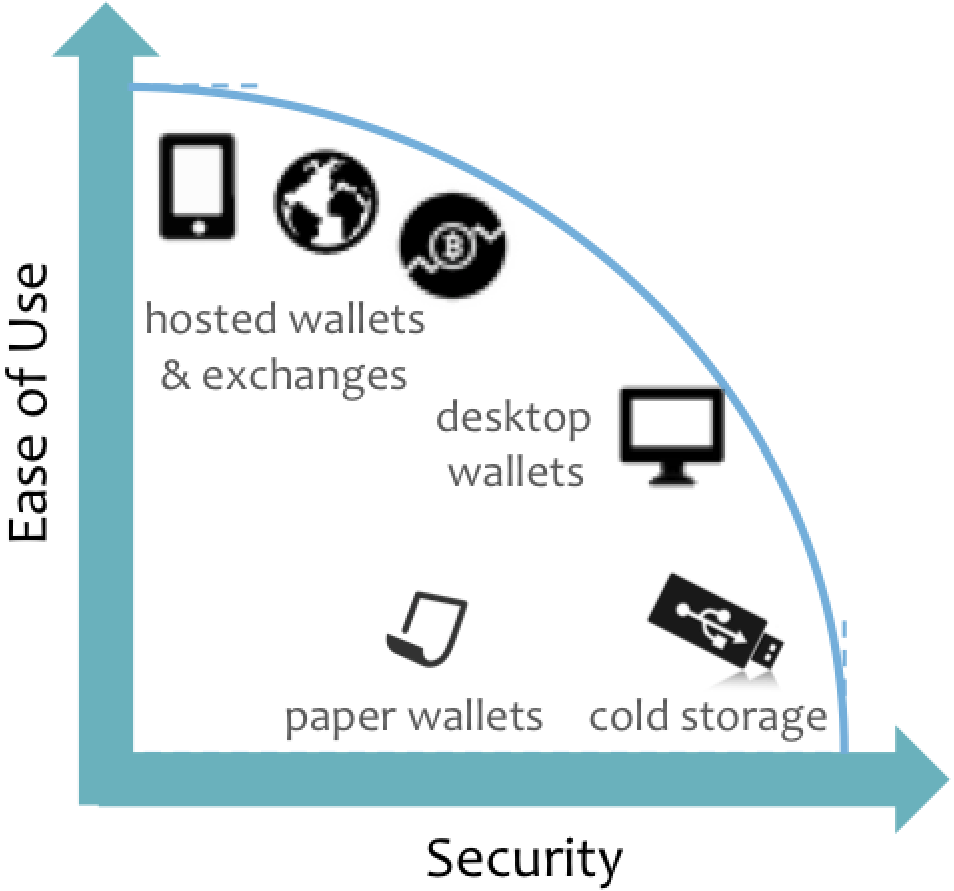
BRAIN WALLET

A COMPUTER MAKES UP A PASS PHRASE OF RANDOM WORDS THAT THE USER COMMITS TO MEMORY

HARDWARE WALLETS

THAT CAN ONLY BE ACCESSED WITH PHYSICAL CONTACT TO THE WALLET HAVE HIT THE SCENE THIS YEAR

Source: https://cointelegraph.com/storage/uploads/view/df5b95e155ca91306394db1c659c87a6.jpg



Source: https://i.stack.imgur.com/6ZCyt.png

Summary

- **Relationship between keys and Bitcoin address**
  - **Generating Private Key**
  - **Generating Public Key using Private Key**
  - **Public Key to Bitcoin Address**

- **Wallet**
  - **What is a Wallet?**
  - **Types of Wallet**

References

- Andreas M. Antonopoulos, **Mastering Bitcoin,** O'Reilly, 2014
- https://steemit.com/kr/@icoreport/key-2-ecc
- https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
- https://www.youtube.com/watch?v=-gZe4M-WZV4
- https://en.bitcoin.it/wiki/Paper_wallet