Design and Analysis of Cryptocurrency Wallets

Guided By: Dr. Stanisław P. Radziszowski

Presented By: Ankush Kawanpure

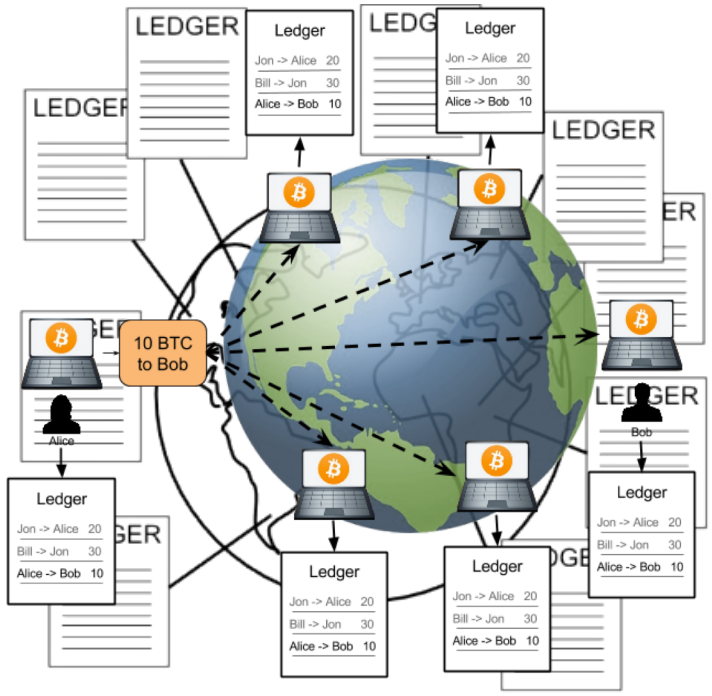
Outline

1. **What is cryptocurrency?**
2. Importance of wallets
3. Types of wallets
4. Hierarchical deterministic wallets
5. Demo
6. Future work

What is Cryptocurrency

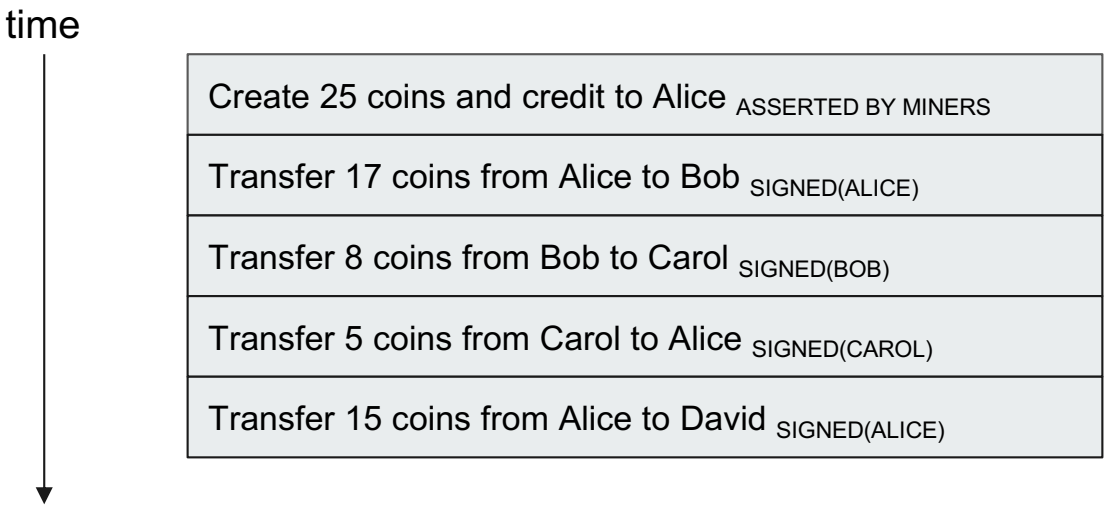
Definition:

- At the core, it's an open ledger keeping track of account balances
- Copy of ledger maintained across the nodes in the network



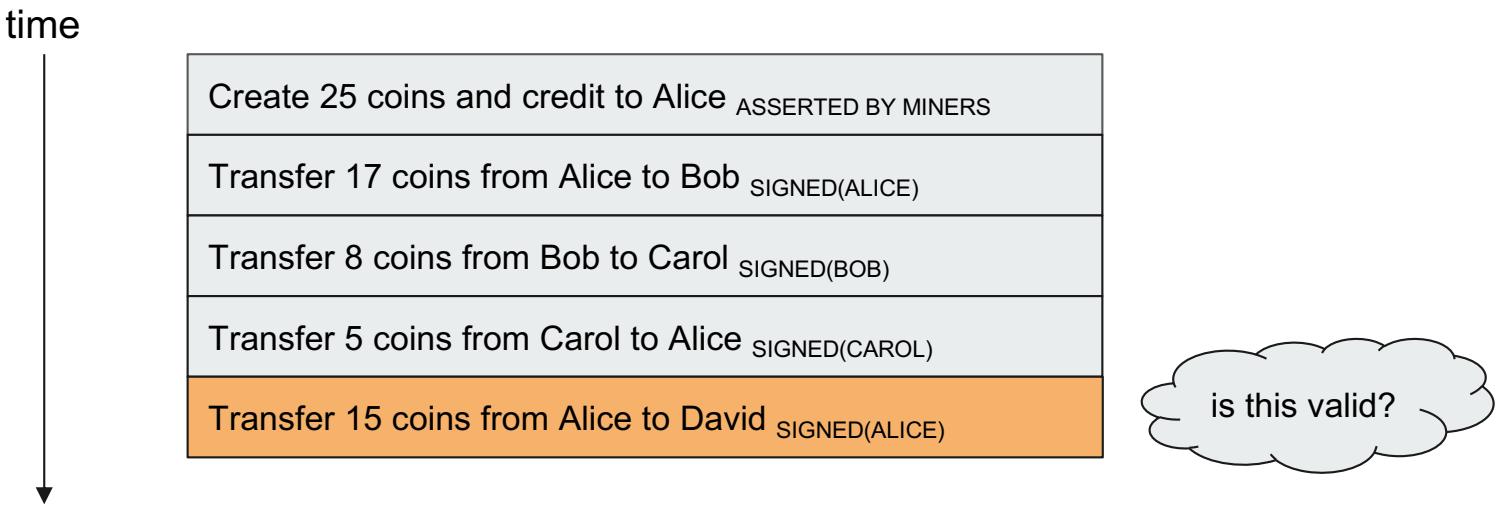
Distributed Ledger

Account based ledger (Not - Bitcoin)



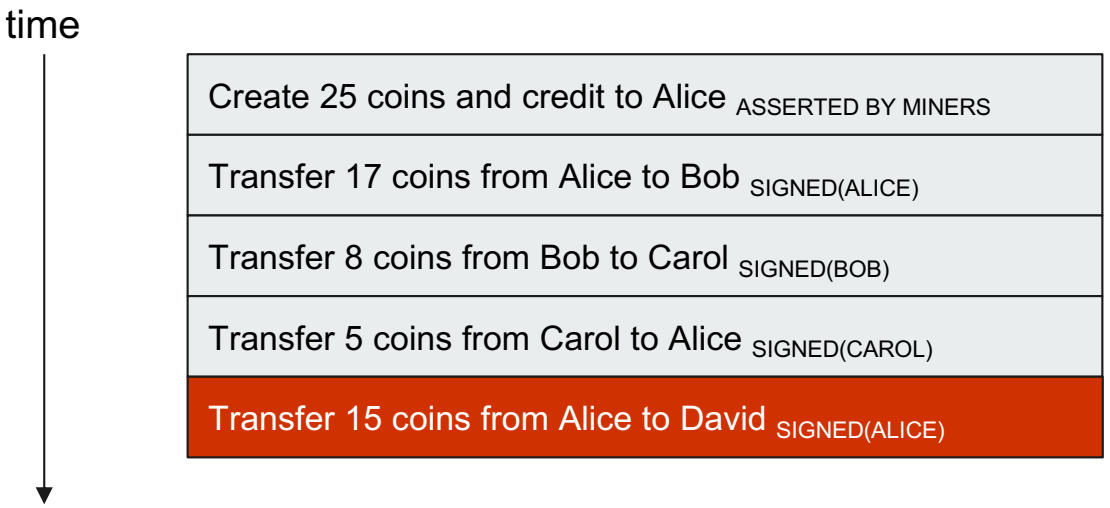
Distributed Ledger

Account based ledger (Not - Bitcoin)



Distributed Ledger

Account based ledger (Not - Bitcoin)



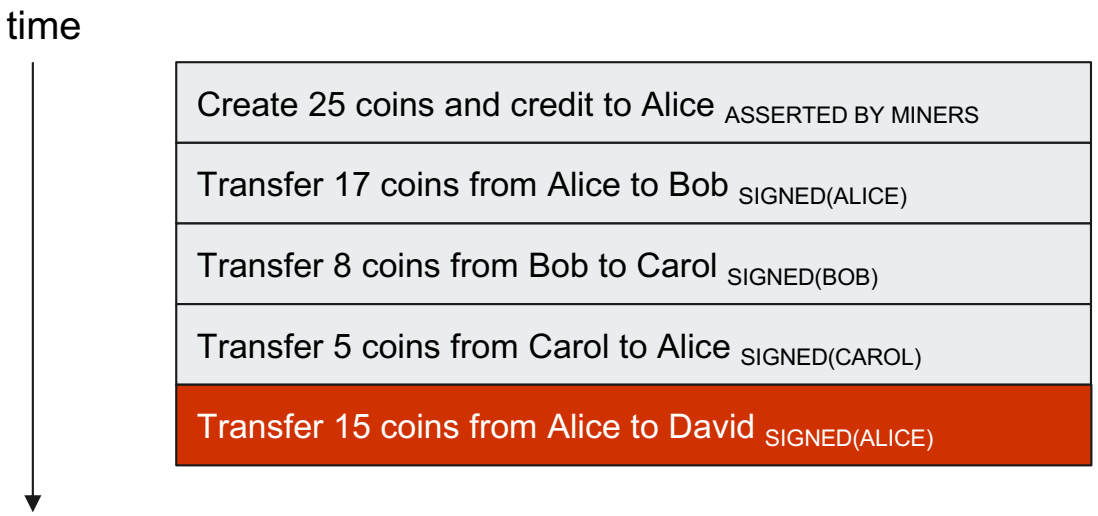
Account	Value
Alice	13?
Bob	9
Carol	3
David	?

Distributed Ledger

Account based ledger (Not - Bitcoin)

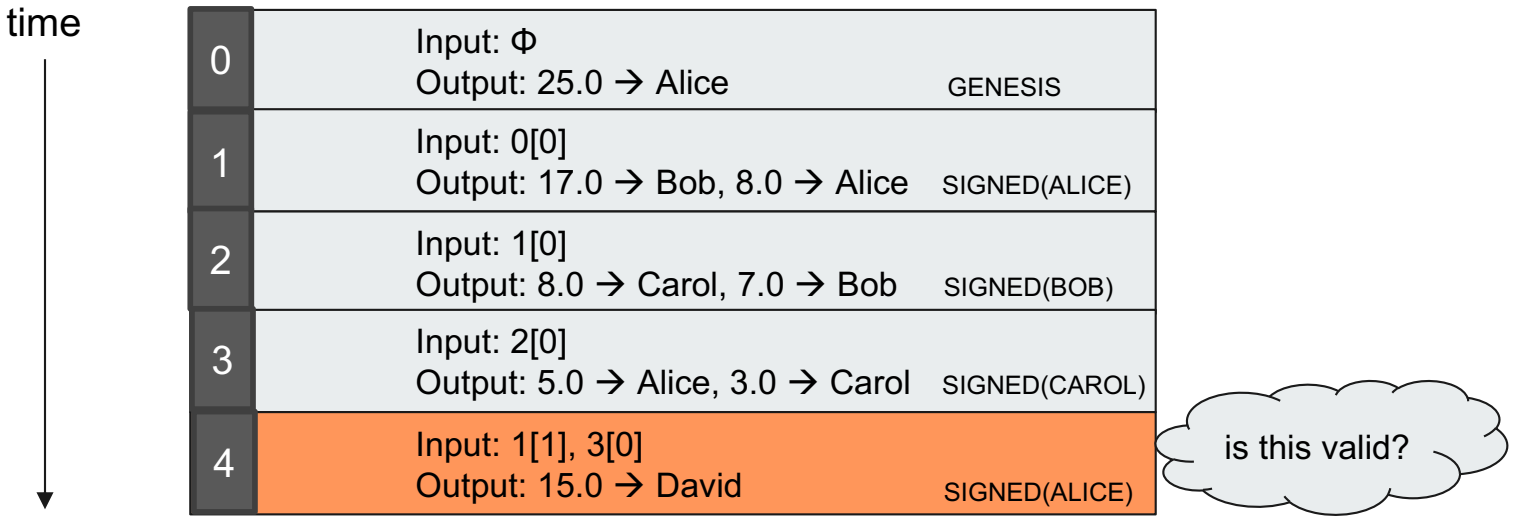
Problems:

