Mastering Bitcoin Ch2-Ch4

Agenda

- How Bitcoin Works?
- Bitcoin Core: The Reference Implement (Installation guide)
- Keys, Address

How Bitcoin Works?

Buying a Cup of Coffee

- Alice has 0.1 BTC (10,000,000 Satoshi)
- Buying a cup of coffee costs 0.015 BTC
- Flow:
  - Alice send a transaction to Bob.
  - After Bob verifying the transaction, Alice got a cup of coffee.

1 BTC = 10^8 Satoshi

Transaction Input: Payment Request

- Bip-21 Format:
  - A URI scheme for making Bitcoin payment
  - easily make payments by simply clicking links on webpages or scanning QR Codes.

```
bitcoin:1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA?
amount=0.015&
label=Bob%27s%20Cafe&
message=Purchase%20at%20Bob%27s%20Cafe

Components of the URL

A bitcoin address: "1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA"
The payment amount: "0.015"
A label for the recipient address: "Bob's Cafe"
A description for the payment: "Purchase at Bob's Cafe"
```

[Bitcoin Improvement Proposals (BIPs)]

Transaction

- Alice's transaction
- Input: Alice’s address
- Two outputs:
  - Pay to Bob.
  - Pay to herself for change. (pay to change address)
- Transaction fee:
  - Fee = Total Input - Total Output

Bob’s View

- Should Bob waits for bitcoin network to confirm the transaction?
  - A merchant may accept a valid small-value transaction with no confirmations, with no more risk than a credit card payment made without an ID or a signature, as merchants routinely accept today.

Discussion of Transaction

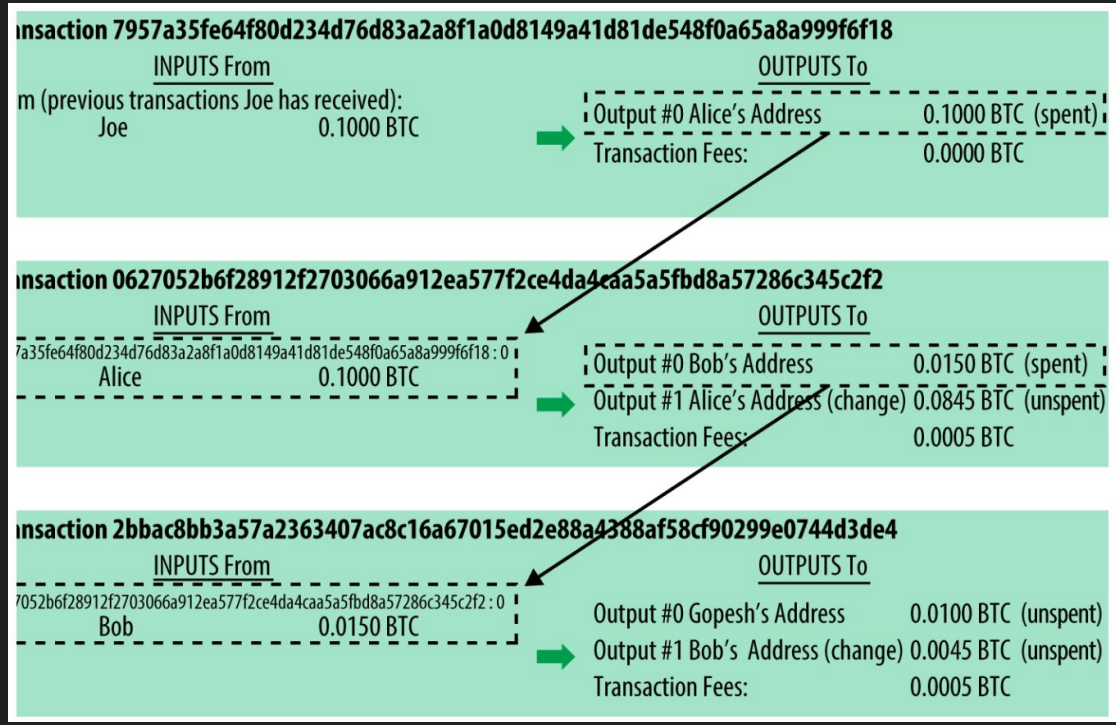
- What is wallet software
  - Lightweight client: Keep track of all the available outputs belonging to addresses in the wallet
  - No copy: Ask a full-node using an application programming interface (API) call
  - Aggregate many small inputs, or use one that is equal to or larger than the desired payment.

```
$ curl https://blockchain.info/unspent?active=1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
```

