Sun City Computer Club

Crypto Currencies

Cyber Security Seminar Series

Questions, Comments, Suggestions welcomed at any time

Even Now

- Audio Recording of this session
- Use the link above to access MP4 audio recording

Bitcoin definition

- Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem.
- Money a medium of exchange
- a unit of account
- a store of value

- Fast, secure, borderless
- Virtual
- Transfer of value sender <-> recipient
- Digital keys prove ownership, unlock value
- Digital keys stored in digital wallet
- Ownership of digital keys allows transactions
- Distributed peer-to-peer ledger
- Created via mining

  Finding solution(s) to mathematical problem while processing transactions

  Replacing currency issuance and clearing

Bitcoin features

Digital currency mining

- Algorithms to verify and record transactions
- Algorithms adjust to add bitcoin every 10 minutes
- Algorithms adjust by half every 4 years
- 21 million bitcoin limit   by year 2140
- Diminishing rate -> deflationary

- Bitcoin protocol

  decentralized peer-to-peer network
- Blockchain

  Public transaction ledger
- Transaction script

  Decentralized transaction verification
- Distributed mining

  mathematical & deterministic issuance

- *Bitcoin: A Peer-to-Peer Electronic Cash System*
  Satoshi Nakamoto 2008
  Decentralized No Central Authority
  Distributed computation system *proof-of-work*
  Global *election -> Consensus*

Distributed computation increased exponentially

Satoshi Nakamoto s/he them ? 2011

Other uses: fairness of elections, asset registries, notarization, contracts, …

- Many implementations of bitcoin standard
- Can run on many platforms
- Three main forms of clients (peers)
- Full client

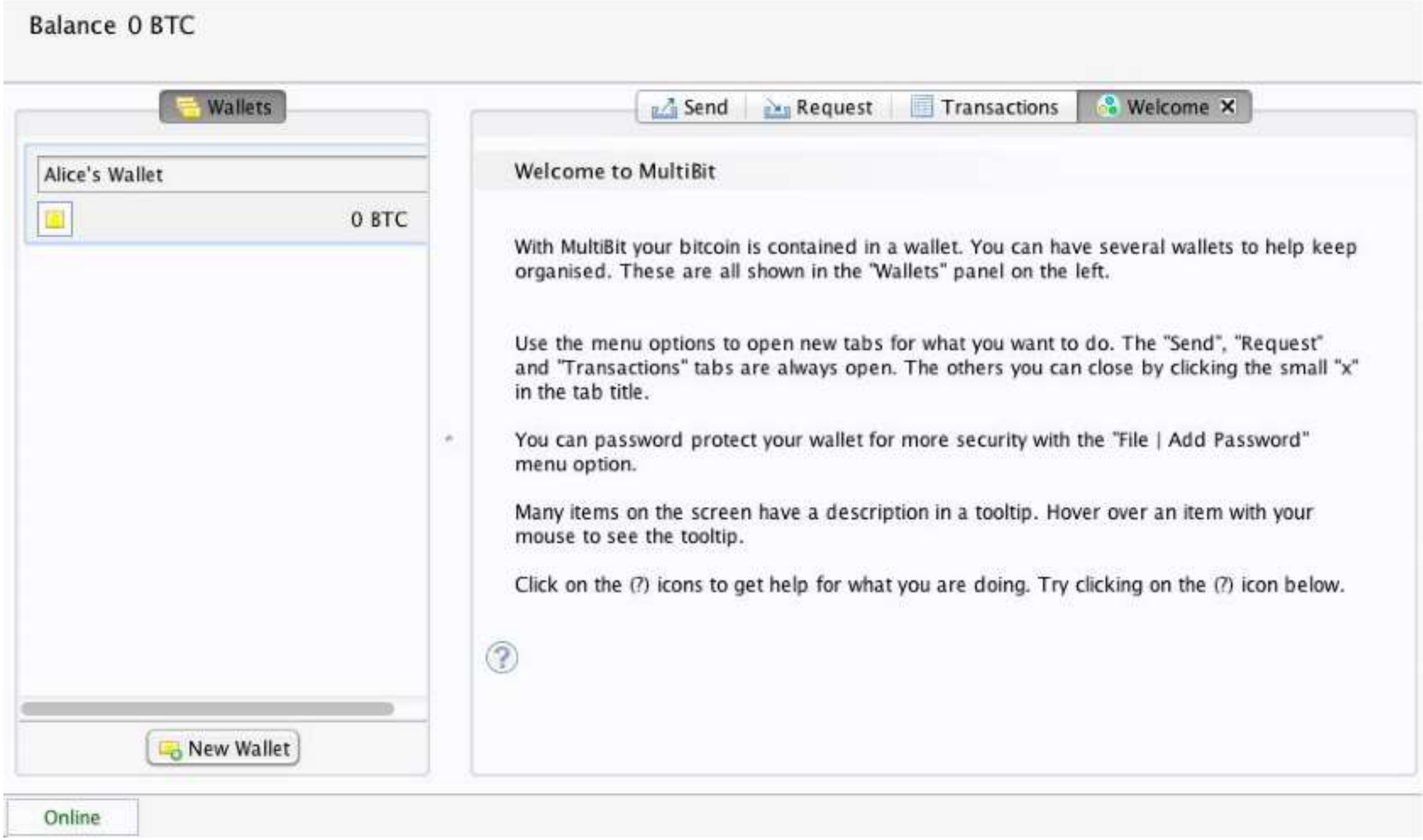
  every transaction
- Lightweight client

  wallet(s)
- WEB client

  third party owned client

- Digital currency is protected by digital means
- Can be instantly used by you or by *them*

WARNING WARNING WARNING



Welcome to MultiBit

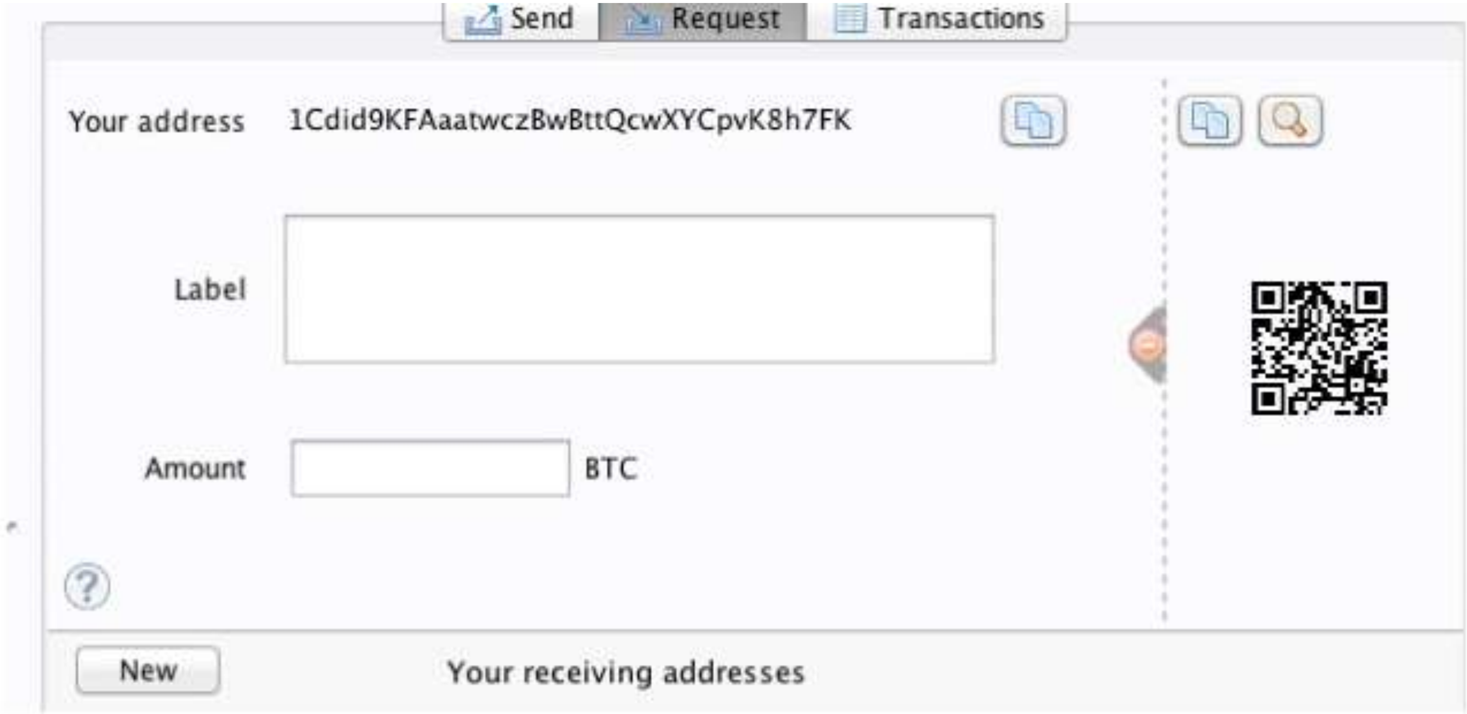
With MultiBit your bitcoin is contained in a wallet. You can have several wallets to help keep organised. These are all shown in the "Wallets" panel on the left.