- Validity
- Authenticity



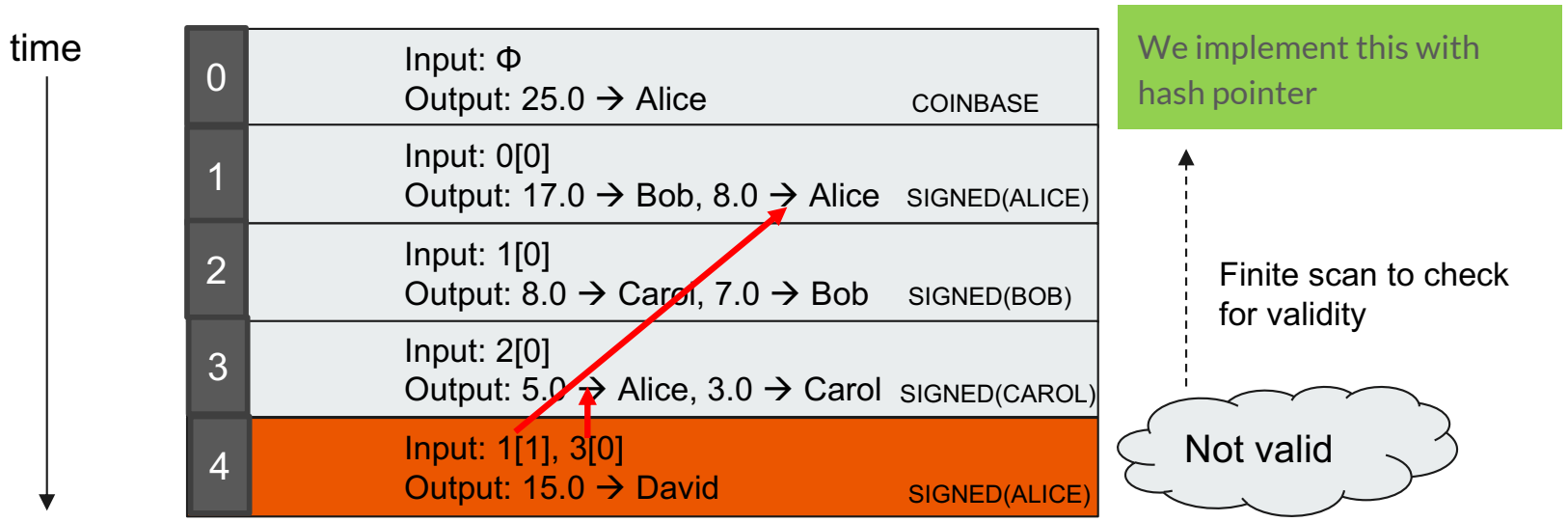
Distributed Ledger

Transaction-based ledger (Bitcoin like)



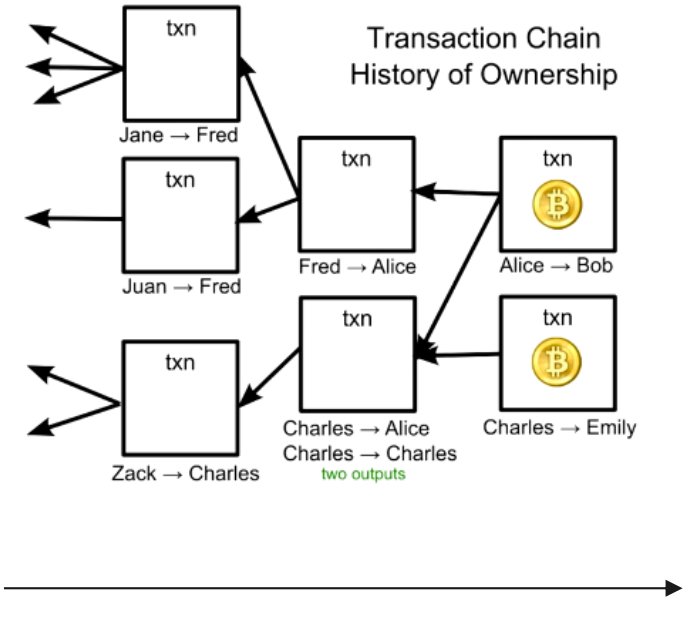
Distributed Ledger

Transaction-based ledger (Bitcoin like)



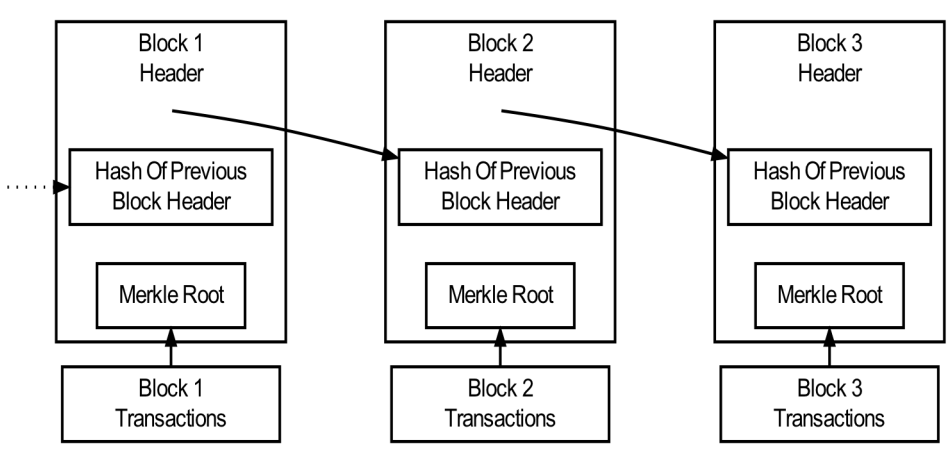
Transaction-based Ledger

- Each new Transaction refer to earlier unspent transaction.
- Validity checked by miner



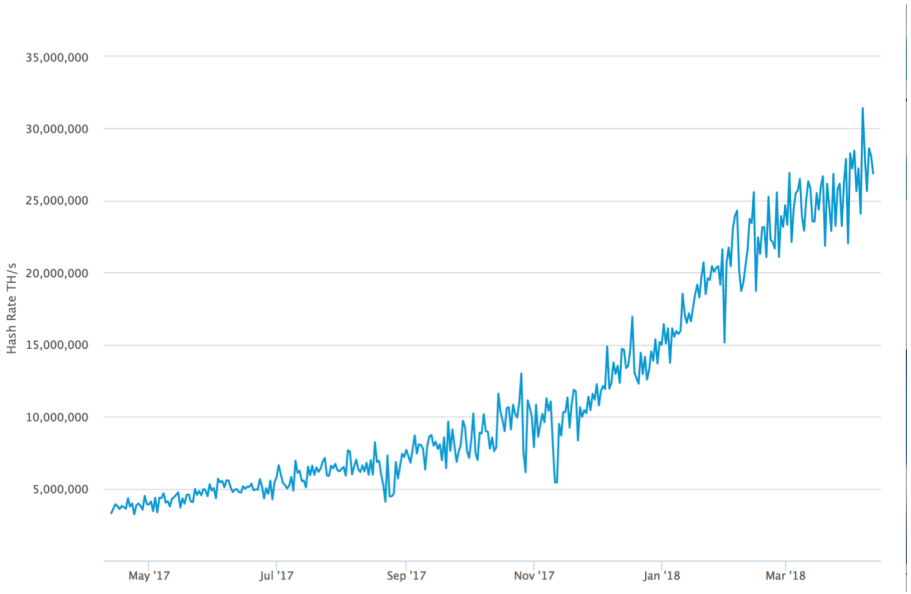
Block Chain

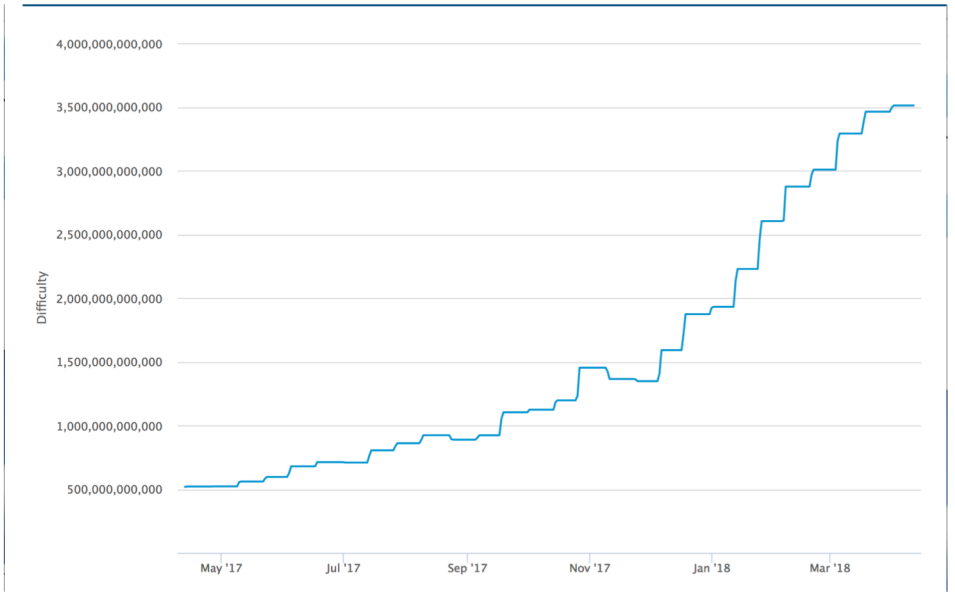
- Public ledger, an ordered and timestamped record of transactions
- New block added based on network consensus.
- Proof of work:
  - Cryptographic Puzzle
  - Takes advantage of random nature of hash algorithm.



Simplified Bitcoin Block Chain

Hash rate and Difficulty

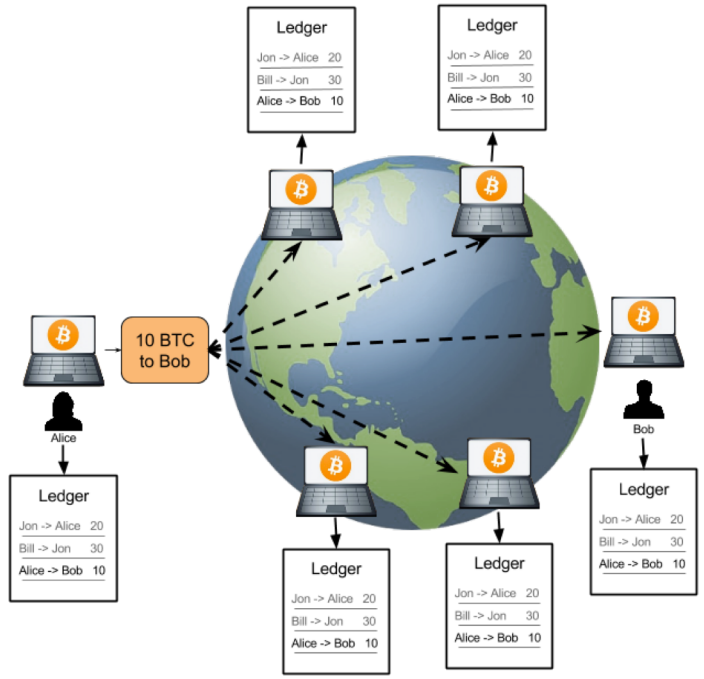




What is Cryptocurrency

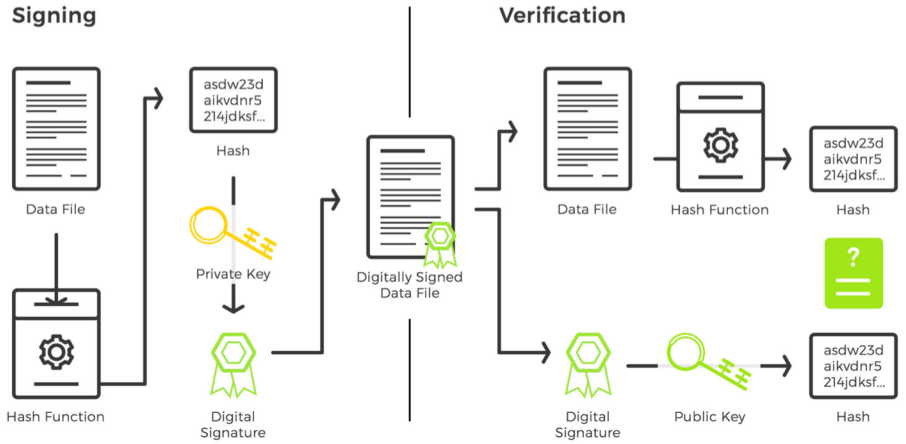
Definition:

- At the core, it's an open ledger keeping track of ~~account balances~~ transactions
- Distributed system that lets a group of computers maintain a ledger.