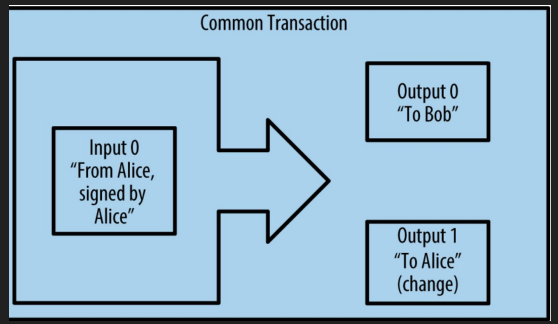

```
{
        "unspent_outputs":[
                {
                        "tx_hash":"186f9f998a5...2836dd734d2804fe65fa35779",
                        "tx_index":104810202,
                        "tx_output_n": 0,
                        "script":"76a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac",
                        "value": 10000000,
                        "value_hex": "00989680",
                        "confirmations":0
                }
        ]
}
```

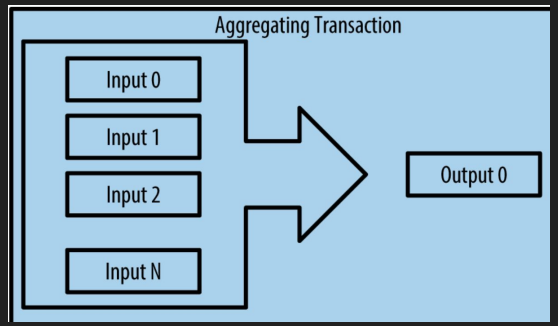
More and More Transaction: Transaction Chains

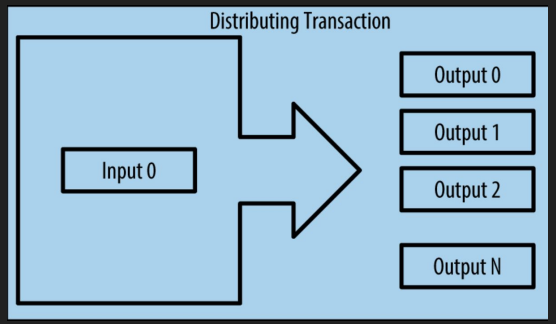
- Alice gets bitcoin from Joe.
- Alice buys a cup of coffee.
- The inputs from the latest transaction correspond to outputs from previous transactions.



Bitcoin Transaction Types







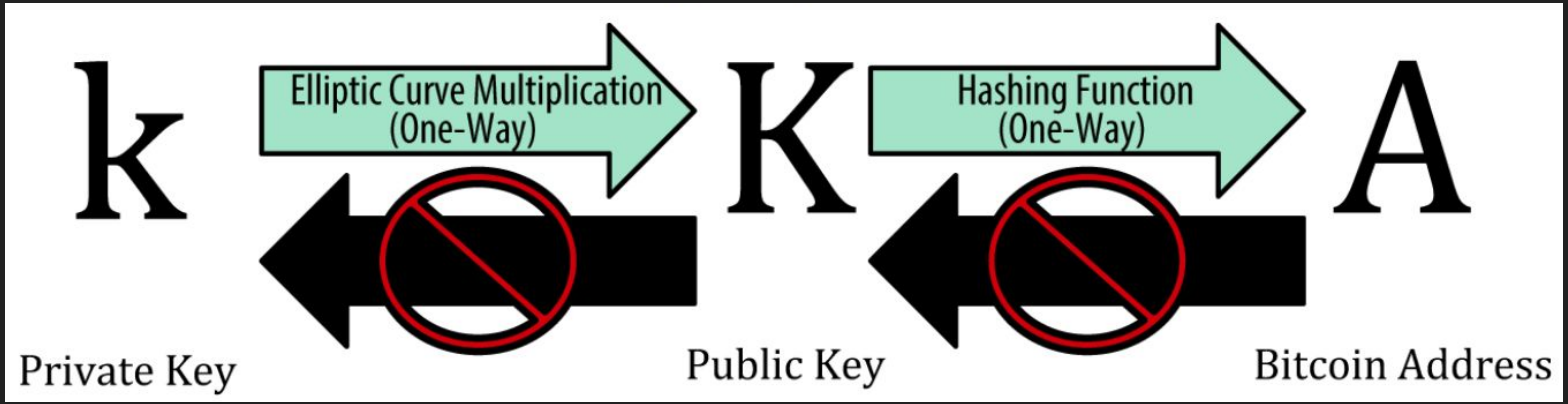
Keys, Address

What are Key Pairs Doing in Blockchain Tech

- Provide:
    - Decentralized trust
    - Control
    - Ownership attestation
- Cryptography is not an important part of bitcoin.

