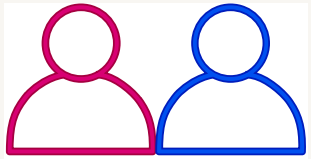
CSE446: Blockchain & Cryptocurrencies

Lecture – 7: Bitcoin - 1

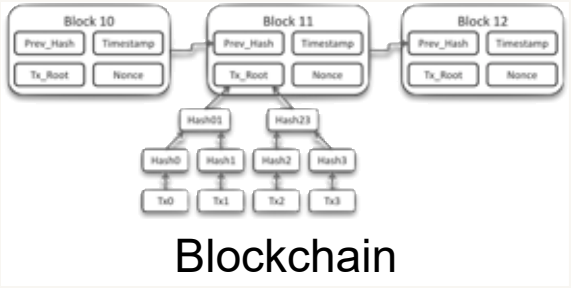
Agenda

- Bitcoin
- Bitcoin components
  - Users & Wallets
  - Nodes and network

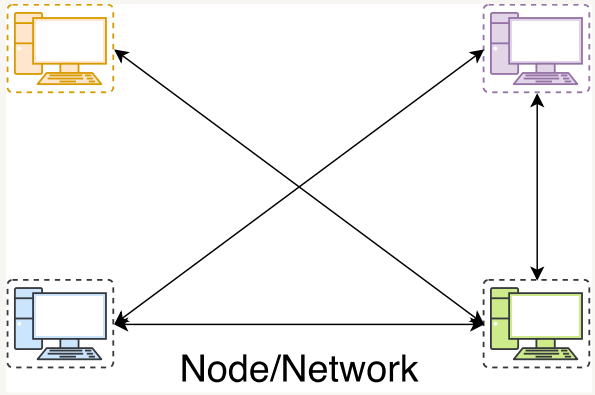
Bitcoin/Blockchain components



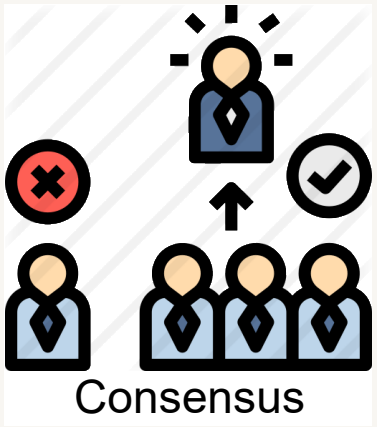
Users



Blockchain



Node/Network



Consensus

Decentralised Identity

- Proving the identity of users is a must in many online services
- To create an identity, you need to register to the Service Provider (SP)
- An identity requires a unique identifier to uniquely identify an entity within the system
  - Username -> unique only within a system
  - Email/mobile phone number are universal identifiers
- These identifiers need to be accompanied by a credential (e.g. a password) to prove the ownership of the identifier
- But all these need to rely on a specific SP
  - For emails, it is the Email provider and so on, if such an SP ceases to exist, all services dependent on the identifiers become vulnerable