Sign and Verify Transaction

- ECDSA to Verity the authenticity
- Bitcoin, Litecoin, Ethereum
  - Secp256k1
  - Private key to sign transaction
  - Public key to verify transaction



Bitcoin Transaction

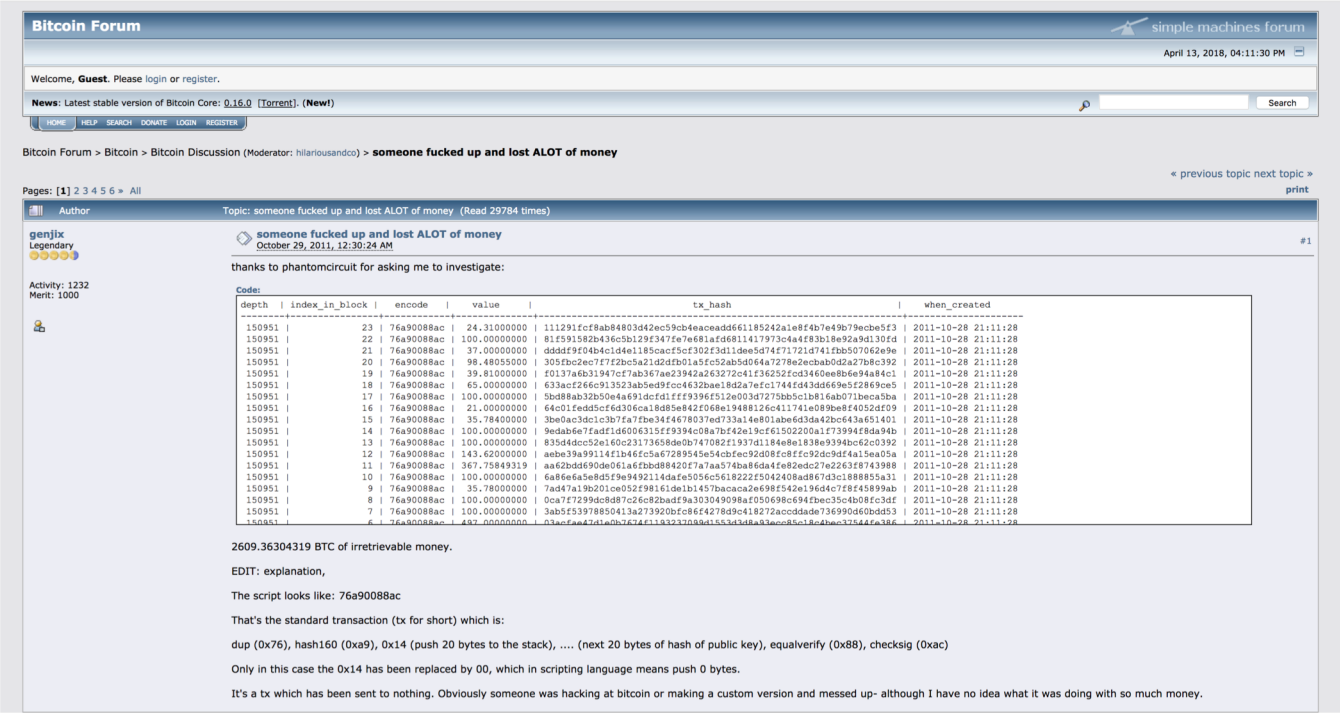
- Input Transaction
- Output Transaction
- Bitcoin scripting language


```
{
  "hash":"ac0cf1caa359f4d8be6bcd3f61ec69078ace4b8d52cf8502363150d077a3b65f",
  "ver":1,
  "vin_sz":1,
  "vout_sz":41,
  "lock_time":0,
  "size":1552,
  "in":[
    {
      "prev_out":{

"hash":"9f7b8b96f83843fbdc9a54e55d7a3af4bd2cb98e79494790be47df663ccb400d",
        "n":56
      },

"scriptSig":"3045022040102b9051dbf79c95ea6d398001539cf0d8747d1e38354a9bcef1398a5
835f4022100b884183914545c7b5ba63f05a8b8adfffd26f4c6985855df8220275b51d8621601
02ae6e895ea731a53602831fe2ad85124ad8bd6e2662ce530a0cded0ba0ba3d106"
    }
  ],
  "out":[
    {
      "value":"0.33513406",
      "scriptPubKey":"OP_DUP OP_HASH160 22a0d99bf56128d1dc2d432d6366ff15df8e9eeb
OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value":"0.03036178",
      "scriptPubKey":"OP_DUP OP_HASH160 e8d4dd5c4db1b59d7e9d912f537ee0c985b427c0
OP_EQUALVERIFY OP_CHECKSIG"
    },
```

2609 bitcoin lost in transaction



Bitcoin Forum

simple machines forum

April 13, 2018, 04:11:30 PM

Welcome, **Guest**. Please login or register.

News: Latest stable version of Bitcoin Core: 0.16.0 [Torrent]. **(New!)**

Search

HOME HELP SEARCH DONATE LOGIN REGISTER

Bitcoin Forum > Bitcoin > Bitcoin Discussion (Moderator: hilariousandco) > **someone fucked up and lost ALOT of money**

« previous topic next topic »

Pages: [1] 2 3 4 5 6 » All

print

Author | Topic: someone fucked up and lost ALOT of money (Read 29784 times)

genjix
Legendary

Activity: 1232
Merit: 1000

someone fucked up and lost ALOT of money
October 29, 2011, 12:30:24 AM

#1

thanks to phantomcircuit for asking me to investigate:

Code:

depth	index_in_block	encode	value	tx_hash	when_created
150951	23	76a90088ac	24.31000000	111291fcf8ab84803d42ec59cb4eaceadd661185242a1e8f4b7e49b79ecbe5f3	2011-10-28 21:11:28
150951	22	76a90088ac	100.00000000	81f591582b436c5b129f347fe7e681afd6811417973c4a4f83b18e92a9d130fd	2011-10-28 21:11:28
150951	21	76a90088ac	37.00000000	ddddf9f04b4c1d4e1185cacf5cf302f3d1dee5d74f71721d741fbb507062e9e	2011-10-28 21:11:28
150951	20	76a90088ac	98.48055000	305fbc2ec7f7f2bc5a21d2dfb01a5fc52ab5d064a7278e2ecbab0d2a27b8c392	2011-10-28 21:11:28
150951	19	76a90088ac	39.81000000	f0137a6b31947cf7ab367ae23942a263272c41f36252fcd3460ee8b6e94a84c1	2011-10-28 21:11:28
150951	18	76a90088ac	65.00000000	633acf266c913523ab5ed9fcc4632bae18d2a7efc1744fd43dd669e5f2869ce5	2011-10-28 21:11:28
150951	17	76a90088ac	100.00000000	5bd88ab32b50e4a691dcfd1fff9396f512e003d7275bb5c1b816ab071beca5ba	2011-10-28 21:11:28
150951	16	76a90088ac	21.00000000	64c01fedd5cf6d306ca18d85e842f068e19488126c411741e089be8f4052df09	2011-10-28 21:11:28
150951	15	76a90088ac	35.78400000	3be0ac3dc1c3b7fa7fbe34f4678037ed733a14e801abe6d3da42bc643a651401	2011-10-28 21:11:28
150951	14	76a90088ac	100.00000000	9edab6e7fadf1d6006315ff9394c08a7bf42e19cf61502200a1f73994f8da94b	2011-10-28 21:11:28
150951	13	76a90088ac	100.00000000	835d4dcc52e160c23173658de0b747082f1937d1184e8e1838e9394bc62c0392	2011-10-28 21:11:28
150951	12	76a90088ac	143.62000000	aebe39a99114f1b46fc5a67289545e54cbfec92d08fc8ffc92dc9df4a15ea05a	2011-10-28 21:11:28
150951	11	76a90088ac	367.75849319	aa62bdd690de061a6fbbd88420f7a7aa574ba86da4fe82edc27e2263f8743988	2011-10-28 21:11:28
150951	10	76a90088ac	100.00000000	6a86e6a5e8d5f9e9492114dafe5056c5618222f5042408ad867d3c1888855a31	2011-10-28 21:11:28
150951	9	76a90088ac	35.78000000	7ad47a19b201ce052f98161de1b1457bacaca2e698f542e196d4c7f8f45899ab	2011-10-28 21:11:28
150951	8	76a90088ac	100.00000000	0ca7f7299dc8d87c26c82badf9a303049098af050698c694fbec35c4b08fc3df	2011-10-28 21:11:28
150951	7	76a90088ac	100.00000000	3ab5f53978850413a273920bfc86f4278d9c418272accddade736990d60bdd53	2011-10-28 21:11:28
150951	6	76a90088ac	497.00000000	03acfae47d1e0b7674f1193237089d1553d3d8a93ecc85c18c4bec37544fe386	2011-10-28 21:11:28

2609.36304319 BTC of irretrievable money.

EDIT: explanation,

The script looks like: 76a90088ac

That's the standard transaction (tx for short) which is:

dup (0x76), hash160 (0xa9), 0x14 (push 20 bytes to the stack), ... (next 20 bytes of hash of public key), equalverify (0x88), checksig (0xac)

Only in this case the 0x14 has been replaced by 00, which in scripting language means push 0 bytes.

It's a tx which has been sent to nothing. Obviously someone was hacking at bitcoin or making a custom version and messed up- although I have no idea what it was doing with so much money.

Problems

- Gap between User and Cryptocurrency
- Private keys
  - Keeping track of private keys
  - Ensuring the security of keys

Outline

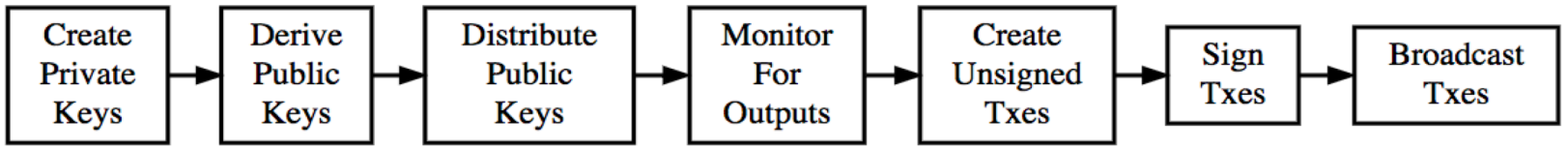
1. What is cryptocurrency?
2. **Importance of wallets**
3. Types of wallets
4. Hierarchical deterministic wallets
5. Demo
6. Future work

Wallets

- Bridge the gap between User and Cryptocurrency
- Easy way to perform transaction
- Key management

Wallet Services

- Generate Private keys
- Derived corresponding public key
  - Monitors for output spent on public key
- Create and broadcast the signed transaction



Goals

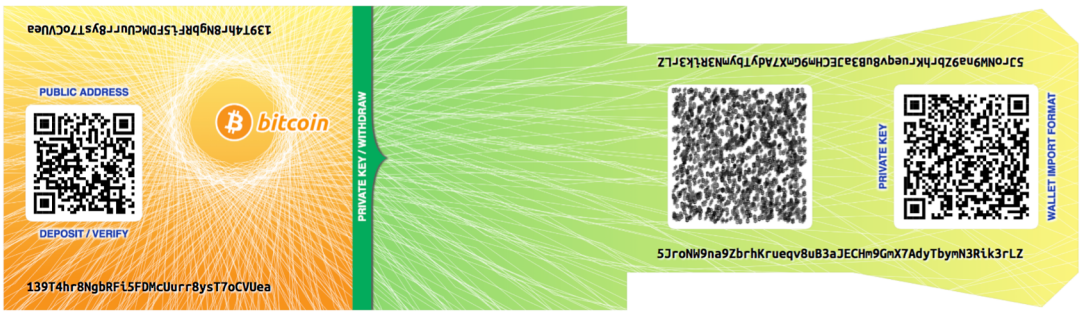
- Availability
  - We can able to spend out coins
- Security
  - Nobody else can spend out coin
- Convenience
  - Relatively easy to use

Outline

1. What is cryptocurrency?
2. Importance of wallets
3. **Types of wallets**
4. Hierarchical deterministic wallets
5. Demo
6. Future work

1. Paper Wallet

- Stores keys on paper
- Availability: As your device
  - Paper lost / damage → Key lost →Coins Lost
- Security: As secure as money in vault
  - Security compromised → Key leaked →Coins stolen
- Convenience: Very Inconvenient



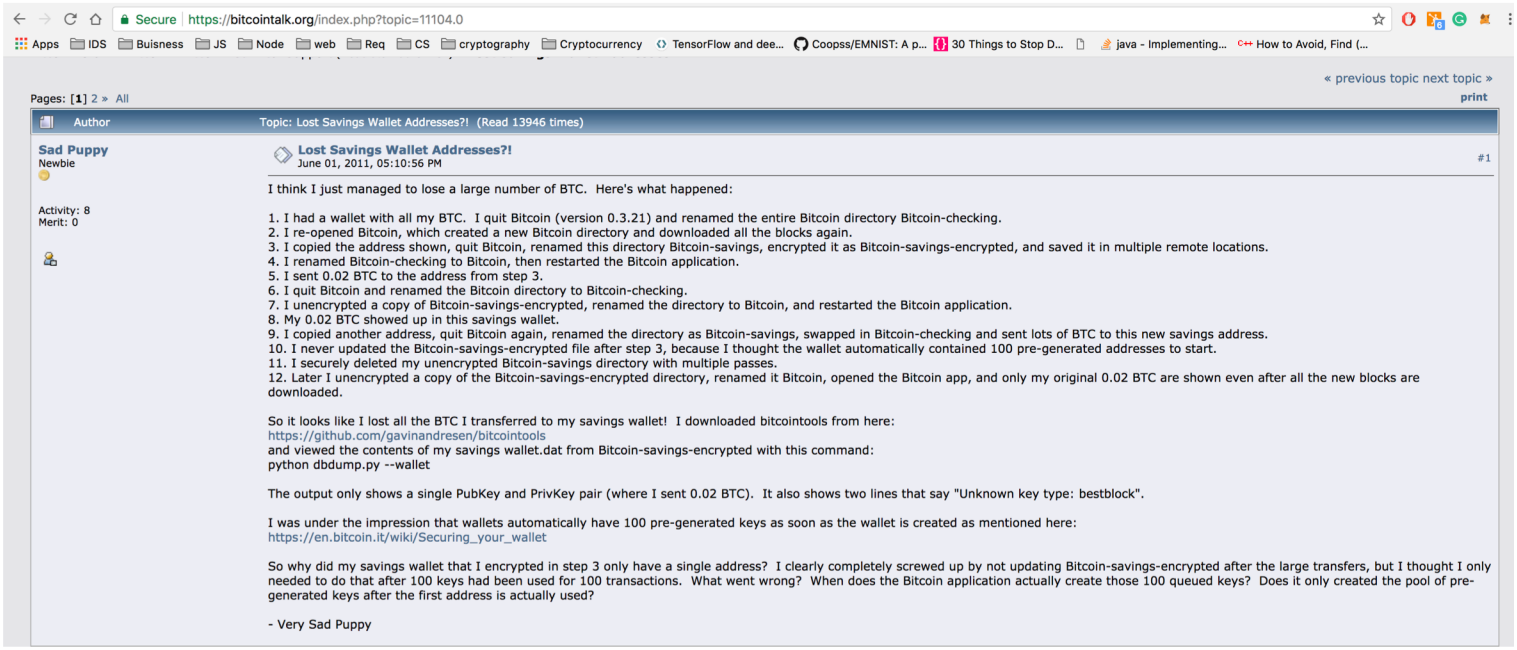
2. Random Independent wallets

- Loose-Key wallets also called “Just a Bunch Of Keys(JBOK)”
- Generate keys using PRNG
- Convenience: Very Convenient
- Availability: As your device
  - Device lost / Wiped → Keys lost → Coins Lost
- Security:
  - Device compromised → Keys leaked → Coins Stolen