How to Generate Key Pairs

- Pick a *random* number as a private key
- Use elliptic curve multiplication to generate public key from private key
- Use hashing function to get address



How to Generate Private Key

- The private key is a number between 1 and 2^256 -1 (*256 bits)
- Generate it by using:
  - Toss a coin 256 times (manually)
  - Feed a larger string of random bits into the SHA256 hash algorithm.
  - Do not use ***simple*** random algorithm.

* 256 nits is defined as the order of the elliptic curve

Encrypted Private Key(Bip-38)

- Motivation: safely store in the wallet.
- User needs Password to activate the wallet.

Public Key

- Elliptic curve multiplication:

  K = k * G

  K: public key; k: private key; G: generate point

- k can be reversed by brute-force searching

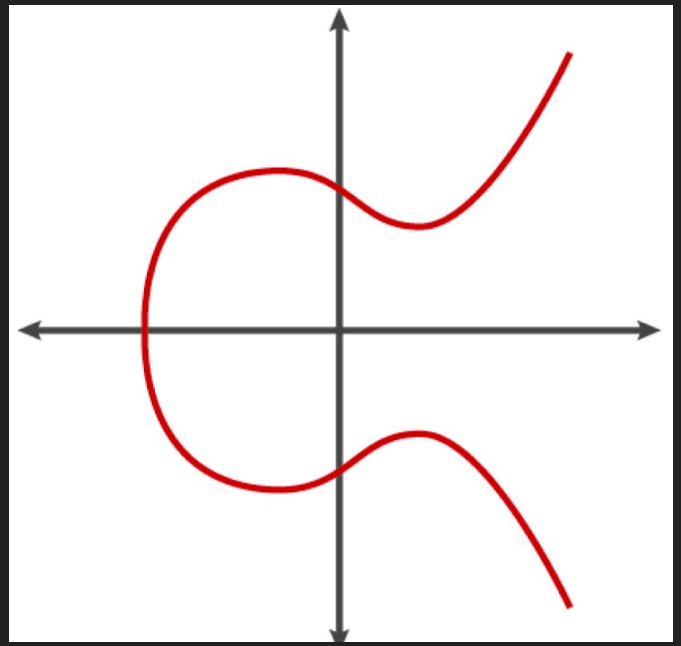
Elliptic Curve Cryptography

- The **secp256k1** Elliptic Curve:

  $y^2 = (x^3 + 7) \bmod p$

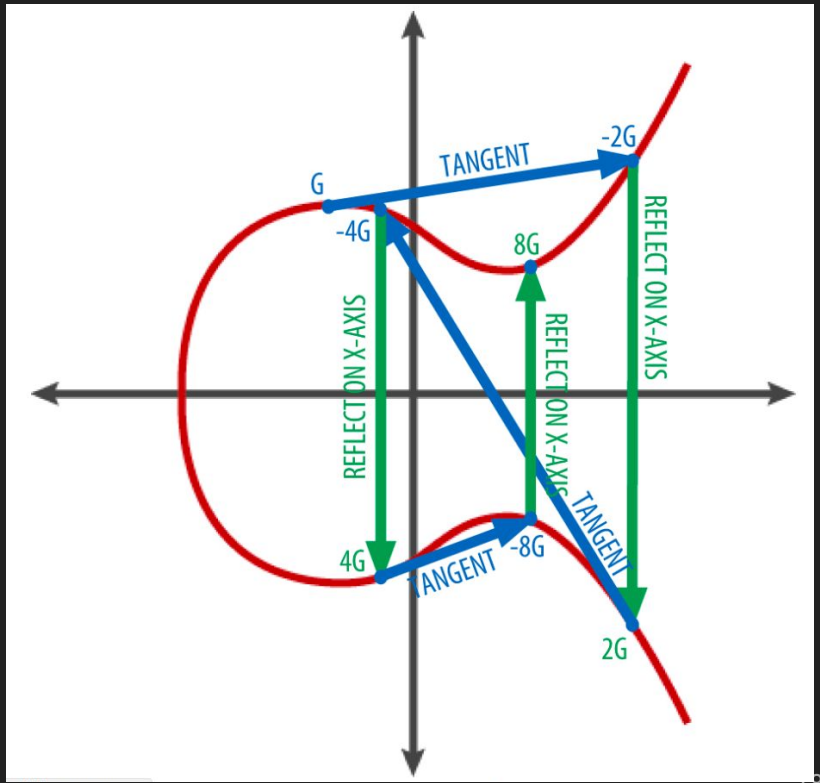
  $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