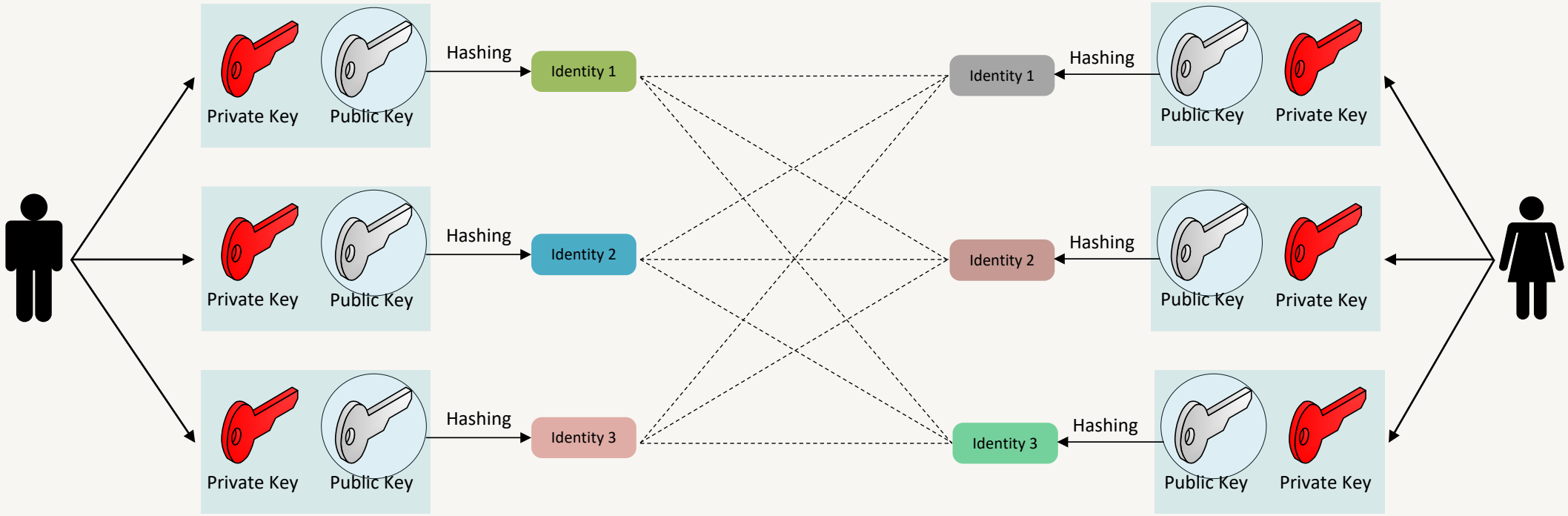
Decentralised Identity

- Decentralised identity is the solution using public key schemes
  - The public key *pk* acts as an identity
  - The private key *sk* is the password to prove the ownership of this identity
- This has some advantages:
  - New identities can be generated at will with the *generateKeys* function
  - Also, these new identities cannot be used to uncover your real-world identity, providing a layer of pseudonymous privacy

Decentralised Identity

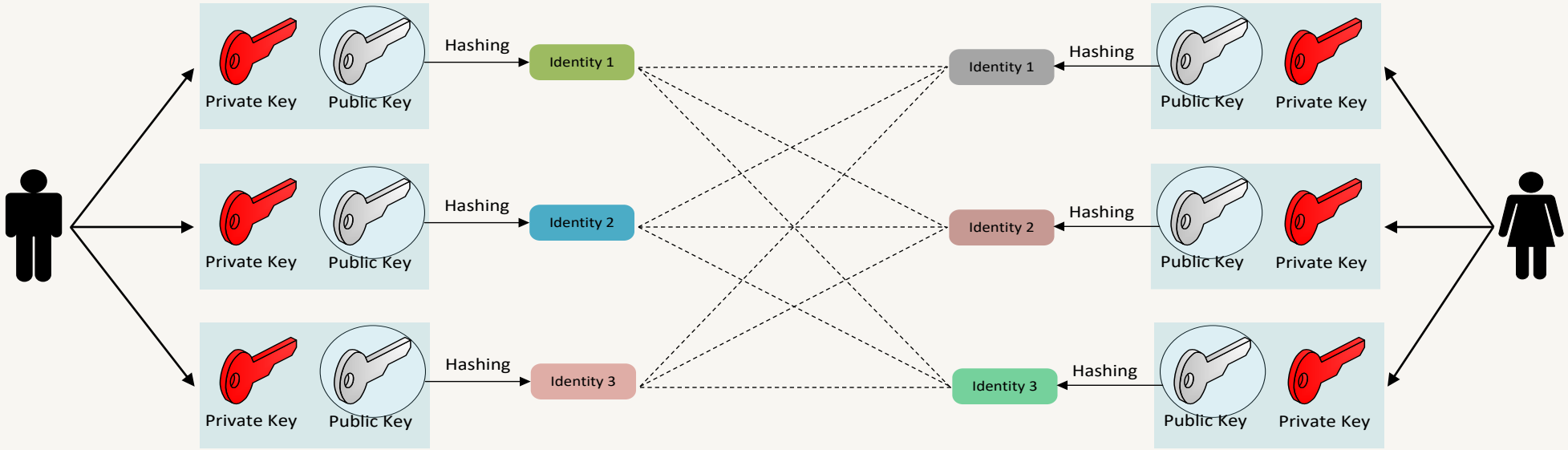
- Public keys are very large
  - You want to hash your public key (pk) to receive an “identity”
- To validate a statement, one must check
  1. if the pk hashes to the identity and
  2. if the message verifies under the public key pk

Decentralised Identity



Almost all (public) blockchain systems adopt this approach

Users



- Public key is used for creating identities
- Such identities can be vetted by a CA (Certificate Authority) for private blockchain systems