3. Deterministic wallets

- Generate Private keys based on seed value
- Example :
  - Privatekey_1 = hash(seed || 1)
  - Privatekey_2 = hash(seed || 2)
- Drawback:
  - Single point of failure
  - Need backups
  - Public/ Private keys stored in the same device

7208 Bitcoins lost due to backup mix-up



Secure | https://bitcointalk.org/index.php?topic=11104.0

Apps | IDS | Buisness | JS | Node | web | Req | CS | cryptography | Cryptocurrency | TensorFlow and dee... | Coopss/EMNIST: A p... | 30 Things to Stop D... | java - Implementing... | How to Avoid, Find (...

« previous topic next topic »

Pages: [1] 2 » All

print

Author	Topic: Lost Savings Wallet Addresses?! (Read 13946 times)

Sad Puppy
Newbie

Activity: 8
Merit: 0

Lost Savings Wallet Addresses?!
June 01, 2011, 05:10:56 PM

#1

I think I just managed to lose a large number of BTC. Here's what happened:

1. I had a wallet with all my BTC. I quit Bitcoin (version 0.3.21) and renamed the entire Bitcoin directory Bitcoin-checking.
2. I re-opened Bitcoin, which created a new Bitcoin directory and downloaded all the blocks again.
3. I copied the address shown, quit Bitcoin, renamed this directory Bitcoin-savings, encrypted it as Bitcoin-savings-encrypted, and saved it in multiple remote locations.
4. I renamed Bitcoin-checking to Bitcoin, then restarted the Bitcoin application.
5. I sent 0.02 BTC to the address from step 3.
6. I quit Bitcoin and renamed the Bitcoin directory to Bitcoin-checking.
7. I unencrypted a copy of Bitcoin-savings-encrypted, renamed the directory to Bitcoin, and restarted the Bitcoin application.
8. My 0.02 BTC showed up in this savings wallet.
9. I copied another address, quit Bitcoin again, renamed the directory as Bitcoin-savings, swapped in Bitcoin-checking and sent lots of BTC to this new savings address.
10. I never updated the Bitcoin-savings-encrypted file after step 3, because I thought the wallet automatically contained 100 pre-generated addresses to start.
11. I securely deleted my unencrypted Bitcoin-savings directory with multiple passes.
12. Later I unencrypted a copy of the Bitcoin-savings-encrypted directory, renamed it Bitcoin, opened the Bitcoin app, and only my original 0.02 BTC are shown even after all the new blocks are downloaded.

So it looks like I lost all the BTC I transferred to my savings wallet! I downloaded bitcointools from here:
https://github.com/gavinandresen/bitcointools
and viewed the contents of my savings wallet.dat from Bitcoin-savings-encrypted with this command:
python dbdump.py --wallet

The output only shows a single PubKey and PrivKey pair (where I sent 0.02 BTC). It also shows two lines that say "Unknown key type: bestblock".

I was under the impression that wallets automatically have 100 pre-generated keys as soon as the wallet is created as mentioned here:
https://en.bitcoin.it/wiki/Securing_your_wallet

So why did my savings wallet that I encrypted in step 3 only have a single address? I clearly completely screwed up by not updating Bitcoin-savings-encrypted after the large transfers, but I thought I only needed to do that after 100 keys had been used for 100 transactions. What went wrong? When does the Bitcoin application actually create those 100 queued keys? Does it only created the pool of pre-generated keys after the first address is actually used?

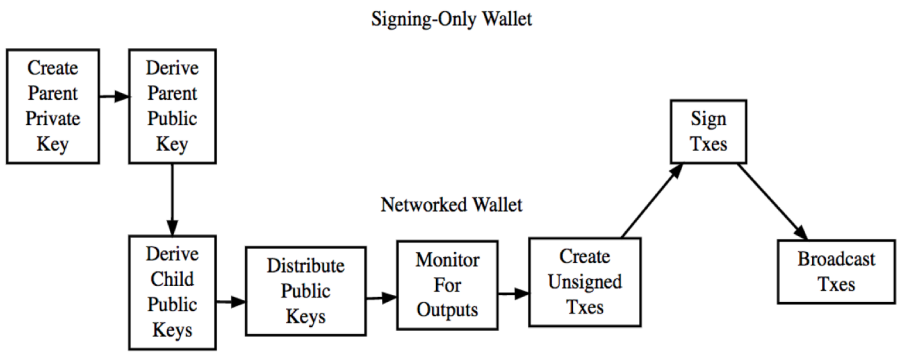
- Very Sad Puppy

4. Hardware Wallets

- Special purpose security hardened device
- Private keys stored in device securely
- Convenience: Convenient
- Availability: Depends on device
  - Device lost / Wiped → Keys lost → Coins Lost
- Security:
  - Very Secure

5. Cold Storage Wallets

- Divide wallet into Online and Offline wallet
- Keep private key offline
- Monitor for transaction using public keys



How to design cold storage wallet?

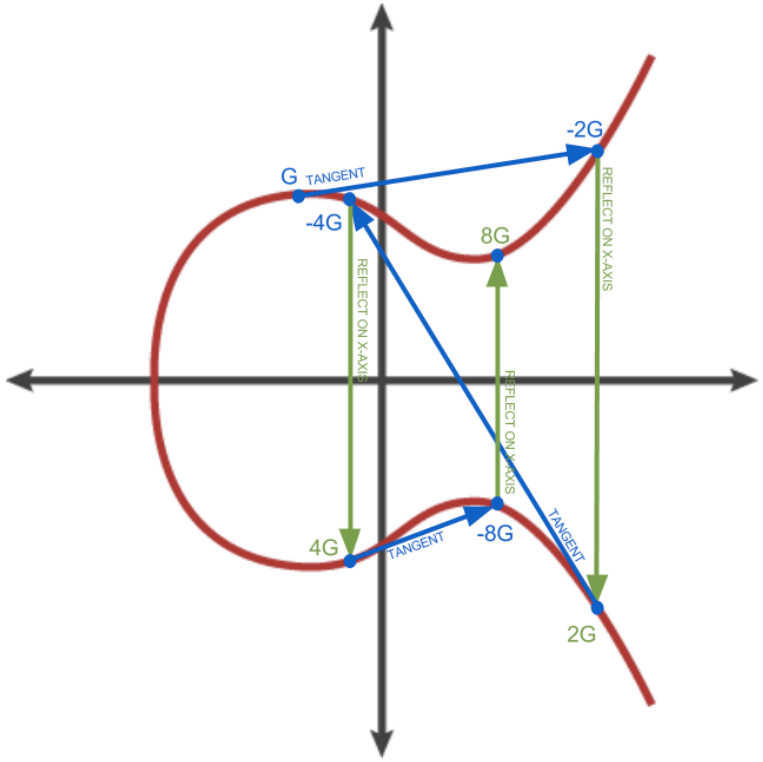
- Separate Send to addresses and Receiving addresses
- Awkward Solution:
  - Generate a big batch of addresses/keys beforehand
- Drawback:
  - Periodically need to connect Hot side with cold side

Outline

1. What is cryptocurrency?
2. Importance of wallets
3. Types of wallets
4. **Hierarchical deterministic wallets**
5. Demo
6. Future work

ECC Point addition

- Private key and Public key
  - point(private_key) = public_key
  - private key: large integer
  - public key : point on the curve

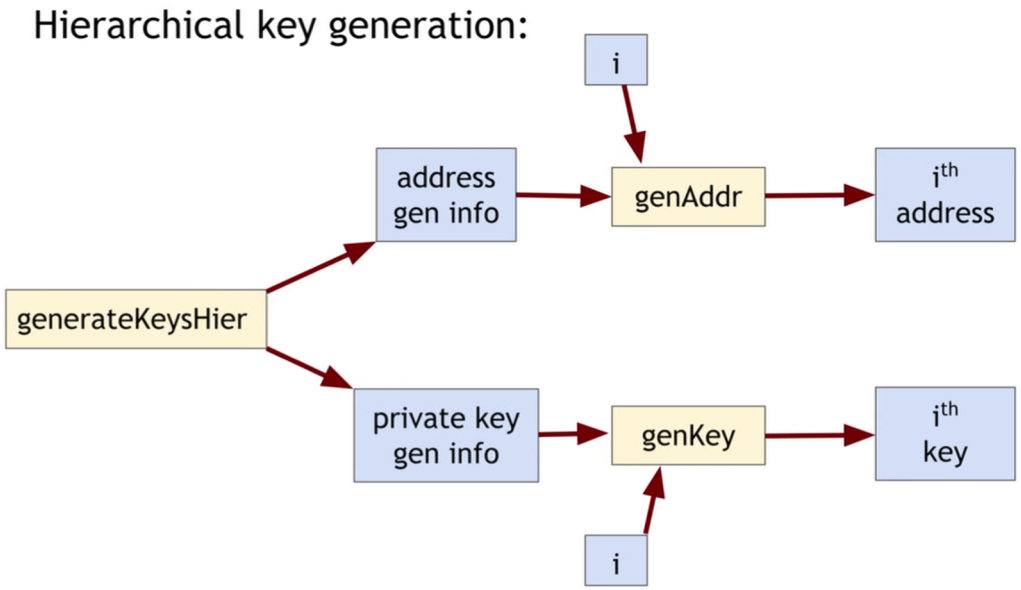


Hierarchical Deterministic wallet

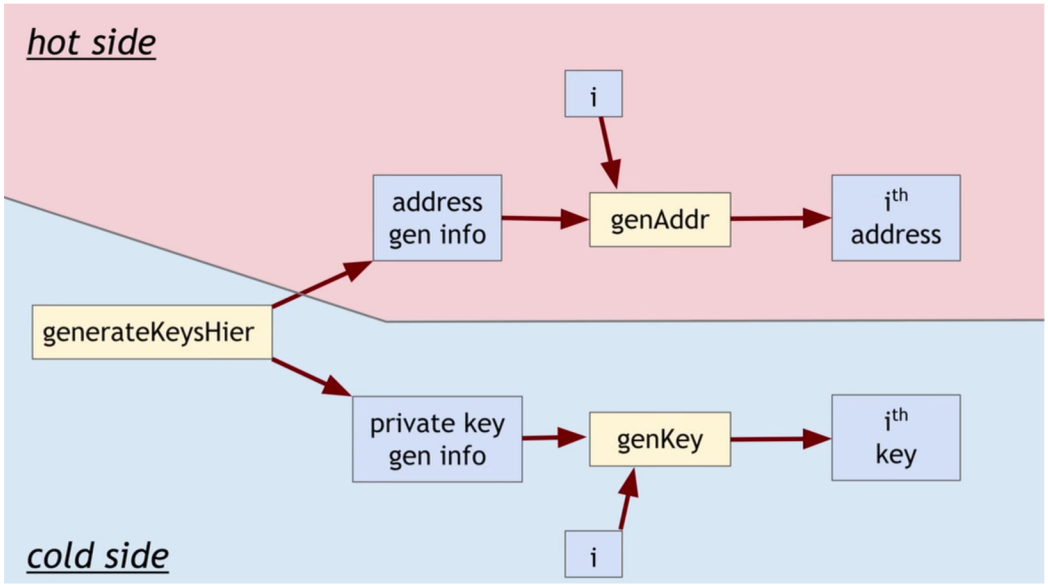
- Homomorphism feature of discrete-log based cryptosystem(ECDSA)
  - Private key and Public key
    - point(private_key) = public_key
    - private key: large integer
    - public key : point on the curve
  - Homomorphism in ECDSA:
    - private_key_new = (private_key1 + privatekey2) %G
    - point(private_key_new) = point(private_key1) + point(private_key2)
    - public_key_new = public_key1 + public_key2