Use the menu options to open new tabs for what you want to do. The "Send", "Request" and "Transactions" tabs are always open. The others you can close by clicking the small "x" in the tab title.

You can password protect your wallet for more security with the "File | Add Password" menu option.

Many items on the screen have a description in a tooltip. Hover over an item with your mouse to see the tooltip.

Click on the (?) icons to get help for what you are doing. Try clicking on the (?) icon below.

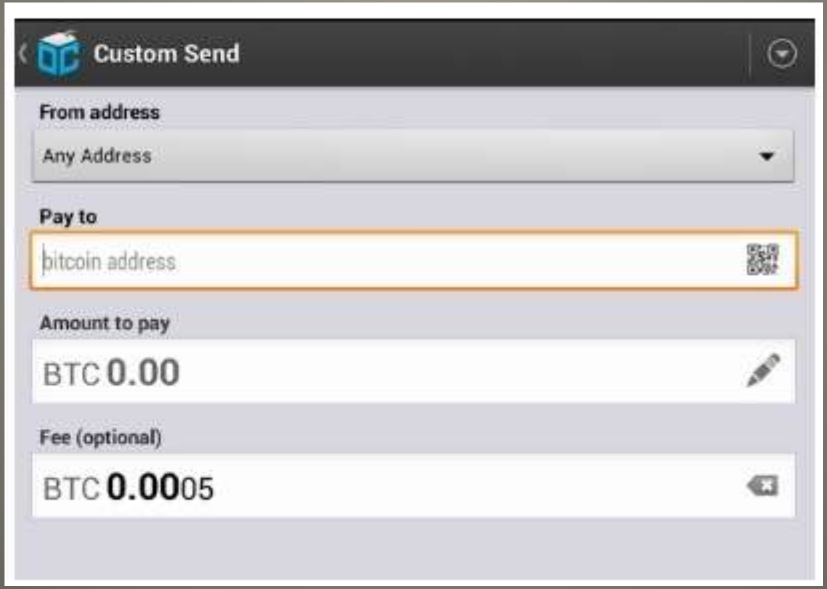


Your address 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

- Similar to physical wallet
- With differences
- Bitcoin address QR code
- Ability to create new bitcoin addresses
- Stored in digital wallet(s)
- Addresses and Keys
- Fund the desired address(es)
- Fiat currency exchange rate
- https://bitcoinwisdom.io/

Digital Currency Wallet

- Transfer to the bitcoin address
- Transaction amount
- Transaction signed by sender’s private key
- Bitcoin network propagates transaction



From address

Any Address

Pay to

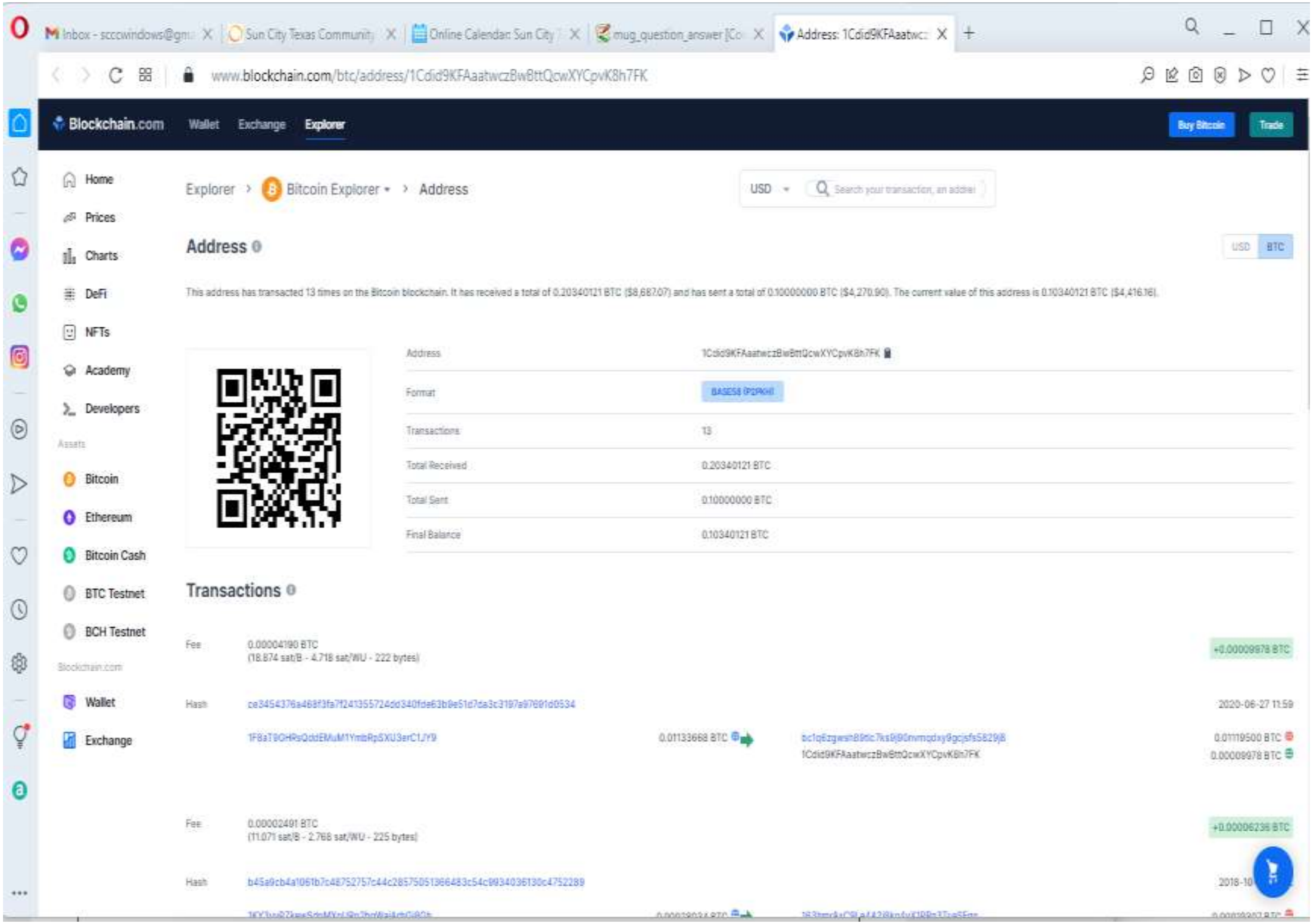
bitcoin address

Amount to pay

BTC 0.00

Fee (optional)

BTC 0.0005



Address

This address has transacted 13 times on the Bitcoin blockchain. It has received a total of 0.20340121 BTC ($8,687.07) and has sent a total of 0.10000000 BTC ($4,270.90). The current value of this address is 0.10340121 BTC ($4,416.16).