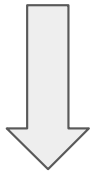
Users

- Bitcoin represent users anonymously
- However, there must be a way to identify a user
- Each user is represented using **an address**, generated by public key cryptography
- Bitcoin uses an elliptic curve (secp256k1) for its public key cryptography
- A user generates a key pair (k_p, k_s)
  - k_p -> represents a public key
  - k_s -> represents a private key
- An **address** can be generated from the public key
- A user **receives** coins with the address
- A user **spends** coins with the private key

Bitcoin address

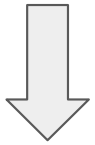
Private key:

5JXesisRRU2Z7HMmwMpNtoiYk1QDMVjV3HLoYMd1PTKEkJhJT1z



Public key:

045a5f526dfe5d5995bf95f1229e70e21818190883c40ab3590458476ad34aaae5
9bc772b98a587035b452638b59238e2a39e954b43ab7a4f32408664d36ec1575



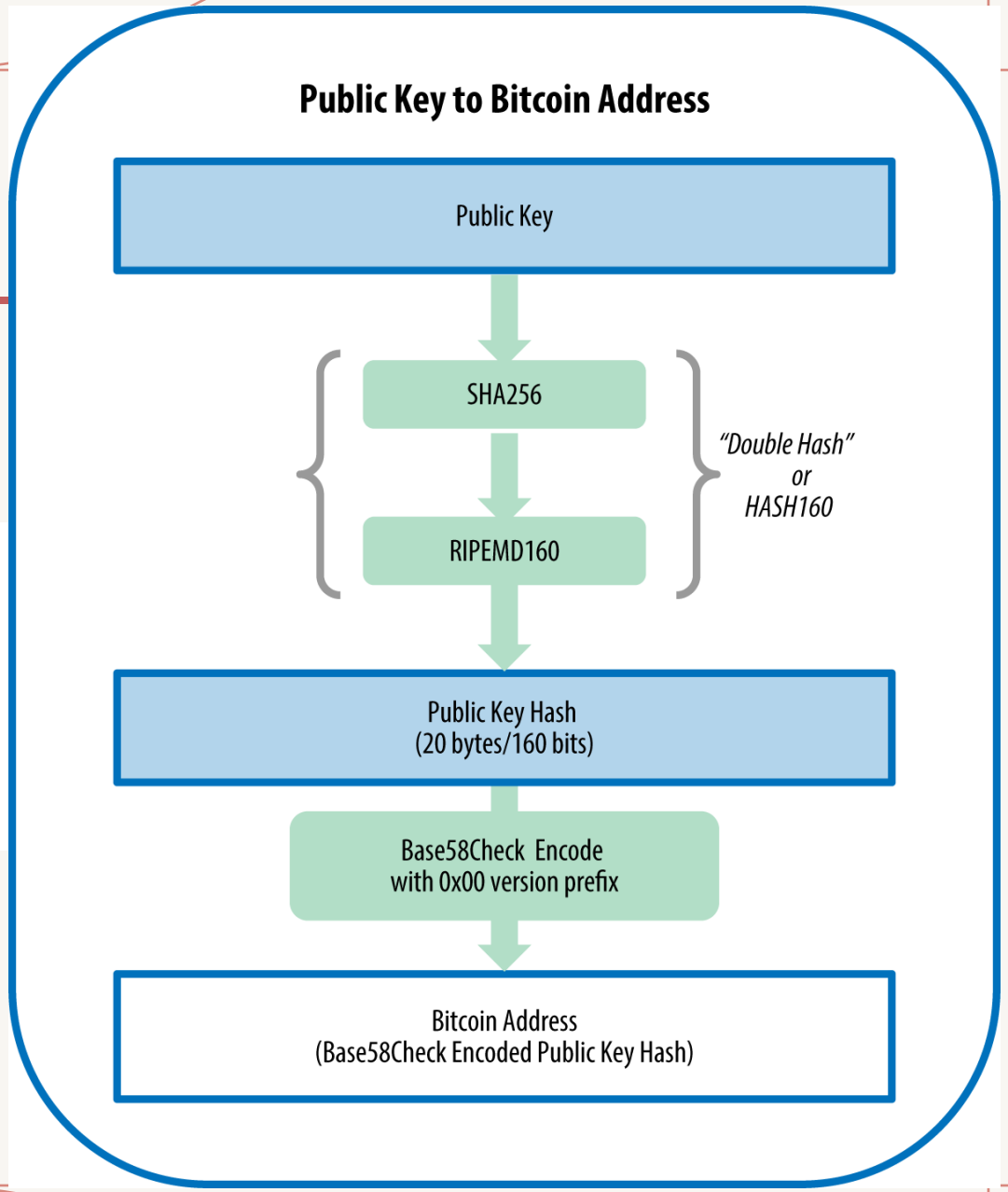
Address: **133GT5661q8RuSKrrv8q2Pb4RwSpUTQU1Z**