+ Arithmetic addition
+ Elliptic curve point addition

Hierarchical Key Generation

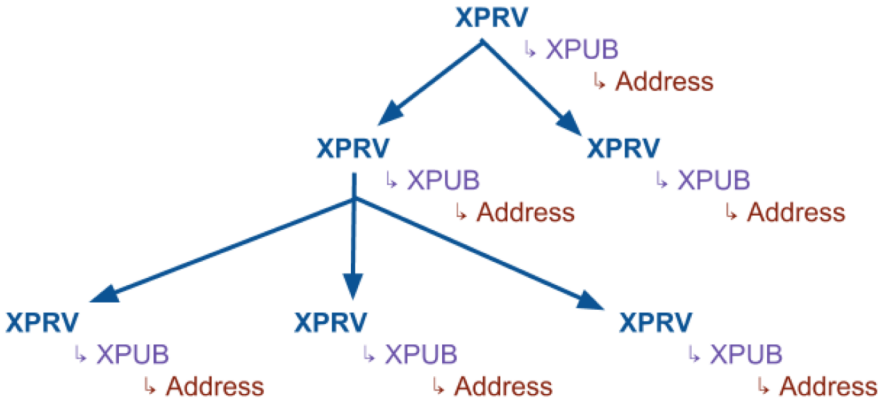


Hierarchical Key Generation

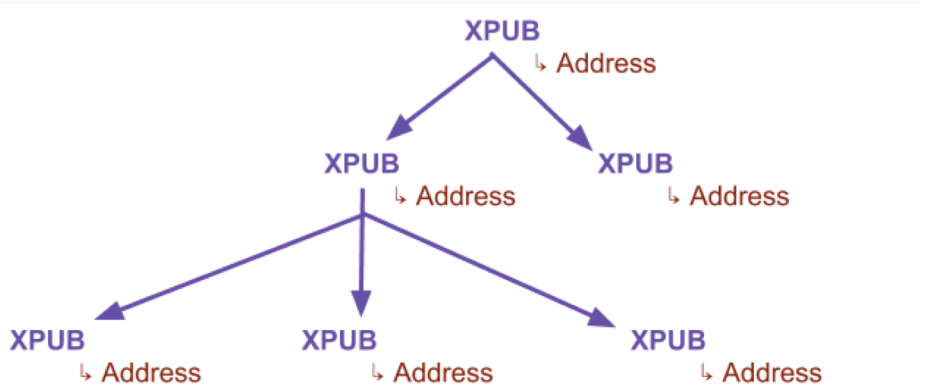


Hierarchical deterministic wallet

Offline Side

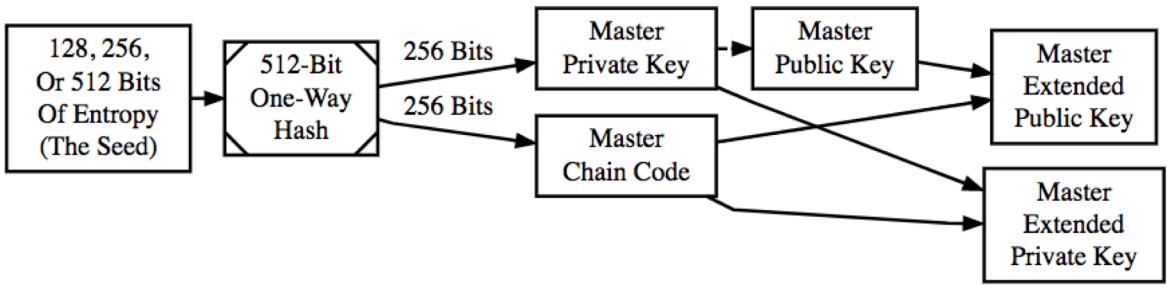


Online Side



Master Key Creation

- HD wallets are create from single root seed
- Everything else deterministically derived from root seed



Creation Of The Master Keys

Extended Keys

- [version][depth][parent fingerprint][key index][chain code][key]

- 4-byte **Version**
  - Private Key: Mainnet(0x0488ADE4)/Testnet(0x04358394)
  - Public Key: Mainnet(0x0488B21E)/Testnet(0x043587CF)
- 1-byte **Depth**
- 4-byte **Fingerprint of parent**
  - First 4-bytes of Hash160 (parent pubic key)
- 4-byte **Index Number**
- 32-byte **Parent Chain Code**
- 34-byte **Key**
  - Private Key: 0x00 + 32 bytes private key
  - Public Key: 34 byte compressed public key
- 4-byte **Checksum**

Child Private Key Generation

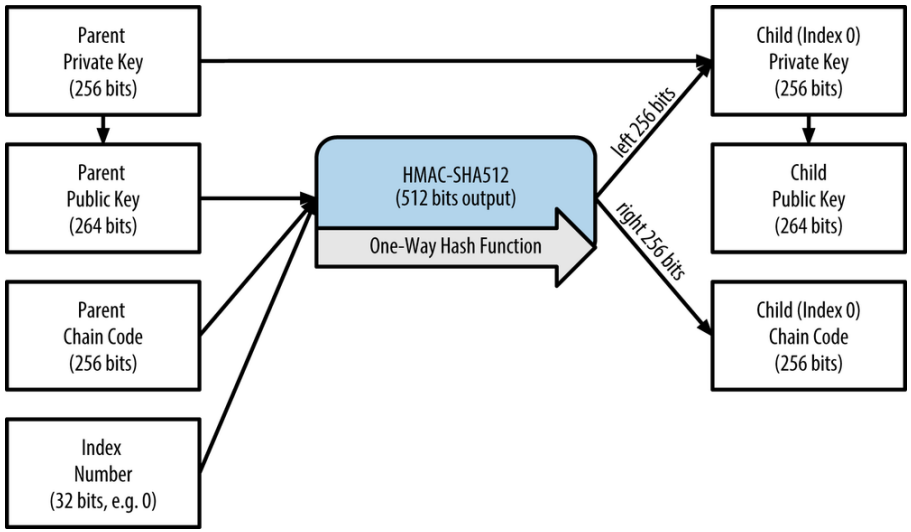
- Parent Private keys →Parent Public keys
- Index Number
- Parent Chain Code

point((parent_private + lefthand_hash) % G) == child_private

****

point(child_private) == child_public

parent_public + point(lefthand_hash) == child_public



+ Arithmetic addition
+ Elliptic curve point addition

Child Public Key Generation

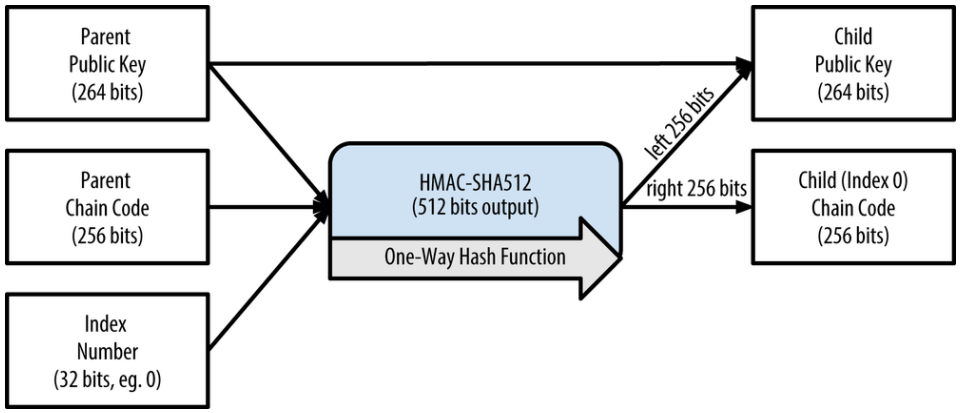
- Parent Public keys
- Index Number
- Parent Chain Code

point((parent_private + lefthand_hash) % G) == child_private

****

point(child_private) == child_public

parent_public + point(lefthand_hash) == child_public

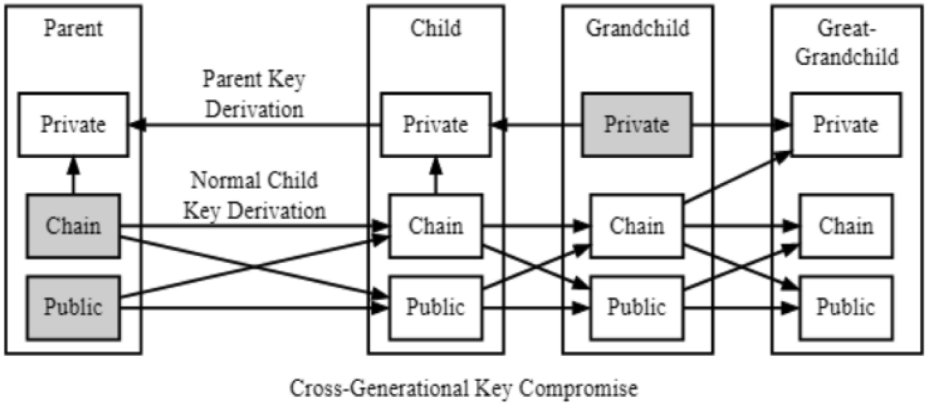


+ Arithmetic addition
+ Elliptic curve point addition

Problem with the key derivation

- Leaked child private key and Leaked chaincode can be used to derive all the other child private keys

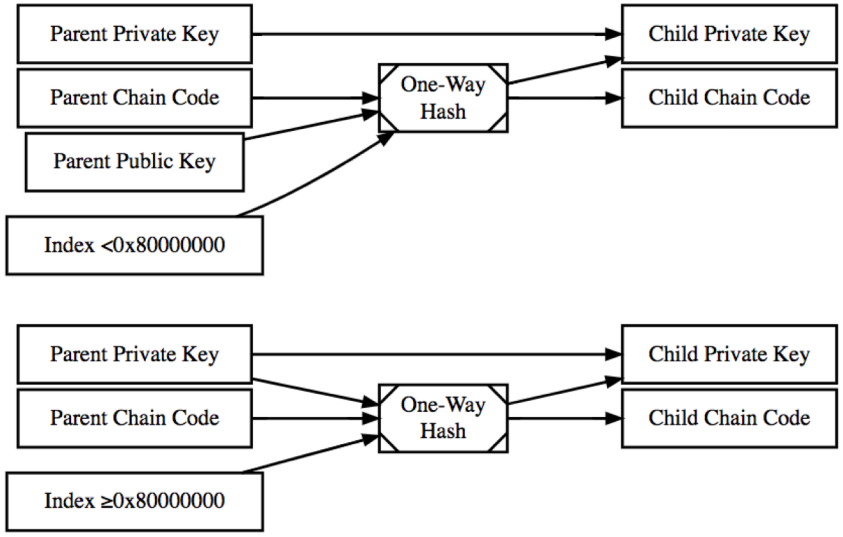
- $pubkey_{i+1} \leftarrow pubkey_i + n_i \cdot G$
- If
  - $privkey_{i+1}$ is compromised
  - chaincodes public or know to attacker
- Solve for
  x: $x + n_i = privkey_{i+1} \bmod order(G)$



Cross-Generational Key Compromise

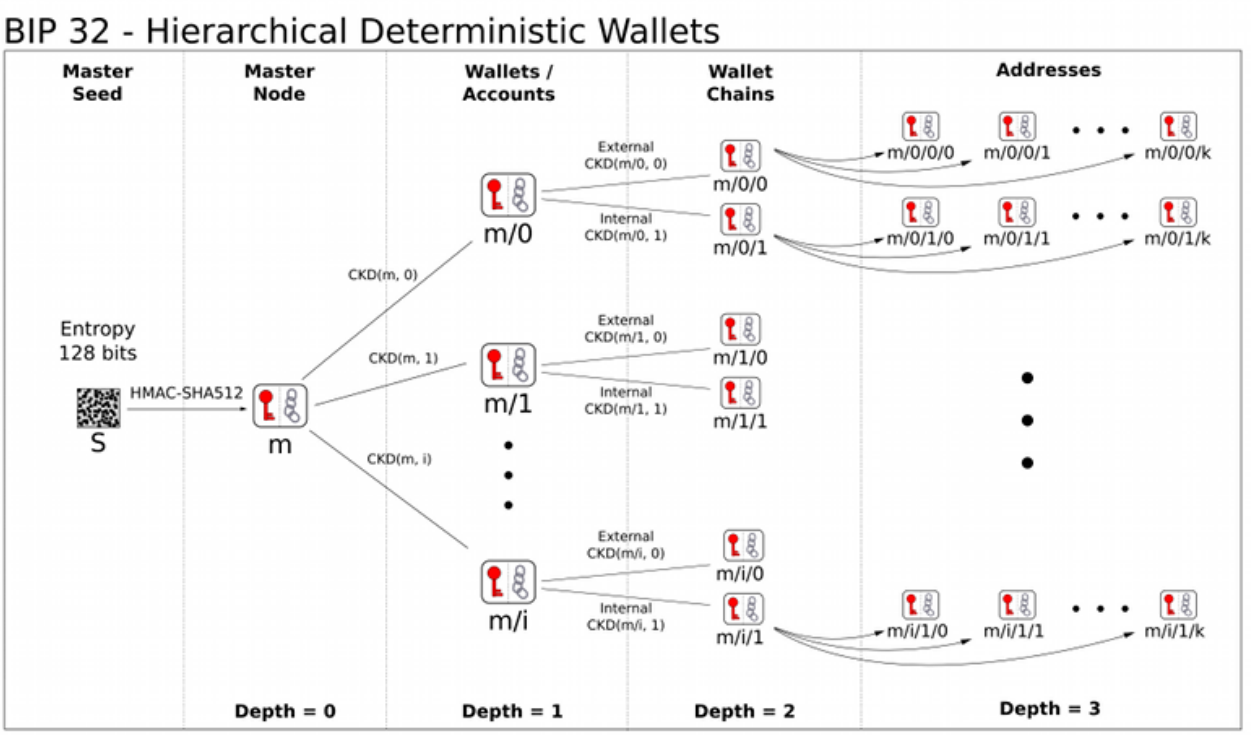
Hardened Keys

- Extended public keys contains the chaincode
- Hardened derivation breaks the relationship between parent public keys and chaincode
- Use parent private key to derive the child chain code
- bip44:
  - m /
  - purpose' /
  - coin_type' /
  - account' /
  - change /
  - address_index