Address	1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
Format	BASE58 (P2PKH)
Transactions	13
Total Received	0.20340121 BTC
Total Sent	0.10000000 BTC
Final Balance	0.10340121 BTC

Transactions

Fee 0.00004190 BTC
(18.874 sat/B - 4.718 sat/WU - 222 bytes)
+0.00009978 BTC

Hash ce3454376a469f3fa7f241355724dd340fde63b9e51d7da3c3197a97691d0534
2020-06-27 11:59

1F8aT9GHRsQddEMuM1YmbRp5XU3erC1JY9 0.01133668 BTC → bc1q6zgwsh89tlc7ks9j90nvmqdxy9gcjsfs5829j8 0.01119500 BTC
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK 0.00009978 BTC

Fee 0.00002491 BTC
(11.071 sat/B - 2.768 sat/WU - 225 bytes)
+0.00006236 BTC

Hash b45a9cb4a1061b7c48752757c44c28575051366483c54c9934036130c4752289
2018-10

- Unconfirmed – propagated but unmined
- Confirmed – in newly created block
- Blockchain explorer – many examples
- Example: Retail purchase

  POS terminal Price $USD and BTC

  QR code

    Bitcoin address

    Amount

    Recipient address

    Payment description

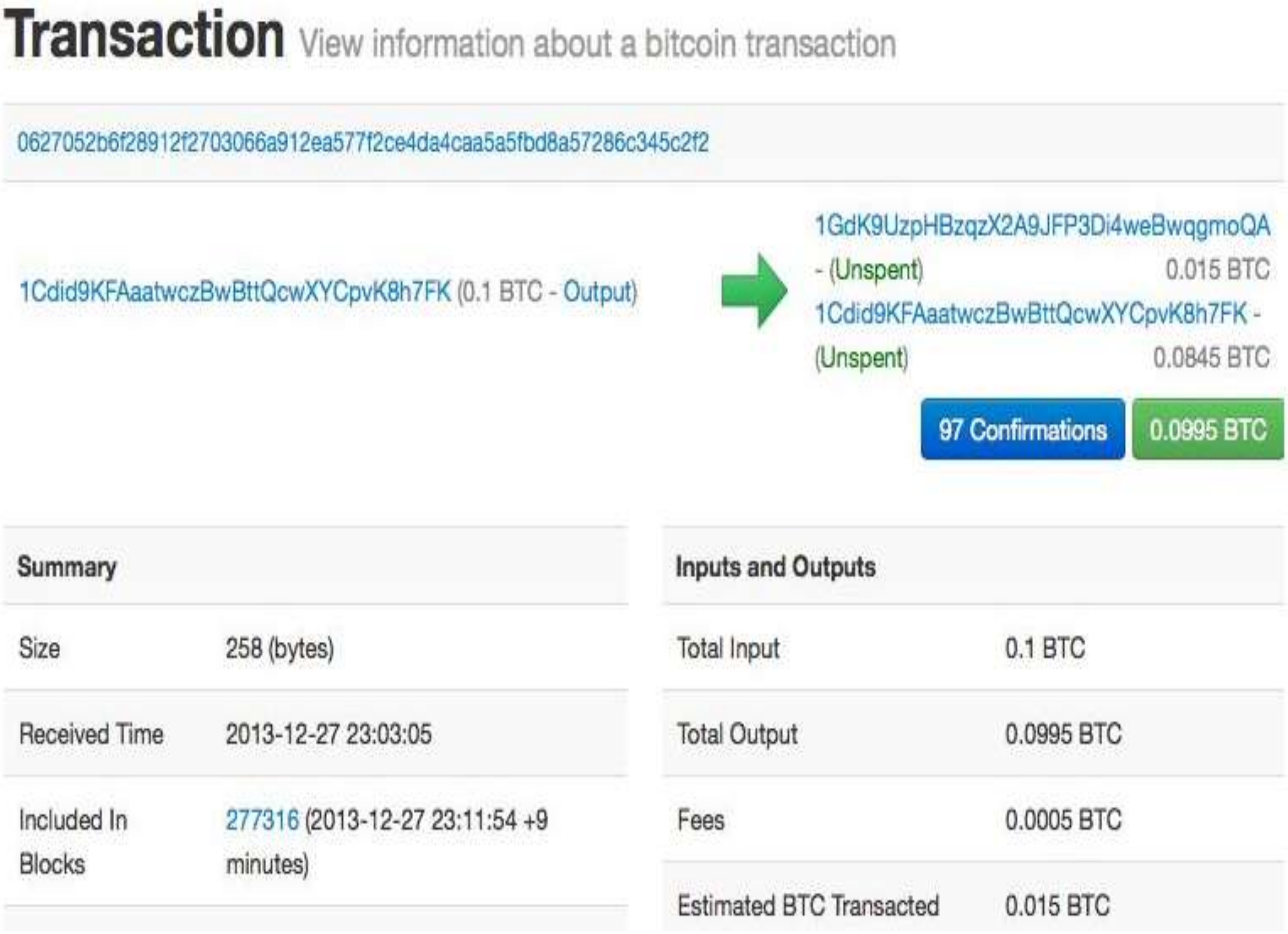
Transaction Life cycle

Transaction Life cycle

- Chain of transactions
- Spending – Sign the transaction
- Distributed ledger input & output
- Transaction fee
- Destination& key *encumbrance*
- Input -> Output (recipient)
  -> Output (sender) change
  -> Output transaction fee
- Transaction can be “offline”

- Transaction output created in form of script
- Script creates encumbrance on value
- Script can only be redeemed by script solution
- This output payable to signature from key corresponding to payee's public address
- Recipient's wallet
- Bitcoin change is second output back to sender
- Bitcoin network generates transaction fee payed to miner

Transition Life cycle



Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

Transaction Life cycle

- Transaction information 258 bytes in size
- Transmitted to peer-to-peer network

  Internet, wired, Wi-Fi, mobile, …

  first node sends this to all its connections

  those nodes send to all their connections

  a few seconds
- Recipient’s wallet “hey, that is for me”

  unconfirmed - may be spent if “small”

  transaction well formed

  uses previously unspent inputs

  contains sufficient transaction fees

Transaction Life cycle - Mining

- Mining based on computation
- Transactions bundled into blocks
  - Destined for blockchain inclusion
  - Very large computation effort to build/prove
  - Much smaller computation effort to verify
- Mining creates new bitcoins in new block
  - number of bitcoins created fixed
  - number of bitcoins diminishes with time
- Mining creates trust
  - Enough computation (proof of work)
  - More blocks > more computation > more trust

- Miners have new transactions AND copy of entire blockchain
- Proof of work – quadrillions of hashing operations
- Potential solution – eventually ~10 seconds

Transaction Life cycle Mining

Aside Computational difficulty

- A LOT of high-end PCs
- Specialized mining kit with GPUs
- ASIC chips

  Application Specific Integrated Circuits
- Mining pool
- Norton
- Botnet provided
- Environment impact Electricity & Minerals

Transaction Life cycle Mining

- Transactions not verified until published on blockchain
- Transactions flow in from peer-to-peer network
- Pool of unverified transactions
- This growing pool + hash of prior block
- That prior block changes
  i.e. added by another minor
  start all over again - you did not win
- Calculate potential next block – proof of work
- Add "reward" (25 BTC per block) currently
- Solution found – published to network
  solution verified by peer-to-peer network
- Start all over again

Transaction Lifecycle Mining

- The next block now used just verified block as its last block so trust builds
- Exponentially harder to reverse more trust
- Irrevocable after 6 or so

- Lightweight clients SPV

  Simplified Payment Verification

  In the blockchain with several blocks after
- Now available to “spend” new transaction

Transaction Life cycle

- Bitcoin full client

  Reference client

  transaction verification engine

  copy of transaction leger (blockchain)

  peer-to-peer network client

  blockchain “out of synch” for several days

  current size Jan 13, 2022 - 385.14GB

Wana play?

Wallets, Keys, Addresses

- Ownership
- Wallet – simple database
- Keys plural – other uses

Digital keys for cryptography functions

Hashing

symmetric encryption & decryption

asymmetric encryption & decryption

signing

tamper proofing

non-repudiation

Keys

- Keys
- Digital signature
  HASH then signed with public/private key
- Public key derives bitcoin address
- Bitcoin addresses can be otherwise derived

- Addresses
- Vanity addresses
- Application and scripts

Cryptography aside

- Hash

  one-way cryptographic function
  variable size input
  fixed size output
- Symmetric encryption – one key
- Asymmetric encryption – two keys

  based on mathematical intractable function
  prime number factorization
  elliptic curve multiplication
  private/public one derives the other

- Public/Private keys
- Stored together
- or derive public from private
- Public key -> bitcoin address
- Private key -> signing (different at each use)
- Public key + signature => ownership
- BACKUP & PROTECT !!
- Lose your keys/wallet real world
- Same Same bitcoin