- Addition operator **+** in F_p
  - P3 = P1 + P2 is defined as:
    - Draw a line L between P1 and P2
    - P3’ is the only one point that L intersect the elliptic curve
    - P3 is the reflect of P3’



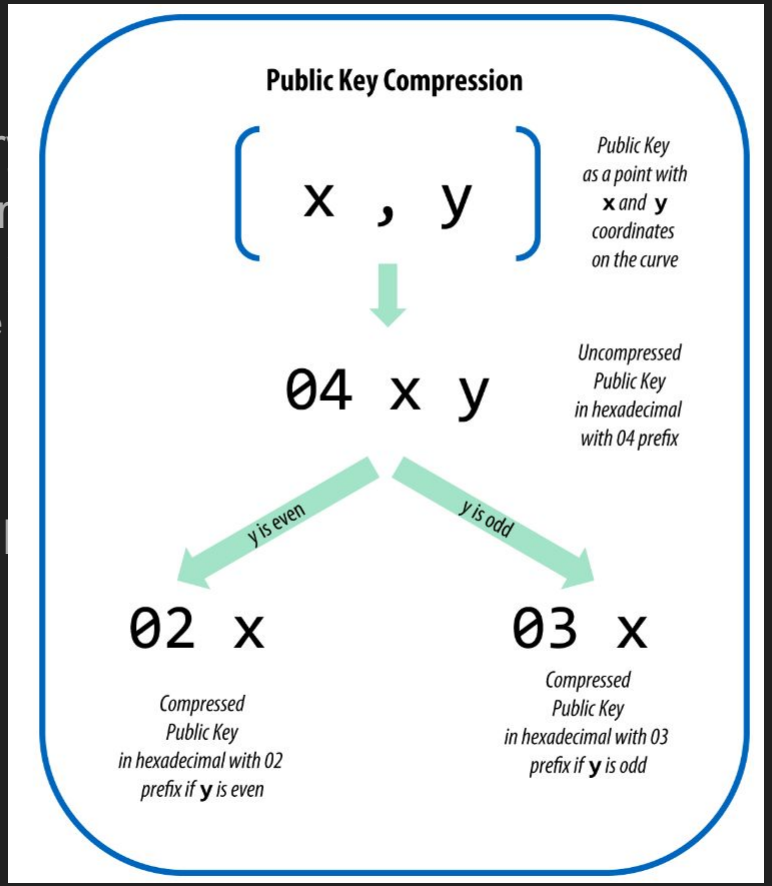
Example

- K = k * G
  - K = G + G + G + ….
  - If P1 and P2 are the same point, L is extend to be the tangent on the curve.
- The steps of generating public key:
  - Draw a tangent line L on the point
  - Find where L intersects the curve to derive P’
  - Reflect P’ on the x-axis to get next P
  - Finish util k times
  - The public key is: **(04 x y)**
    - Where 04 is prefix, (x,y) is the coordinate of K



Compressed Public Keys

- Motivation: reduce the storage size in ever
- Compressed public key: prefix + the x coor
  - The y Coordinate can be derived by (y^2 mod p
  - The problem is y can be positive or negative(use
    - We use prefix to store the sign of y
      - 02: even number
      - 03: odd number
- How to deal with one private key to two pu
  - The bitcoin regards two public keys are different!



Compressed Private Keys???

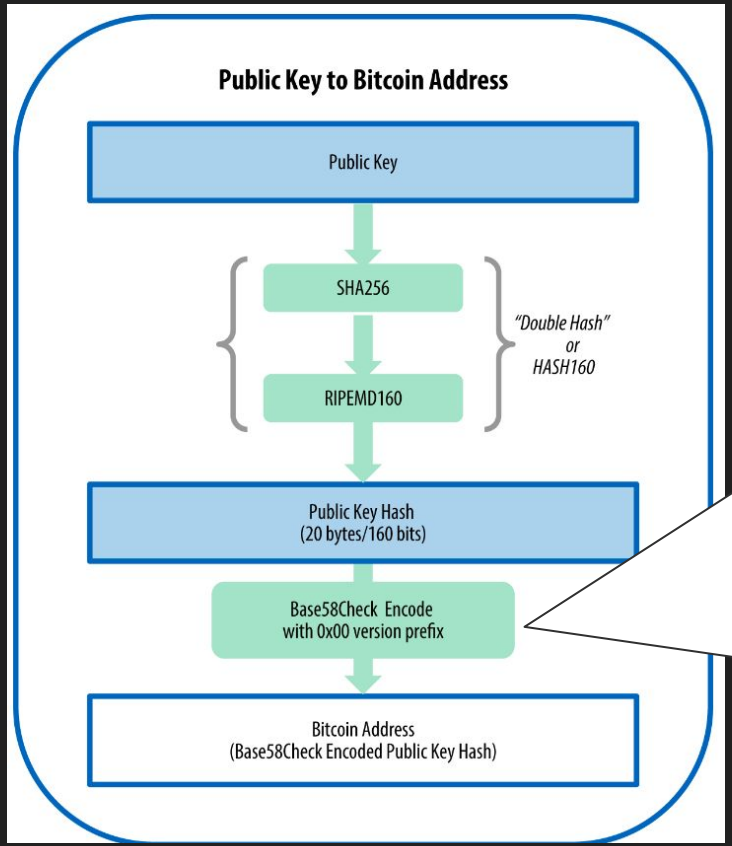
- No real "COMPRESSED” Private keys.
- The compressed private key is the private key with a suffix to signify that the compressed private key should only be used to produce compressed public key.