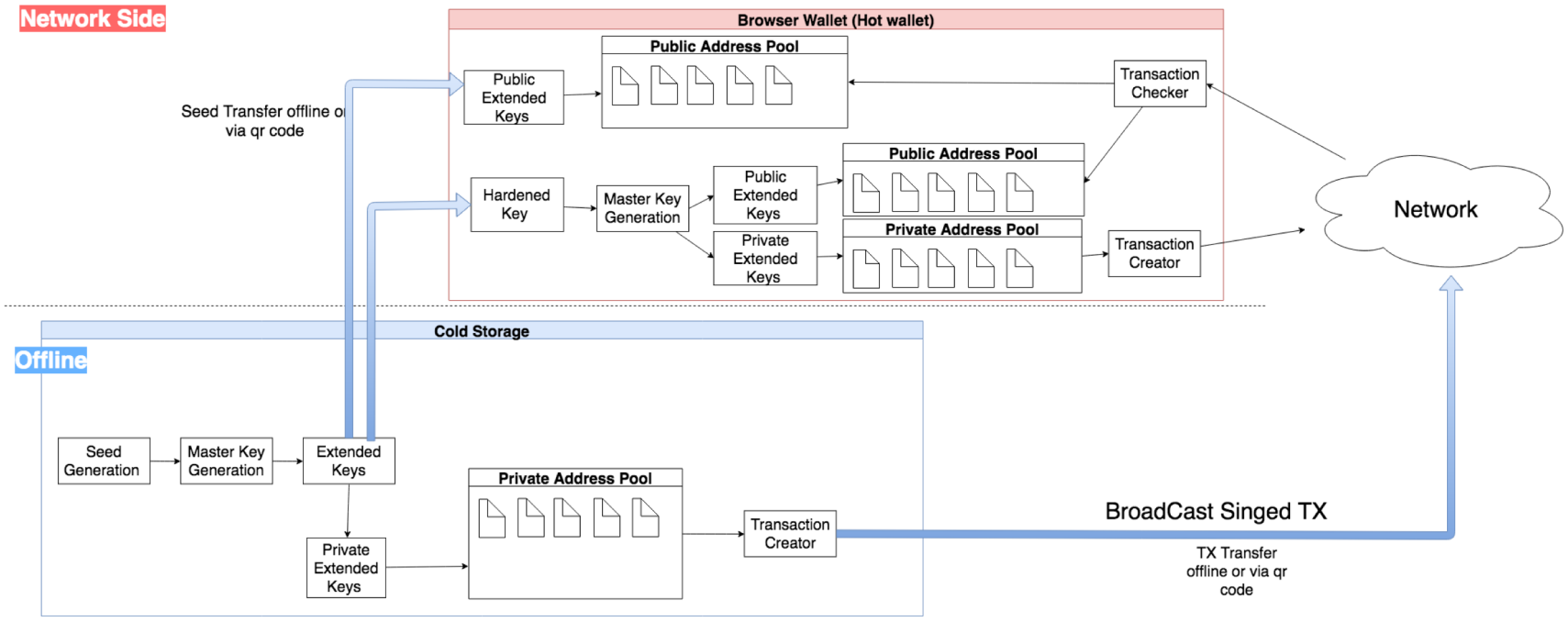
Normal (Top) And Hardened (Bottom) Child Private Key Derivation

BIP 32



Child Key Derivation Function ~ $CKD(x,n) = HMAC\text{-}SHA512(x_{Chain}, x_{PubKey} || n)$

Architecture

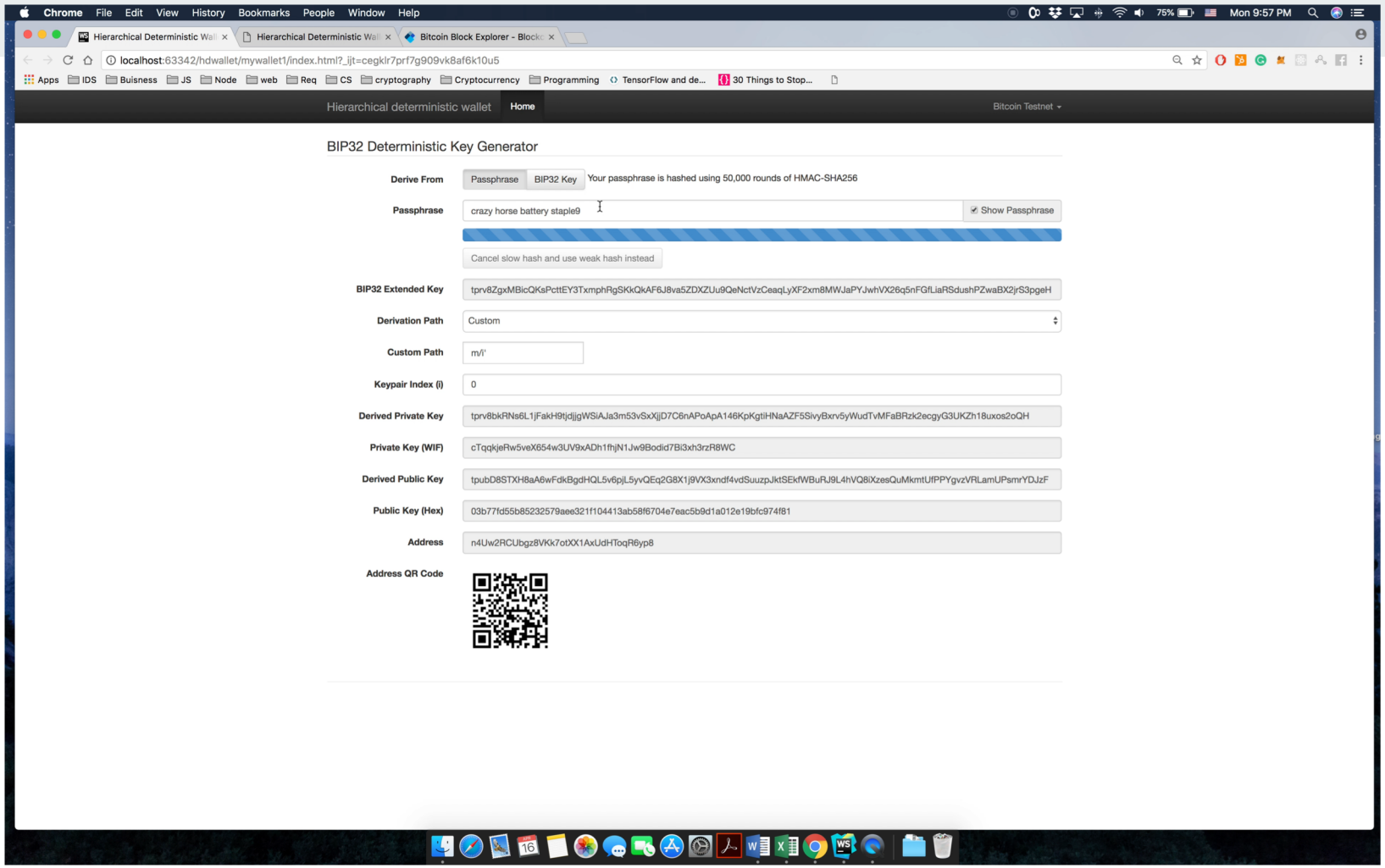


Outline

1. What is cryptocurrency?
2. Importance of wallets
3. Types of wallets
4. Hierarchical deterministic wallets
5. **Demo**
6. Future work

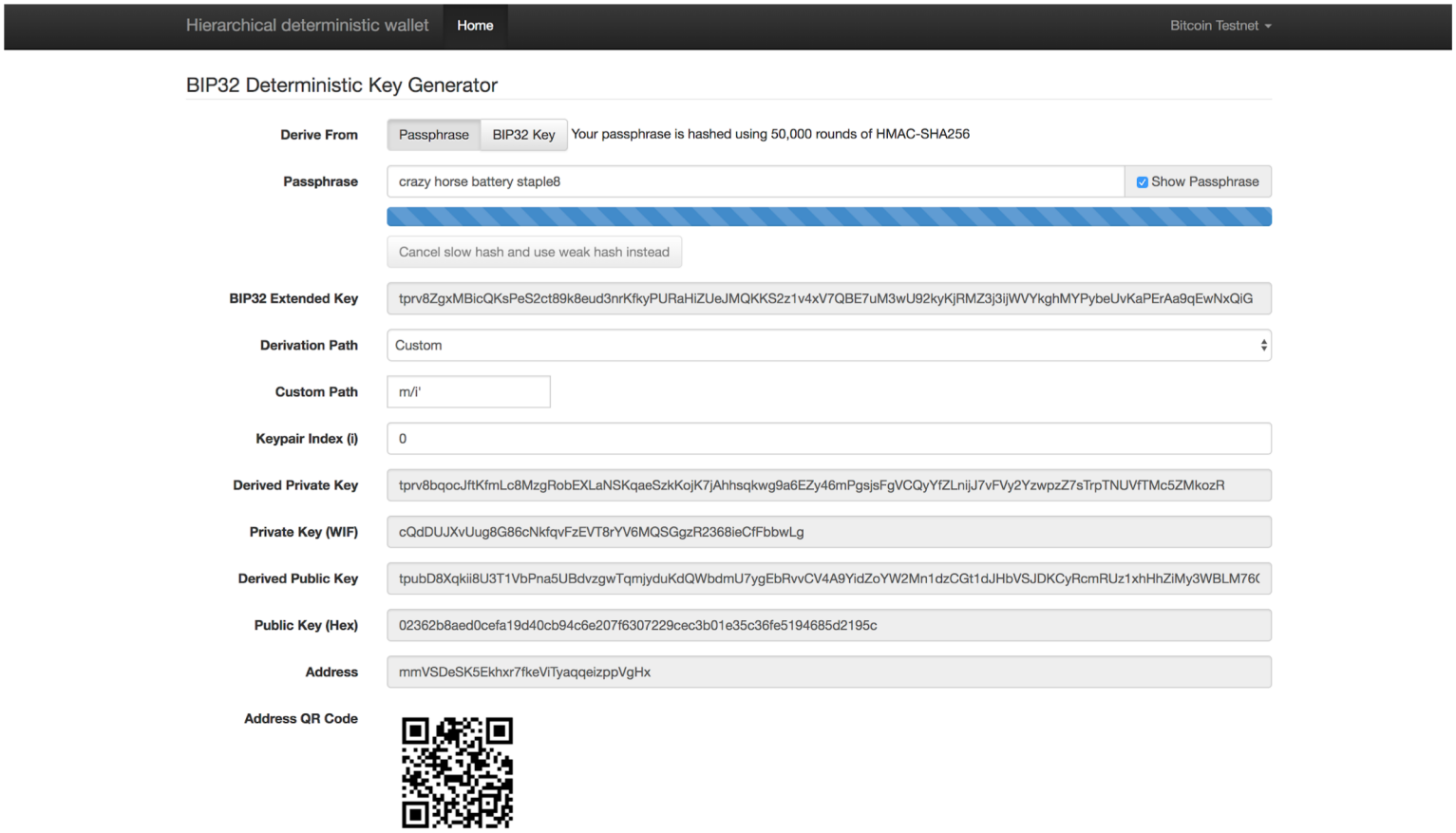
Demo

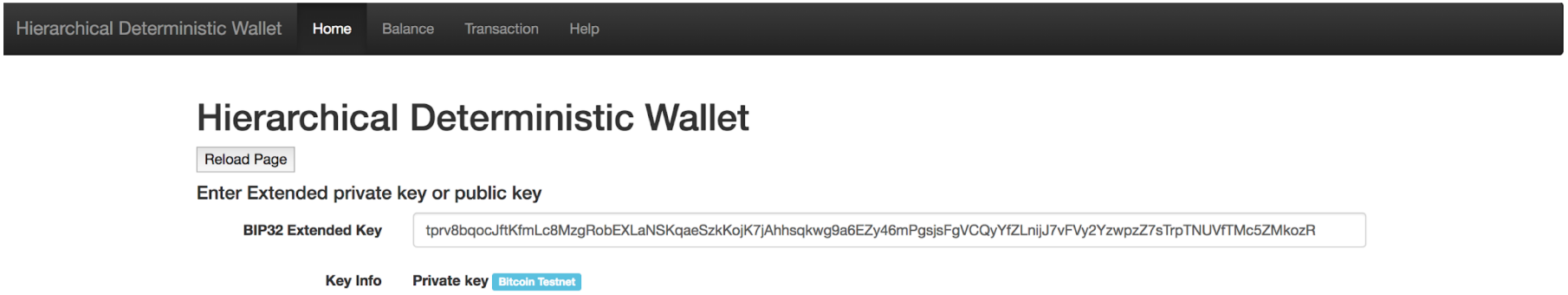
- Used API and Library :
  - Bitcoin Testnet
  - Bitcoinjs-lib (https://www.npmjs.com/package/bitcoinjs-lib)
  - Blockchain.info API (https://testnet.blockchain.info/)