Keys

Generate private key

- Randomness is important!
- 256-bit number
- Private key space 2^{256}
- Large number 10^{77}

number of atoms in universe 10^{80}

example

1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD

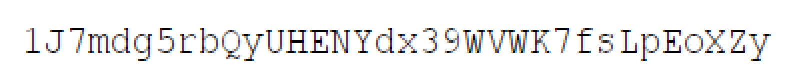
Public key K = k * G

k – private key

G – generator point

elliptic curve multiplication - irreversible

Bitcoin address

- Example 

  1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy

  Starts with digit 1

  Generated from public keys

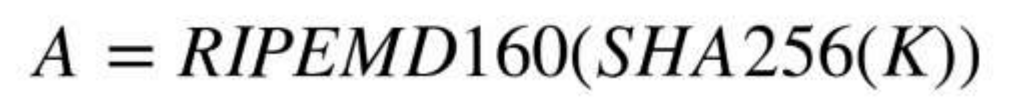
  or

  something else - e.g., payment script

  Secure Hash Algorithm SHA

  RACE Integrity Primitives Evaluation Message Digest

  RIPEMD 160



$$A = RIPEMD160(SHA256(K))$$

- 58 characters + checksum
- Radix 8 – octal
- Radix 10 – decimal
- Radix 16 – Hexadecimal
- Base 64 26 upper 26 lower 10 numerals 2 special
- Base 58 – Base 64 – o 0 1 l

- Base58Check adds 4-byte checksum
- Bitcoin address
- Fixed prefix + data + checksum
- Prefix => type of bitcoin address

Base58Check

Wallets

- Bitcoin wallets contain keys

  usually on keychains

  No Bitcoins Keys

  The coins (currency) are on the blockchain
- Nondeterministic wallets

  100 random private keys

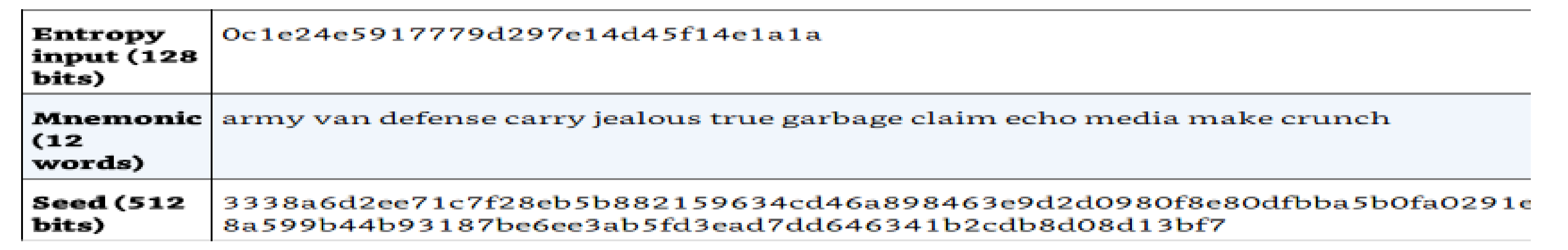
  each key used once (typically)

  Just a Bunch of Keys JBOK

  Backup of JBOK

  Type-0 wallet
- Deterministic (seeded) wallets

- Deterministic (seeded) wallets
  - all keys derived from a common seed
  - a single backup
  - seeded sufficient for wallet import/export
  - Mnemonic codes
    - allow re-creation of wallet and seeds
    - 12 to 24 words

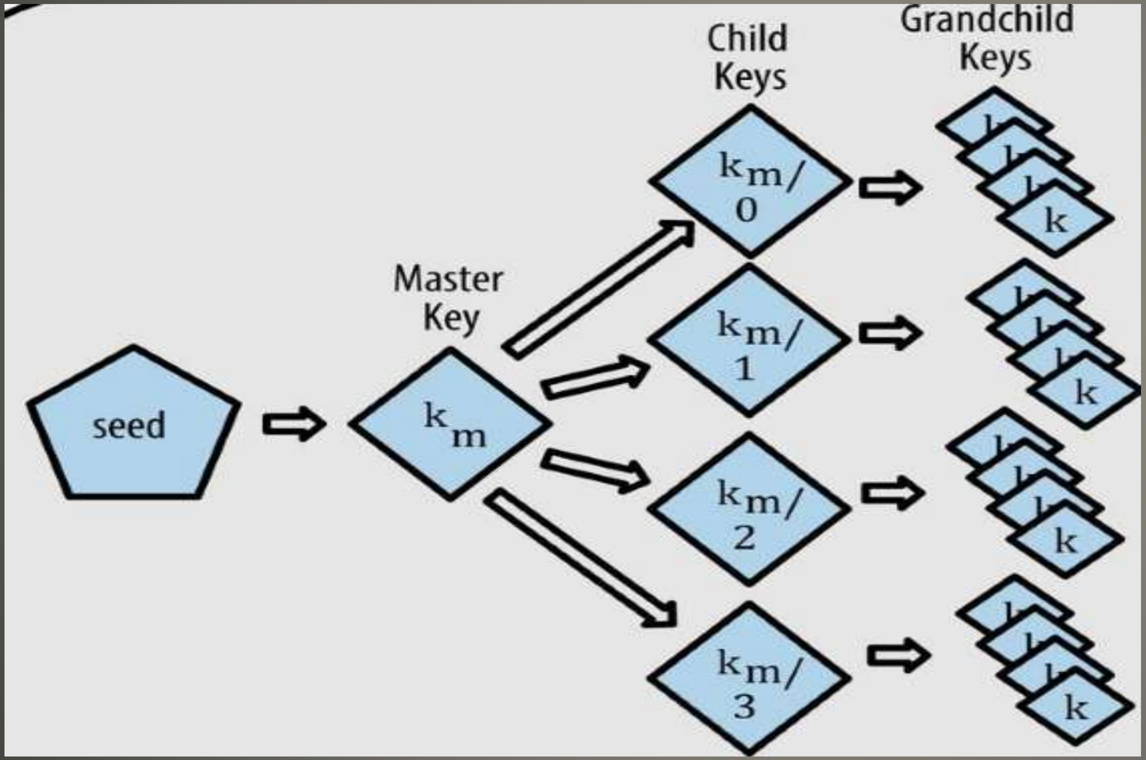


Entropy input (128 bits)	0c1e24e5917779d297e14d45f14e1a1a
Mnemonic (12 words)	army van defense carry jealous true garbage claim echo media make crunch
Seed (512 bits)	3338a6d2ee71c7f28eb5b882159634cd46a898463e9d2d0980f8e80dfbba5b0fa0291e 8a599b44b93187be6ee3ab5fd3ead7dd646341b2cdb8d08d13bf7

Wallets

- Hierarchical Deterministic Wallets

  Tree structure



Wallets

Hierarchical Deterministic Wallet

- Tree structure maps to organizational structure
- Allows creation of sequence of public keys without access to private keys.