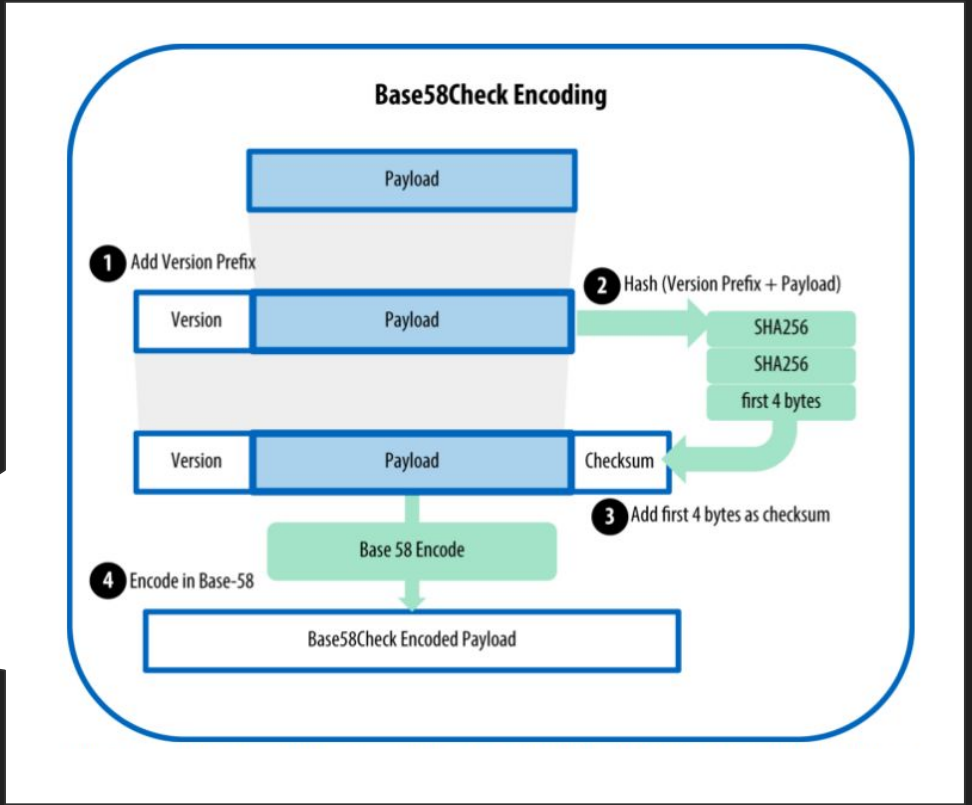
Format	Private key
Hex	1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD
WIF	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn
Hex-compressed	1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD01
WIF-compressed	KxFC1jmwwCoACiCAWZ3eXa96mBM6tb3TYzGmf6YwgdGWZgawvrtJ

Bitcoin Address

- Bitcoin address is not the same as a public key, but it is derived from a public key using one-way function which is called pay-to-public-key-hash (P2PKH).
- Bitcoin addresses are always encoded as Base58Check.
  - Base58 = Base64 - {“0”, “O”, “l”, “I”, “+”, “/”}
    - Base64: 26 lower and capital letters, 10 numbers, “+”, “/”
  - Base58Check = Base58 + error-checking code
    - Error-checking code is derived from the hash of the encoded data and can be used to detect and prevent transcription and typing error.

Bitcoin Address Flowchart





Further Reading

- Pay-to-script-hash(P2SH)
- Vanity addresses (special pattern addresses)