Chrome File Edit View History Bookmarks People Window Help
Mon 9:57 PM
Hierarchical Deterministic Wall
Hierarchical Deterministic Wall
Bitcoin Block Explorer - Block
localhost:63342/hdwallet/mywallet1/index.html?_ijt=cegklr7prf7g909vk8af6k10u5
Apps IDS Buisness JS Node web Req CS cryptography Cryptocurrency Programming TensorFlow and de... 30 Things to Stop...
Hierarchical deterministic wallet
Home
Bitcoin Testnet
BIP32 Deterministic Key Generator
Derive From
Passphrase
BIP32 Key
Your passphrase is hashed using 50,000 rounds of HMAC-SHA256
Passphrase
crazy horse battery staple9
Show Passphrase
Cancel slow hash and use weak hash instead
BIP32 Extended Key
tprv8ZgxMBicQKsPcttEY3TxmphRgSKkQkAF6J8va5ZDXZUu9QeNctVzCeaqLyXF2xm8MWJaPYJwhVX26q5nFGfLiaRSdushPZwaBX2jrS3pgeH
Derivation Path
Custom
Custom Path
m/i'
Keypair Index (i)
0
Derived Private Key
tprv8bkRNs6L1jFakH9tjdjjgWSiAJa3m53vSxXjjD7C6nAPoApA146KpKgtiHNaAZF5SivyBxrv5yWudTvMFaBRzk2ecgyG3UKZh18uxos2oQH
Private Key (WIF)
cTqqkjeRw5veX654w3UV9xADh1fhjN1Jw9Bodid7Bi3xh3rzR8WC
Derived Public Key
tpubD8STXH8aA6wFdkBgdHQL5v6pjL5yvQEq2G8X1j9VX3xndf4vdSuuzpJktSEkfWBuRJ9L4hVQ8iXzesQuMkmtUfPPYgvzVRLamUPsmrYDJzF
Public Key (Hex)
03b77fd55b85232579aee321f104413ab58f6704e7eac5b9d1a012e19bfc974f81
Address
n4Uw2RCUbgz8VKk7otXX1AxUdHToqR6yp8
Address QR Code

Capstone Project

- Implementation of convenient, secure wallet
  - Improve convenience
  - Recoverable keys (Availability)
  - Cryptographically secure (Security)


Hierarchical deterministic wallet
Home
Bitcoin Testnet
BIP32 Deterministic Key Generator
Derive From
Passphrase
BIP32 Key
Your passphrase is hashed using 50,000 rounds of HMAC-SHA256
Passphrase
crazy horse battery staple8
Show Passphrase
Cancel slow hash and use weak hash instead
BIP32 Extended Key
tprv8ZgxMBicQKsPeS2ct89k8eud3nrKfkyPURaHiZUeJMQKKS2z1v4xV7QBE7uM3wU92kyKjRMZ3j3ijWVYkghMYPybeUvKaPErAa9qEwNxQiG
Derivation Path
Custom
Custom Path
m/i'
Keypair Index (i)
0
Derived Private Key
tprv8bqocJftKfmLc8MzgRobEXLaNSKqaeSzkKojK7jAhhsqkwg9a6EZy46mPgsjsFgVCQyYfZLnijJ7vFVy2YzwpzZ7sTrpTNUVfTMc5ZMkozR
Private Key (WIF)
cQdDUJXvUug8G86cNkfqvFzEVT8rYV6MQSGgzR2368ieCfFbbwLg
Derived Public Key
tpubD8Xqkii8U3T1VbPna5UBdvzgwTqmjyduKdQWbdmU7ygEbRvvCV4A9YidZoYW2Mn1dzCGt1dJHbVSJDKCyRcmRUz1xhHhZiMy3WBLM76(
Public Key (Hex)
02362b8aed0cefa19d40cb94c6e207f6307229cec3b01e35c36fe5194685d2195c
Address
mmVSDeSK5Ekhxr7fkeViTyaqqeizppVgHx
Address QR Code


Hierarchical Deterministic Wallet
Home
Balance
Transaction
Help
Hierarchical Deterministic Wallet
Reload Page
Enter Extended private key or public key
BIP32 Extended Key
tprv8bqocJftKfmLc8MzgRobEXLaNSKqaeSzkKojK7jAhhsqkwg9a6EZy46mPgsjsFgVCQyYfZLnijJ7vFVy2YzwpzZ7sTrpTNUVfTMc5ZMkozR
Key Info
Private key
Bitcoin Testnet

Hierarchical Deterministic Wallet

Reload Page

Spendable balance found

0.6819286 BTC (pending, unspendable transactions don't show)

Receiving Addresses

Receiving addresses are the addresses found on the external address chain (i.e. `m/i'/0/k` in BIP32 terminology). These should be used to to give to other people, where they can send payments.

#	Address	Balance (BTC)
0	mwv7br7jqzVlAYNsxA57oEAgVEwlFCYmkw	0.6819286
1	mh78ZcwaHQp6hYn5qKns3F3EnQdDBBlpan	0
2	mgMQLYLxEhnTVCqcLzJ2x9jaPQc14Z9DMn	0
3	mx2ZnLrBtc4XMQhkWFg2PYqgUFo2MhmYRg	0
4	mys5xCSokLr6zjXwnnTzQl6MbfRp8wuDqd	0
5	mmaiTYCKKBYMmDGZWTtl2aQREy7EoNzZRA	0
6	mgMVWoYAu3yg1uYBUHGz8ikj28y5jCSYkZ	0
7	my5YdD6zVMs7PBARXDgp1i9MsZPTAyRk92	0
8	n2SnA2KxHY5pzRtjNcfozQSieaYWubSSEG	0
9	mjnhia7svazooJbAwz8oGoAzqs1GRgf6wK	0
10	myw1sB9DZg4XipnzgMGHX1XK4n4vCMqPXK	0

Change Addresses

Change addresses are the addresses found on the internal address chain (i.e. `m/i'/1/k` in BIP32 terminology). These should be used just by the wallet software (e.g. this page) to generate new address every time you have change from an outgoing transaction. Should not use them directly.

#	Address	Balance (BTC)
0	mkqQMcXftseBf5sRgtTv1qt2GXG3yqHbco	0
1	msznCgoqUSVa1eJLGtcBBraYWyUDe9LHBH	0
2	mh8SVp4UYegvD5QWsPLQn9N3byChAjNw9D	0
3	moNbhQAFjQcm5PsNVM38c23SHDjwtXfxUx	0

Warning! This is the testnet3 blockchain. Testnet coins have no value.

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	mwv7br7jqzV1AYNsxA57oEAgVEw1FCYmkw
Hash 160	b3e3593c44824a93d6c9fa40dedf986799150909
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	1
Total Received	0.6819286 BTC
Final Balance	0.6819286 BTC

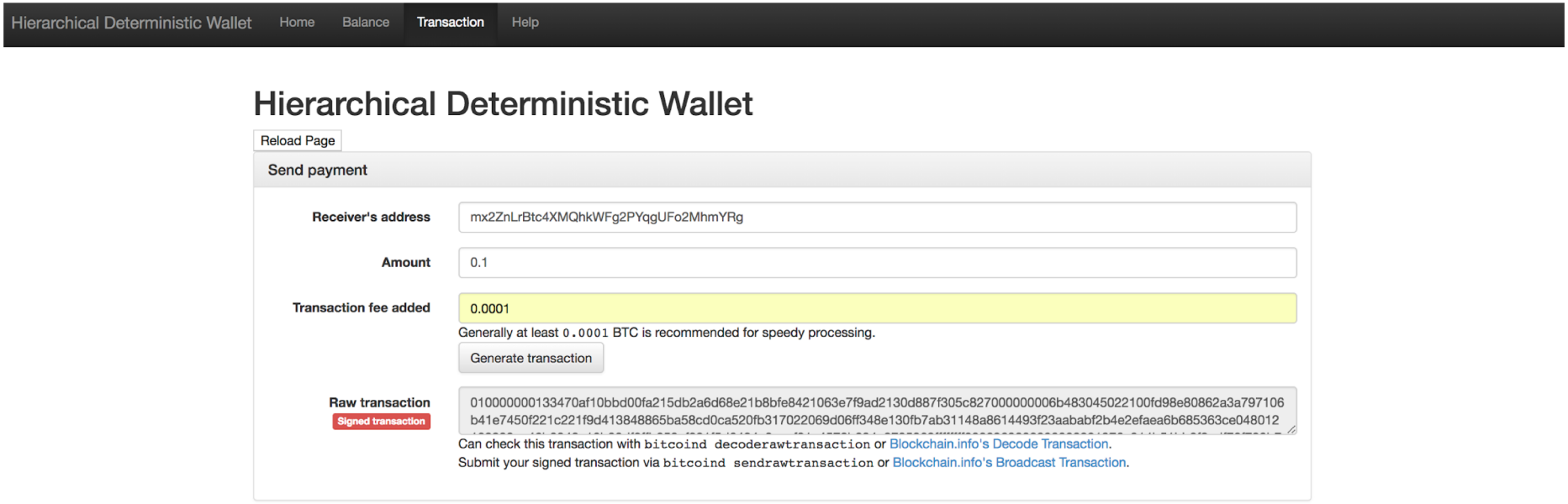
Request Payment Donation Button

Transactions (Oldest First)

Filter

27c805f387d83021adf9e7631042e8bfb8218ed6a6b25d21fa00bd0bf10a4733			2018-04-12 04:30:18
myxTKQSUEdqFbpQ6DijRQCe72ZMM6snqGw	→	mwv7br7jqzV1AYNsxA57oEAgVEw1FCYmkw	0.6819286 BTC

3 Confirmations 0.6819286 BTC


Hierarchical Deterministic Wallet
Home
Balance
Transaction
Help
Hierarchical Deterministic Wallet
Reload Page
Send payment
Receiver's address
mx2ZnLrBtc4XMQhkWFg2PYqgUFo2MhmYRg
Amount
0.1
Transaction fee added
0.0001
Generally at least 0.0001 BTC is recommended for speedy processing.
Generate transaction
Raw transaction
Signed transaction
010000000133470af10bbd00fa215db2a6d68e21b8bfe8421063e7f9ad2130d887f305c827000000006b483045022100fd98e80862a3a797106
b41e7450f221c221f9d413848865ba58cd0ca520fb317022069d06ff348e130fb7ab31148a8614493f23aababf2b4e2efaea6b685363ce048012
Can check this transaction with bitcoind decoderawtransaction or Blockchain.info's Decode Transaction.
Submit your signed transaction via bitcoind sendrawtransaction or Blockchain.info's Broadcast Transaction.

```
{
   "lock_time":0,
   "size":226,
   "inputs":[
      {
         "prev_out":{
            "index":0,
            "hash":"27c805f387d83021adf9e7631042e8bfb8218ed6a6b25d21fa00bd0bf10a4733"
         },
         "script":"483045022100fd98e80862a3a797106b41e7450f221c221f9d413848865ba58cd0ca520fb317022069d06ff348e130fb7ab31148a8614493f23aababf2b4e
      }
   ],
   "version":1,
   "vin_sz":1,
   "hash":"a7bb63ddf3da44988a43ae0544ca79fb3cd9d59567dfefe8474626a8695a1199",
   "vout_sz":2,
   "out":[
      {
         "script_string":"OP_DUP OP_HASH160 b51bb2f8adf70f700b76fa905cbf641f118d1552 OP_EQUALVERIFY OP_CHECKSIG",
         "address":"mx2ZnLrBtc4XMQhkWFg2PYqgUFo2MhmYRg",
         "value":10000000,
         "script":"76a914b51bb2f8adf70f700b76fa905cbf641f118d155288ac"
      },
      {
         "script_string":"OP_DUP OP_HASH160 3a55df04b86e9a3334a3fb2637b1fc454b5dfa96 OP_EQUALVERIFY OP_CHECKSIG",
         "address":"mkqQMcXftseBf5sRgtTv1qt2GXG3yqHbco",
         "value":58182860,
         "script":"76a9143a55df04b86e9a3334a3fb2637b1fc454b5dfa9688ac"
      }
   ]
}
```