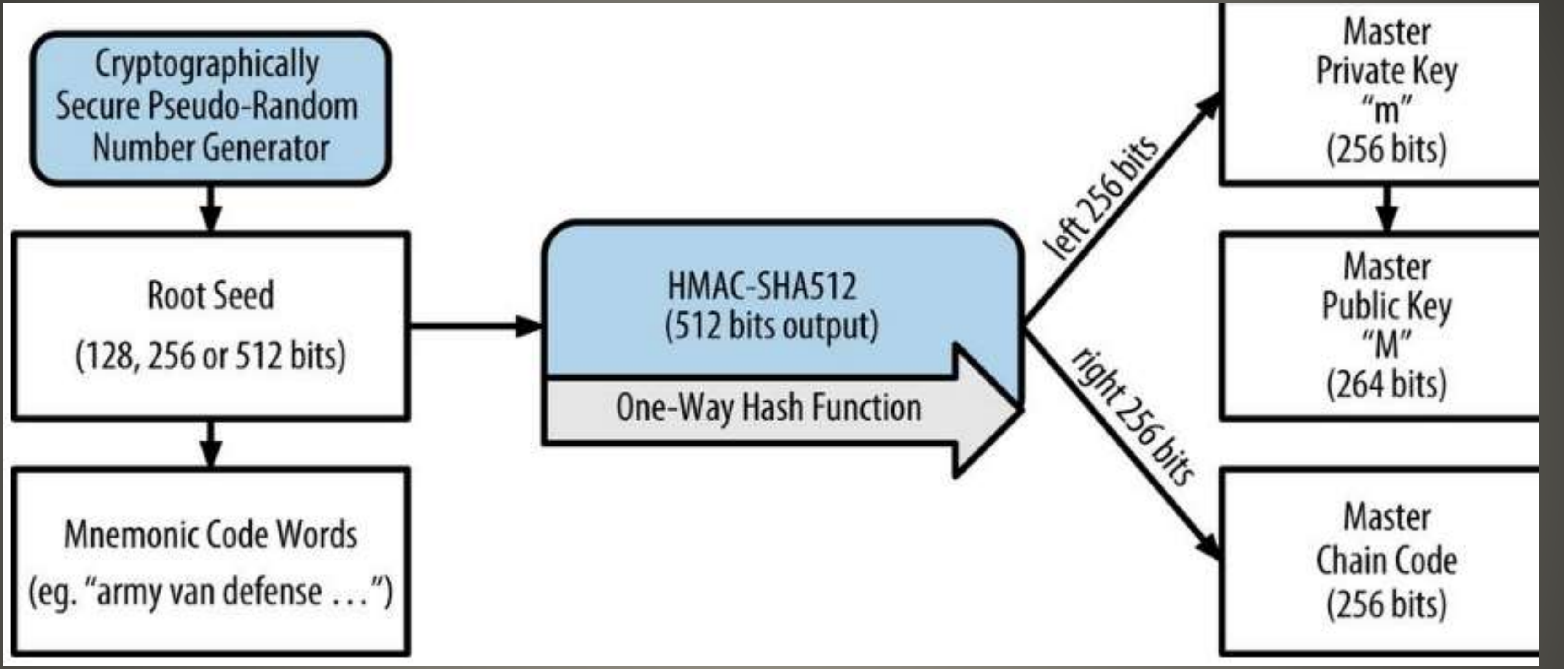
Allows insecure server

Allows receive-only wallet

Often referred to as HD wallet

Hash gives master private key
and master chain code

These generate master public key


Cryptographically Secure Pseudo-Random Number Generator
Root Seed
(128, 256 or 512 bits)
Mnemonic Code Words
(eg. "army van defense . . .")
HMAC-SHA512
(512 bits output)
One-Way Hash Function
left 256 bits
right 256 bits
Master Private Key "m" (256 bits)
Master Public Key "M" (264 bits)
Master Chain Code (256 bits)

HD wallet generation from seed

- Child key
- Inputs:

  Parent private or public key

  Seed (chain code - 256 bits)

  index number (32 bits)

  Child key then used as parent key to generate more children keys …

  Requires parent key and chain code

  Can not use child code to determine parent code or sibling codes

Extended key = child key + chain code

Extended private key

Extended public key

HD Wallet Private child key derivation

HD wallet advantages

- Deploy large numbers of public child keys without knowing private keys

  Very secure public key deployments

  large number of public key and bitcoin addresses

  Unable to spend any coin sent to those addresses

  Extended private can derive private keys to sign transactions

Encrypted private keys

- Confidentiality vs availability
- Backup
- Backup protection
- Private keys prove ownership by their knowledge or possession
- Wallet protection by password
- Password
- Backups now multiple protection issues

- BIP0038
- Common standard

  encrypt private keys with passphrase

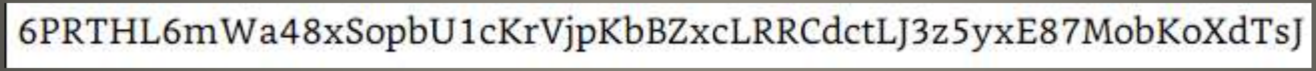
  encoding with Base58Check

  Stored on paper Paper Wallets

  USB Cold Storage

  Input WIF (wallet Import Format)

  Output Base58Check with *6P* prefix



6PRTHL6mWa48xSopbU1cKrVjpKbBZxcLRRCdctLJ3z5yxE87MobKoXdTsJ

Bitcoin Improvement Proposal 38

- Private Key -> Public key -> Bitcoin address
- Bitcoin address starts with 1

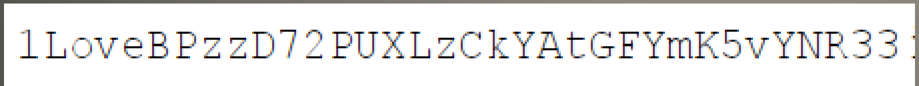
- Bitcoin address starting with 3

  Pay-to-script addresses

  Multi-signature M-of-N

- Vanity bitcoin addresses

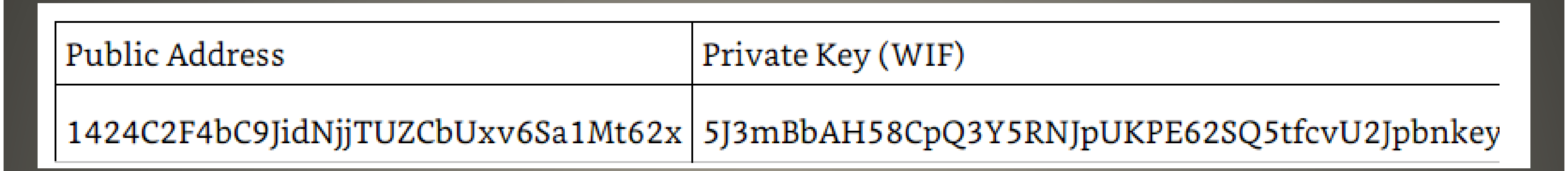
  Trial and error   resemble vanity address



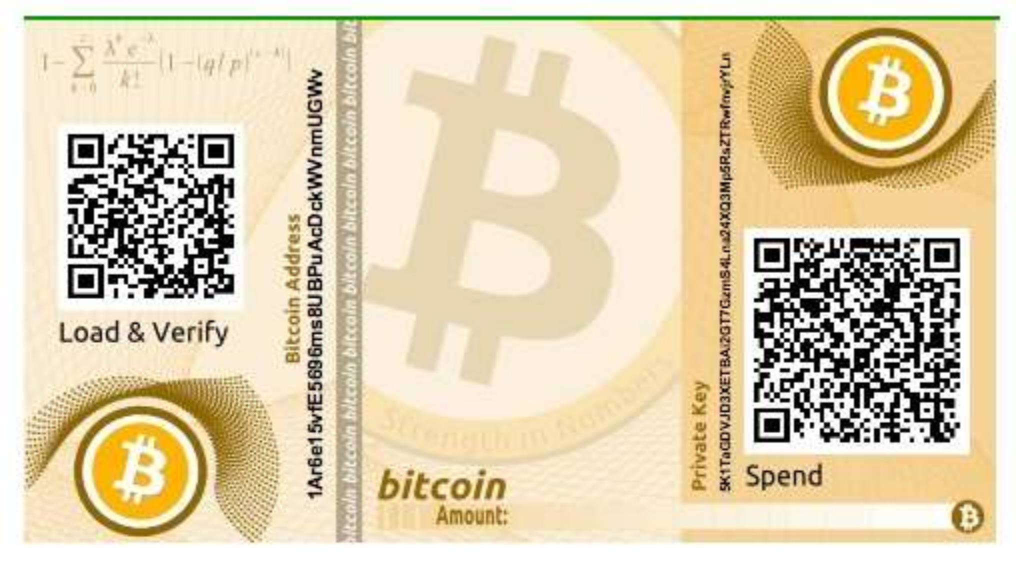
1LoveBPzzD72PUXLzCkYAtGFYmK5vYNR33

Bitcoin address variations

- Printed on paper
- Cold Storage



Public Address	Private Key (WIF)
1424C2F4bC9JidNjjTUZCbUxv6Sa1Mt62x	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2Jpbnkey


Load & Verify
Bitcoin Address
1Ar6e15vfE5696ms8UBPuAcDckWVnmUGWv
bitcoin bitcoin bitcoin bitcoin bitcoin bitcoin
Strength in Numbers
bitcoin
Amount:
Private Key
5K1TaGDVJD3XETBAi2GT7GzmS4Lna24XQ3Mp5RsZTRwfnwjrYLn
Spend

Paper Wallets & Cold Storage

Paper Wallets & Cold Storage

- Offline theft methods
- Copy paper, photograph of paper
- Use BIP0038 – now needs the passphrase
- Never been online
- Scratch off sticker