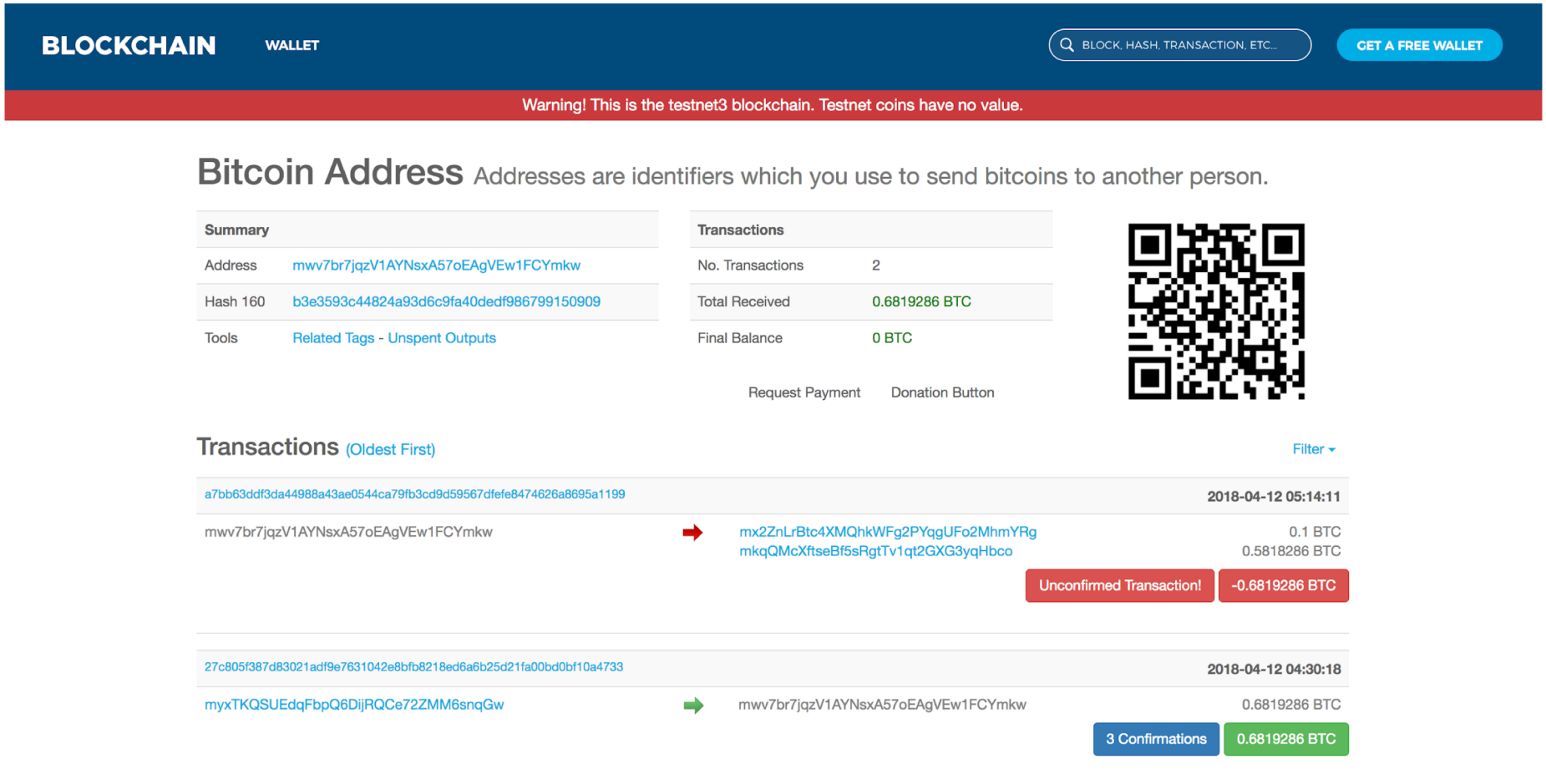
Broadcast Transaction

Tip: Check your transaction before broadcasting using the decode transaction tool

This page allows you to paste a raw transaction in hex format (i.e. characters 0-9, a-f) and broadcast it over the bitcoin network.

010000000133470af10bbd00fa215db2a6d68e21b8bfe8421063e7f9ad2130d887f305c827000000006b483045022100fd98e80862a3a797106b41e7450f221c221f9d413848865ba58cd0ca520fb317022069d06ff348e130fb7ab31148a8614493f23aababf2b4e2efaea6b685363ce048012103839cc46b0348a16b00df2ffb053af201f5d6434a3aeaf01c4578b894c2785369ffffffff02809698000000000001976a914b51bb2f8adf70f700b76fa905cbf641f118d155288accccc77030000000001976a9143a55df04b86e9a3334a3fb2637b1fc454b5dfa9688ac00000000

Submit Transaction


BLOCKCHAIN
WALLET
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE WALLET
Warning! This is the testnet3 blockchain. Testnet coins have no value.
Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.
Summary
Address mwv7br7jqzV1AYNsxA57oEAgVEw1FCYmkw
Hash 160 b3e3593c44824a93d6c9fa40dedf986799150909
Tools Related Tags - Unspent Outputs
Transactions
No. Transactions 2
Total Received 0.6819286 BTC
Final Balance 0 BTC
Request Payment
Donation Button
Transactions (Oldest First)
Filter
a7bb63ddf3da44988a43ae0544ca79fb3cd9d59567dfefe8474626a8695a1199
2018-04-12 05:14:11
mwv7br7jqzV1AYNsxA57oEAgVEw1FCYmkw
mx2ZnLrBtc4XMQhkWFg2PYqgUFo2MhmYRg
mkqQMcXftseBf5sRgtTv1qt2GXG3yqHbco
0.1 BTC
0.5818286 BTC
Unconfirmed Transaction!
-0.6819286 BTC
27c805f387d83021adf9e7631042e8bfb8218ed6a6b25d21fa00bd0bf10a4733
2018-04-12 04:30:18
myxTKQSUEdqFbpQ6DijRQCe72ZMM6snqGw
mwv7br7jqzV1AYNsxA57oEAgVEw1FCYmkw
0.6819286 BTC
3 Confirmations
0.6819286 BTC

Hierarchical Deterministic Wallet

Reload Page

Spendable balance found

0.6818286 BTC (pending, unspendable transactions don't show)

Receiving Addresses

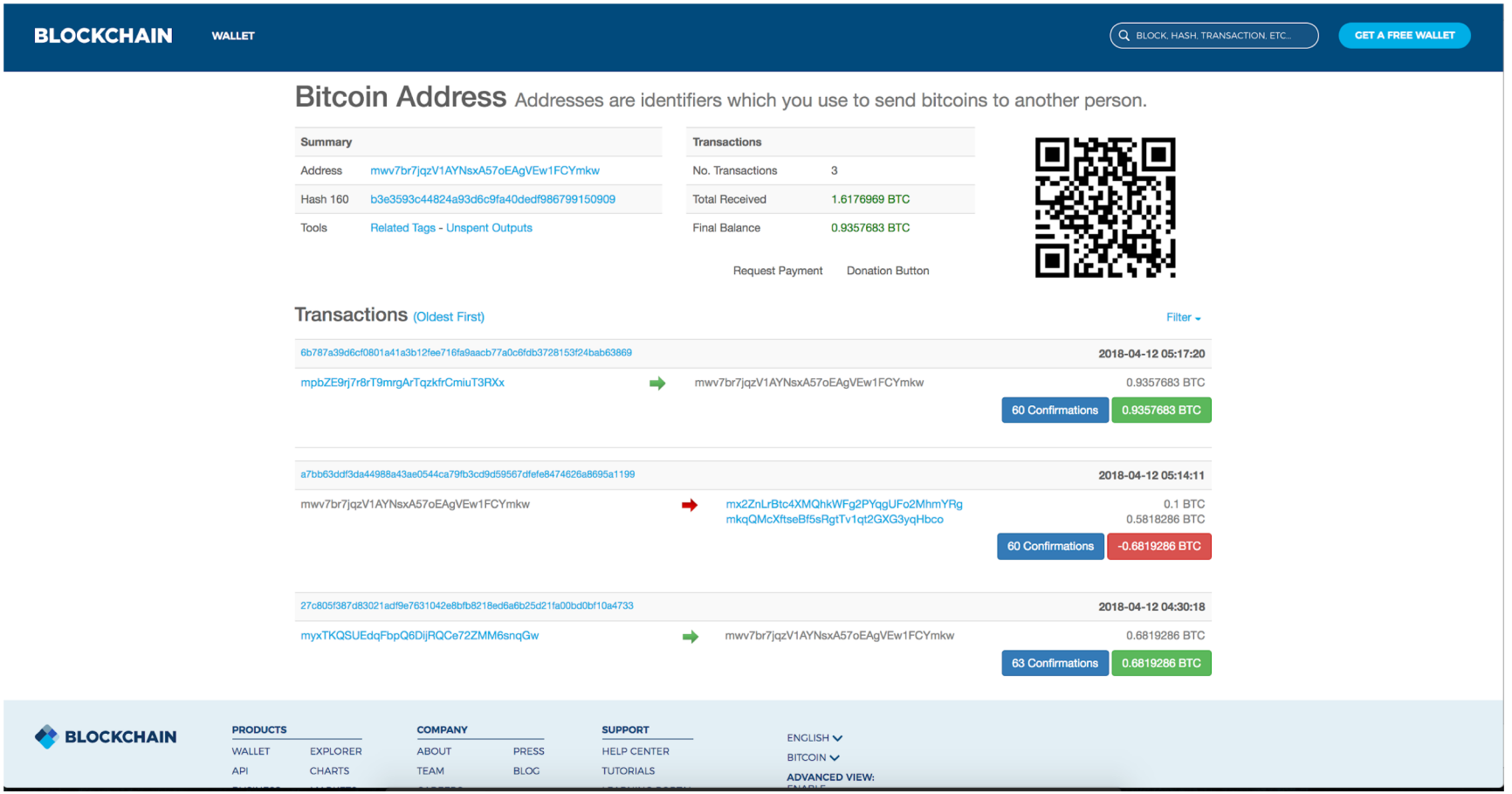
Receiving addresses are the addresses found on the external address chain (i.e. `m/i'/0/k` in BIP32 terminology). These should be used to to give to other people, where they can send payments.

#	Address	Balance (BTC)
0	mwv7br7jqzV1AYNsxA57oEAgVEW1FCYmkw	0
1	mh78ZcwaHQp6hYn5qKns3F3EnQdDBB1pan	0
2	mgMQLYLxEhnTVCqcLzJ2x9jaPQc14Z9DMn	0
3	mx2ZnLrBtc4XMQhkWFg2PYqgUFo2MhmYRg	0.1
4	mys5xCSokLr6zjXwnnTzQ16MbfRp8wuDqd	0
5	mmaiTYCKKBYMmDGZWTt12aQREy7EoNzZRA	0
6	mgMVWoYAu3yg1uYBUHGz8ikj28y5jCSYkZ	0
7	my5YdD6zVMs7PBARXDgp1i9MsZPTAyRk92	0
8	n2SnA2KxHY5pzRtjNcfozQSieaYWubSSEG	0
9	mjnhia7svazooJbAwz8oGoAzqs1GRgf6wK	0
10	mywlsB9DZg4XipnzgMGHX1XK4n4vCMqPXK	0
11	n2TaX8vz4pAn1AzhxbAxbdSDb8UWrBJ3kQ	0
12	mkWZ2vv76EUc91NoQmkeCar9yz777cJiYN	0
13	moB666p8sxLDgTAvJdTCZt6h6Sfy6syTBc	0

Change Addresses

Change addresses are the addresses found on the internal address chain (i.e. `m/i'/1/k` in BIP32 terminology). These should be used just by the wallet software (e.g. this page) to generate new address every time you have change from an outgoing transaction. Should not use them directly.

#	Address	Balance (BTC)
0	mkqQMcXftseBf5sRgtTv1qt2GXG3yqHbco	0.5818286
1	mszncgoqUSValeJLGtcBBraYWyUDe9LHBH	0
2	mh8SVp4UYegvD5QWsPLQn9N3byChAjNw9D	0
3	moNbhQAFjQcm5PsNVM38c23SHDjwtXfxUx	0
4	mmrzNcu7i91QLqXtn9BDMxChes28o3tooT	0


BLOCKCHAIN
WALLET
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE WALLET
Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.
Summary
Address mwv7br7jqzV1AYNsxA57oEAgVEw1FCYmkw
Hash 160 b3e3593c44824a93d6c9fa40dedf986799150909
Tools Related Tags - Unspent Outputs
Transactions
No. Transactions 3
Total Received 1.6176969 BTC
Final Balance 0.9357683 BTC
Request Payment
Donation Button
Transactions (Oldest First)
Filter
6b787a39d6cf0801a41a3b12fee716fa9aacb77a0c6fdb3728153f24bab63869
2018-04-12 05:17:20
mpbZE9rj7r8rT9mrgArTqzkfrCmiuT3RXx
mwv7br7jqzV1AYNsxA57oEAgVEw1FCYmkw
0.9357683 BTC
60 Confirmations
0.9357683 BTC
a7bb63ddf3da44988a43ae0544ca79fb3cd9d59567dfefe8474626a8695a1199
2018-04-12 05:14:11
mwv7br7jqzV1AYNsxA57oEAgVEw1FCYmkw
mx2ZnLrBtc4XMQhkWFg2PYqgUFo2MhmYRg
mkqQMcXftseBf5sRgtTv1qt2GXG3yqHbco
0.1 BTC
0.5818286 BTC
60 Confirmations
-0.6819286 BTC
27c805f387d83021adf9e7631042e8bfb8218ed6a6b25d21fa00bd0bf10a4733
2018-04-12 04:30:18
myxTKQSUEdqFbpQ6DijRQCe72ZMM6snqGw
mwv7br7jqzV1AYNsxA57oEAgVEw1FCYmkw
0.6819286 BTC
63 Confirmations
0.6819286 BTC
BLOCKCHAIN
PRODUCTS
WALLET
EXPLORER
API
CHARTS
COMPANY
ABOUT
PRESS
TEAM
BLOG
SUPPORT
HELP CENTER
TUTORIALS
ENGLISH
BITCOIN
ADVANCED VIEW:

Future work

- Multisignature transaction
- Seed Generation (Bitcoin improvement proposal 39)
- Secret sharing scheme

Thank you !