Bitcoin and real-world analogies

- Paper check/cheque

  Created by anyone – not necessarily the signer

  Not known by network until signed and submitted
- 300 to 400 bytes
- Tens of thousand bitcoin nodes
- Transaction contains no

  confidential information

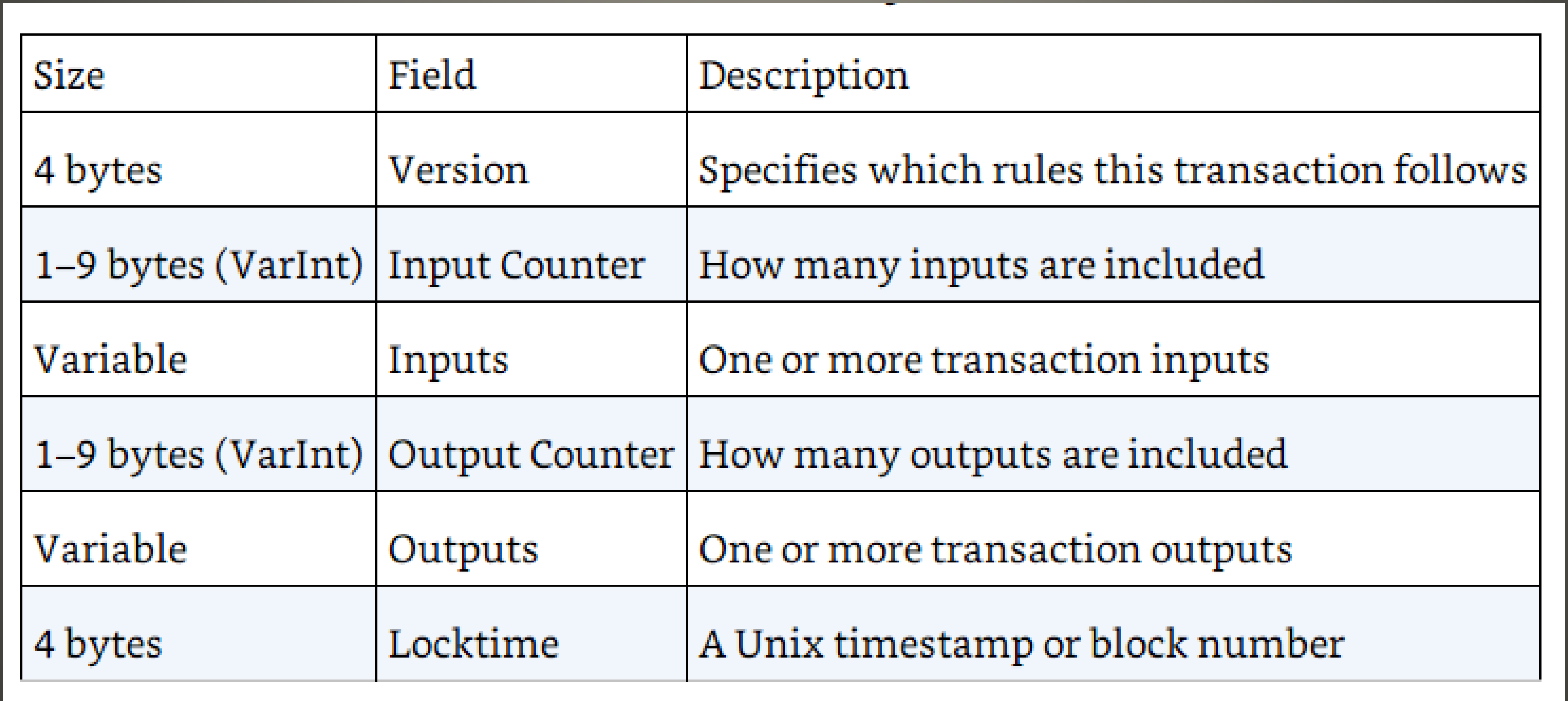
  private keys

  credentials

  so broadcast over public network

  unlike credit card transaction or check
- Currency now a data structure

- Bitcoin network mesh w/o structures
- Each node validates each transaction before forwarding



Size	Field	Description
4 bytes	Version	Specifies which rules this transaction follows
1–9 bytes (VarInt)	Input Counter	How many inputs are included
Variable	Inputs	One or more transaction inputs
1–9 bytes (VarInt)	Output Counter	How many outputs are included
Variable	Outputs	One or more transaction outputs
4 bytes	Locktime	A Unix timestamp or block number

- Unspent Transaction Output

  UTXO

  Undividable chunks

  Wallets balance derived by scanning blockchain

  Coin divided to 8 decimal places   Satoshi

  UTXO NOT - you get change

  Consume UTXO – unlock with owner's signature

  Create UTXO lock to new owner's bitcoin address

  Coinbase transaction – created by miners

  Currency creation

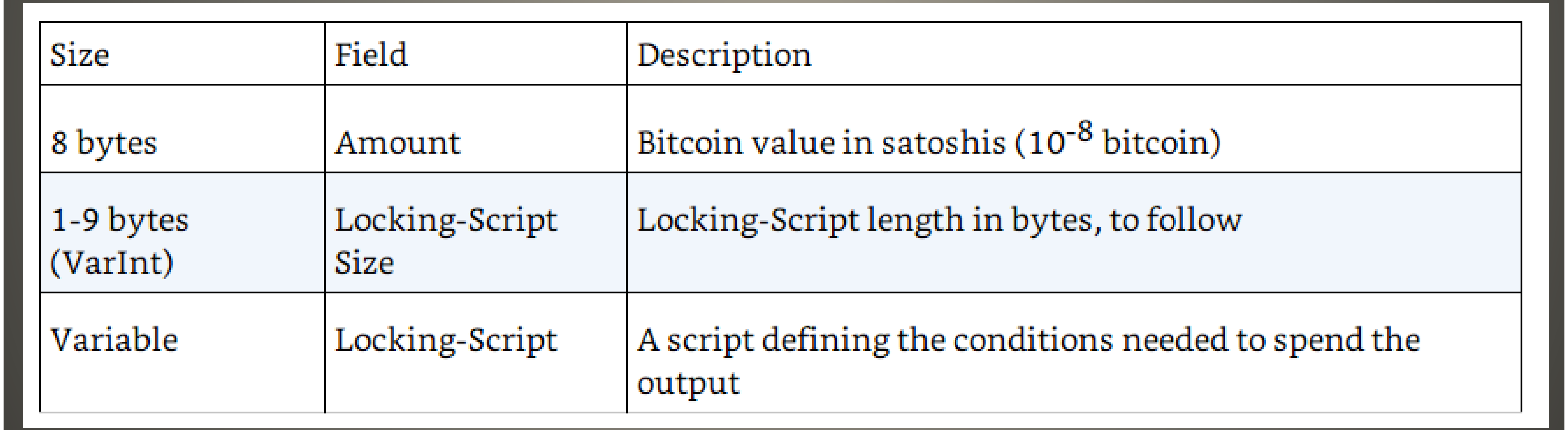
Transaction units

Transaction Output

- Amount in Satoshis
- Locking script

  conditions for spending

  encumbrance



Size	Field	Description
8 bytes	Amount	Bitcoin value in satoshis (10^{-8} bitcoin)
1-9 bytes (VarInt)	Locking-Script Size	Locking-Script length in bytes, to follow
Variable	Locking-Script	A script defining the conditions needed to spend the output

Transaction

- Spend
  coin locked to recipient's bitcoin address
  coin unlocked with private key
- Collect available UTXOs
- Get change
- Pay transaction fee
  Fees based on size & "market forces"
  Not mandatory
  Fees = Sum (Inputs) – Sun (outputs)
  including change
  20 UTXO to spend 1 payment needs 20 change outputs plus fees
  OR "keep the change" as fees
  Many small inputs => larger size transaction
  thus, larger fees

Transaction complexity

- CoinJoin – privacy protection
- Parent – child – grandchild

  arrival out of sequence

  orphan transaction pool

  size of pool limited to avoid denial of service attack

Transaction scripting

- Simple Pay-to-Public-key-hash
- Complex

- Locking and Unlocking scripts

- *Script* Forth-like reverse Polish
  Shared stack
  Stateless
  No loops

Other transaction types

- Pay-to-Public-Key-Hash (P2PKH)
- Multi-Signature
- Data Output
- Pay-to-Script-Hash (P2SH)

- Peer-to-peer
- Bitcoin P2P protocol
- Stratum – mining
- Routing
- blockchain database
- Mining
- Wallet services

- Full nodes
- Simplified Payment Verification (SPV)
- Lightweight
- Mining

Bitcoin network

New node

- Handshake
- IP address exchanges

- Genesis block
- Build chain as peer list grows

- Probabilistic search filter
- Privacy protection

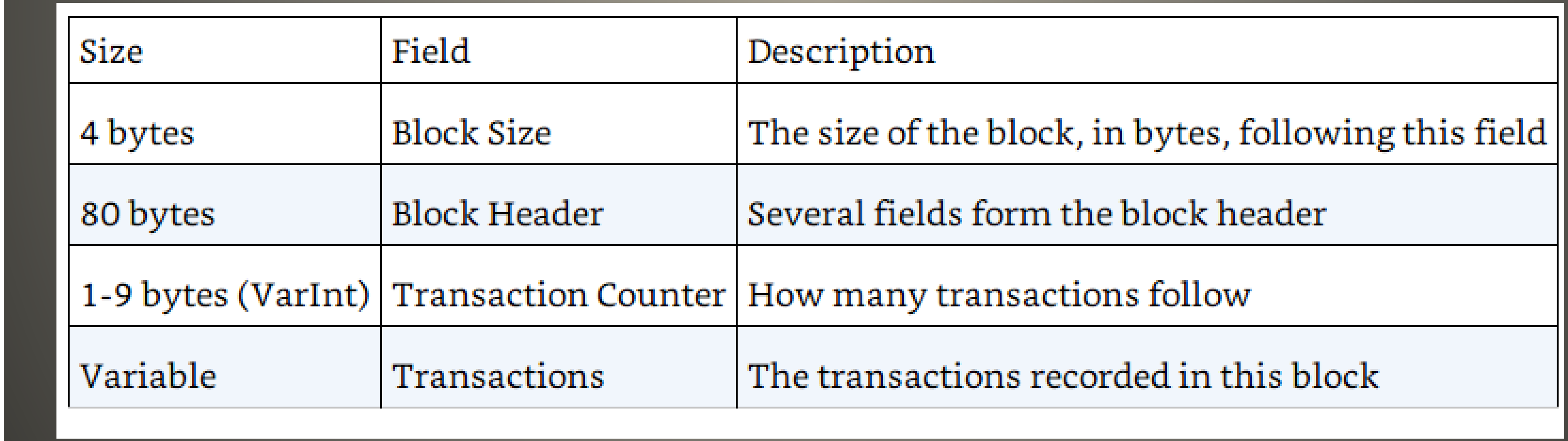
Bloom filters

Transaction pools

- Temporary list
- Pending or incomplete transactions

- Block header has hash of parent block
- Block can have several child block candidates – forks

  Resolved
- Block header 80 bytes



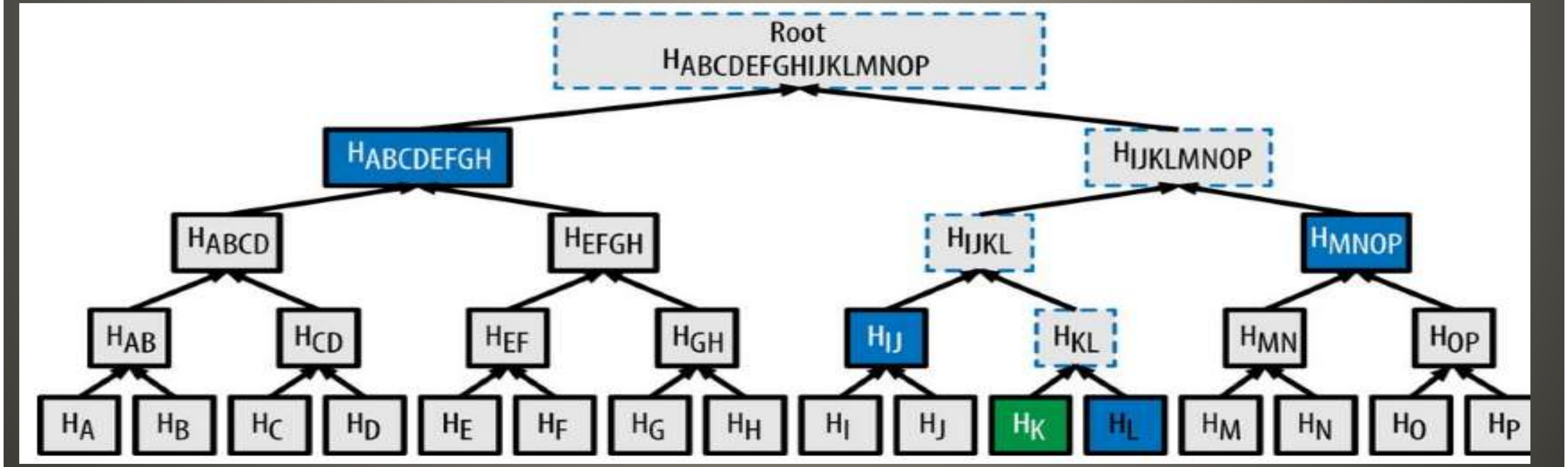
Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Blocks & Blockchain

- Block hash
- Block “height”
- Genesis block
- text “The Times 03/ Jan/ 2009 Chancellor on brink of second bailout for banks.”

Blocks and Blockchain

- Merkle Trees   binary hash tree
- Summary of all transactions in block
- Merkle root 32 bytes
- Specific transaction in this block?
- Authentication path Merkle path



Merkle Trees

- “Hey, have my transaction(s)?”
- Bloom filter privacy
- Peer node responds with *merkleblock*

  block header & Merkle path

  1 KB vs 1MB

Simplified Payment Verification nodes

Mining

- New coin added to blockchain
- Bitcoin reward for first to create
- And validate all transactions to be added
- And fees
- Solve difficult mathematical problem
- Solution to proof of work
  yields new coin and fees
- 50 bitcoin per block + fees 2009
- 25 bitcoin per block + fees 2012
- 12.5 bitcoin per block + fees 2016
- By 2140 just fees 21million limit
- Deflationary due to diminishing supply
- Universal “truth” without trust

Mining

- Each & every peer-to-peer node
- Acting on information transmitted over insecure network
- Arrives at same conclusion

  emergent consensus
- Independent verification of each transaction
- Independent aggregation transactions > blocks
- Independent verification of new blocks building chain
- Independent selection of every node with most cumulative computation demonstrated through proof of work
- Long checklist of criteria
- Transaction Age, Fees, Priority
- Miners balance these to construct candidate blocks

- Generation transaction – pay the miner pay miner wallet 25.09094928 bitcoin
- Construct block header
- Hash, check, change a parameter, hash, check, ……
- Quadrillions
- 100 petahashes per second

- Difficulty target

New Difficulty = Old Difficulty * (actual time of last 2016 blocks / 20160 minutes)

related to electricity cost and exchange rate of bitcoin to pay for electricity

Mining

- Bing Bing – I found candidate block
- Oh yeah – send it over
- Peers validate just found candidate block
- Looks good to me, what do you think?

-or-

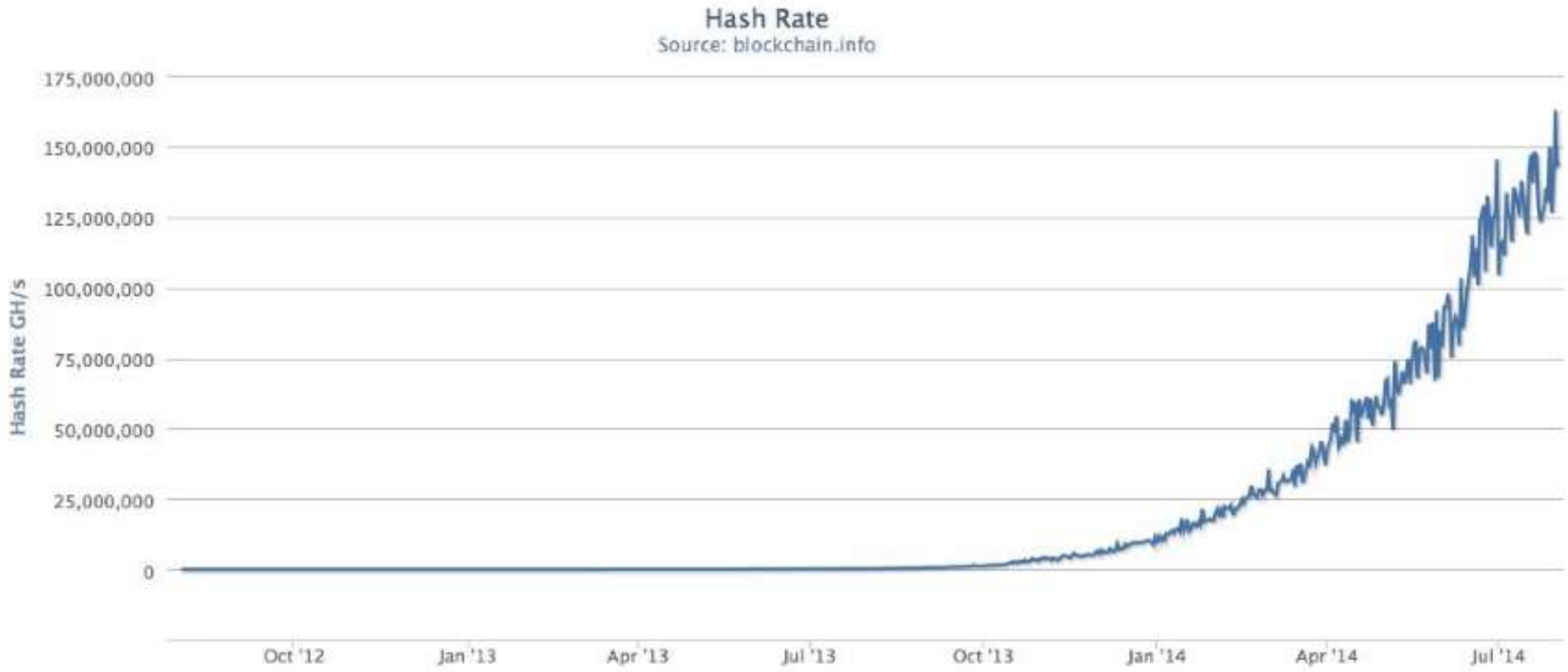
REJECTED try again

Miner’s time + expenses wasted

If valid, add to block chain

Start process yet again

Mining

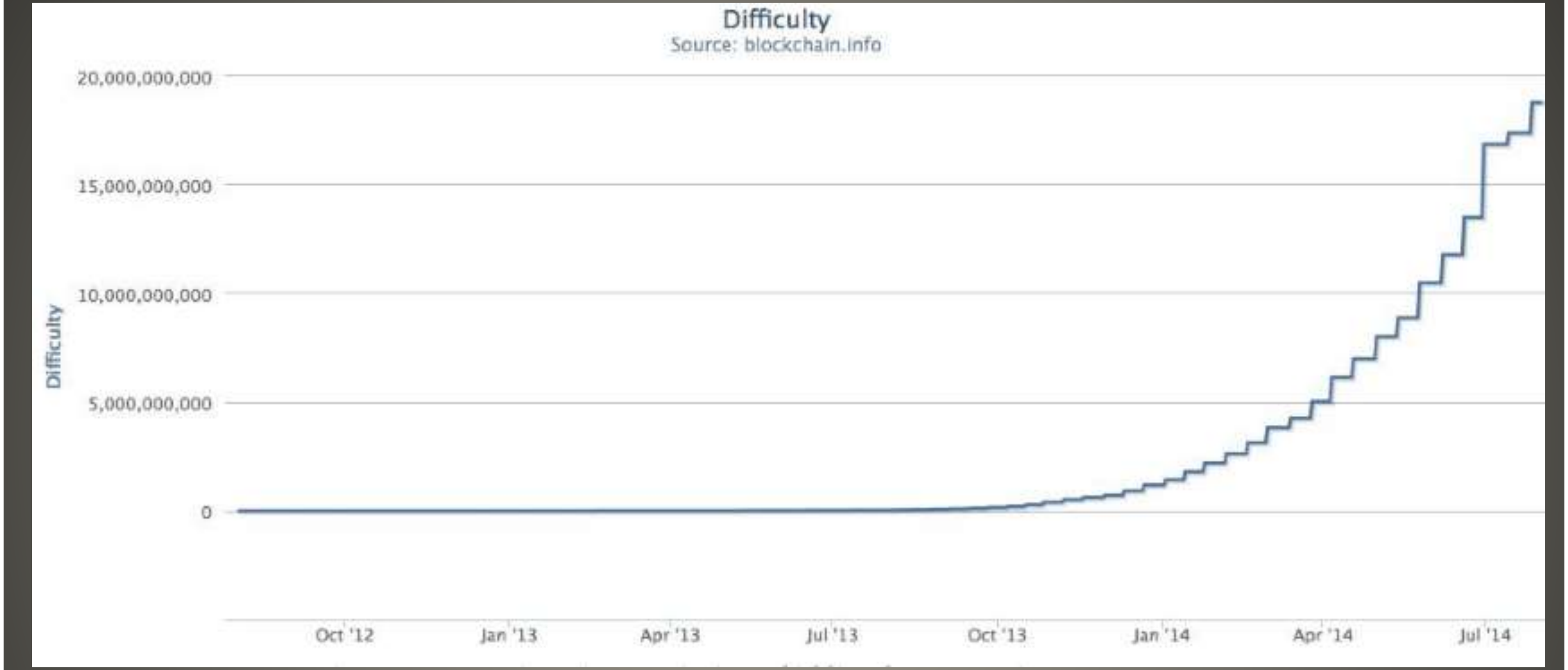


Hash Rate

Source: blockchain.info

Figure 8-7. Total hashing power, gigahashes per second, over two years

Mining & hashing race



Mining & Difficulty

- Warehouse filled with ASIC mining chips
- Located near power plants

- Construct pools
- Split the mining reward

- Join a pool
- Pool joins you

Mining Pools

- Colored Coins

meta protocol to layer small snippets of information on bitcoin. *Free magazine*

- Counterparty

Other currencies

- Namecoin, IXCoin, Tenebrix, Litecoin,

50 or so

Crypto.com

10 million users, 3000 employees

Domain name $10 Million

Rename of Staples Center

Matt Damon brand ambassador

Sponsorships Formula One, Philadelphia 76ers, Montreal Canadians, Water.org

AND others

Bitcoin Security

- Digital cash
- Like information it gives no indication of being stolen – cloned

Information has mass, motion, topography

- Relies on possession and protection of keys
- Keys can be backed up - unlike cash and money
- Possession is ten-tenths of the law
- Lose it, misplace it, have it stolen, give wrong amount, …
- Credit card “open ended”

Stolen at rest or in transit

Identity theft (cloning)

Bitcoin Security

- Bitcoin transaction

Authorizes specific value to specific recipient

Can not be easily forged

Does not reveal any Personal Identifiable Information

YOU are souly responsible

Private key protection relies on cyber hygiene

Hacked bitcoin exchanges

Theft Instant

Theft irrevocable

No money laundering required

Hardware wallets Trezor

Bitcoin Security

- Diversification
- Multi signature
- Survivability private key
  Digital Asset Executor

NFT

- Non-fungible token

  unique and non-interchangeable unit of data

  usually associated with reproducible data

  blockchain

  "there are many like it, but this is MY NFT"

  authorship, ownership chain, history, etc.

  u can prove this by looking up xyzfu423955jftuitrtuihvftgkoye on CL1T Blockchain V2.

- Social media create, buy & sale NFTs

What is crypto currency anyway?

- Satoshi Nakamoto

  secure without the need to trust third party middleman

  Secure individual transactions

  Verifiable record keeping capability
- OR bubble, Ponzi scheme, environmental disaster

- Maintain value
- Universally accepted as payment
- Measure of earnings, expenses, debts, assets
- Medium of exchange

- Anonymity

- Gold? E-Gold 1996
- *Electronic claim checks*
- Payments & users anonymous
- Company could not be

Currency

- Bitcoin 2019
- Supply limitations – retain value

  21 million bitcoins

  25 new coins created every 10 minutes
- Cryptographic hash functions
- Public/Private cryptography
- Blockchain

Ethereum

- Blockchain to define, enforce, contracts
- Smart contract functionality
- Ether
- Decentralized application platform
- Financial service

  Borrow, collect interest
- NFTs
- 15 transactions/sec -> tens of thousands/sec

Other Blockchain uses

Some more

- Immune from counterfeiting
- Cash & commodity
- A first purchase

  2 takeout pizzas 10,000 bitcoin

  $939 million today

  Satoshi Nakamoto

  Samsung Toshiba Nakamichi *Moto*rola ?
- Unlick stocks, no fixed trading hours
- You store/guard Your cryptocurrencies

- Recalls
- Logistics
- Supply chain food (wild salmon or farmed)
- Education

Blockchain

- Our thanks for viewing a presentation In Cyber Security SIG Seminar Series

- Topic suggestions are most welcome

scccyber@gmail.com