Bitcoin address

Public key:

045a5f526dfe5d5995bf95f1229e70e21818190883c40ab3590458476ad34aaae5
9bc772b98a587035b452638b59238e2a39e954b43ab7a4f32408664d36ec1575

Address: **133GT5661q8RuSKrrv8q2Pb4RwSpUTQU1Z**



Base64 Encoding

- A binary-to-text encoding scheme
  - to represent binary data in an ASCII string format by translating it into a radix-64 representation (radix means the number of unique digits)
- Base64 alphabet:
  - English letters 26 lower + 26 upper + 10 numeral + '+' + '/'

Base64 Table

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

source ASCII (if <128)	M								a								n							
source octets	77 (0x4d)								97 (0x61)								110 (0x6e)							
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19								22								5							
Base64-encoded	T								W								F							
encoded octets	84 (0x54)								87 (0x57)								70 (0x46)							

Base58 Encoding

- Base64 alphabets minus six alphabets:
  - 0 (number zero), O (capital o), l (lower L), I (capital i), '+', '/'

Base58 Table

Value	Character	Value	Character	Value	Character	Value	Character
0	1	1	2	2	3	3	4
4	5	5	6	6	7	7	8
8	9	9	A	10	B	11	C
12	D	13	E	14	F	15	G
16	H	17	J	18	K	19	L
20	M	21	N	22	P	23	Q
24	R	25	S	26	T	27	U
28	V	29	W	30	X	31	Y
32	Z	33	a	34	b	35	c
36	d	37	e	38	f	39	g
40	h	41	i	42	j	43	k
44	m	45	n	46	o	47	p
48	q	49	r	50	s	51	t
52	u	53	v	54	w	55	x
56	y	57	z				

```
base10 = 123456789

123456789 % 58 = 19
  2128565 % 58 = 23
    36699 % 58 = 43
      632 % 58 = 52
       10 % 58 = 10

base58 = [10][52][43][23][19]
base58 = BukQL
```

Encoding example

Base58 Encoding

Base58 Table

Value	Character	Value	Character	Value	Character	Value	Character
0	1	1	2	2	3	3	4
4	5	5	6	6	7	7	8
8	9	9	A	10	B	11	C
12	D	13	E	14	F	15	G
16	H	17	J	18	K	19	L
20	M	21	N	22	P	23	Q
24	R	25	S	26	T	27	U
28	V	29	W	30	X	31	Y
32	Z	33	a	34	b	35	c
36	d	37	e	38	f	39	g
40	h	41	i	42	j	43	k
44	m	45	n	46	o	47	p
48	q	49	r	50	s	51	t
52	u	53	v	54	w	55	x
56	y	57	z				

- Base-58 encode the word:

C a t

Character	ASCII dec value				
C	67	$67 * 2^{2*8}$	$67 * 2^{16}$	67 * 65536	**4390912**
a	97	$97 * 2^{1*8}$	$97 * 2^{8}$	97 * 256	**24832**
t	116	$116 * 2^{0*8}$	$116 * 2^{0}$	116 * 1	**116**
					4415860

- The word "Cat" in decimal representation: **4415860**

https://www.youtube.com/watch?v=GedV3S9X89c

Base58 Encoding

Base58 Table

Value	Character	Value	Character	Value	Character	Value	Character
0	1	1	2	2	3	3	4
4	5	5	6	6	7	7	8
8	9	9	A	10	B	11	C
12	D	13	E	14	F	15	G
16	H	17	J	18	K	19	L
20	M	21	N	22	P	23	Q
24	R	25	S	26	T	27	U
28	V	29	W	30	X	31	Y
32	Z	33	a	34	b	35	c
36	d	37	e	38	f	39	g
40	h	41	i	42	j	43	k
44	m	45	n	46	o	47	p
48	q	49	r	50	s	51	t
52	u	53	v	54	w	55	x
56	y	57	z				

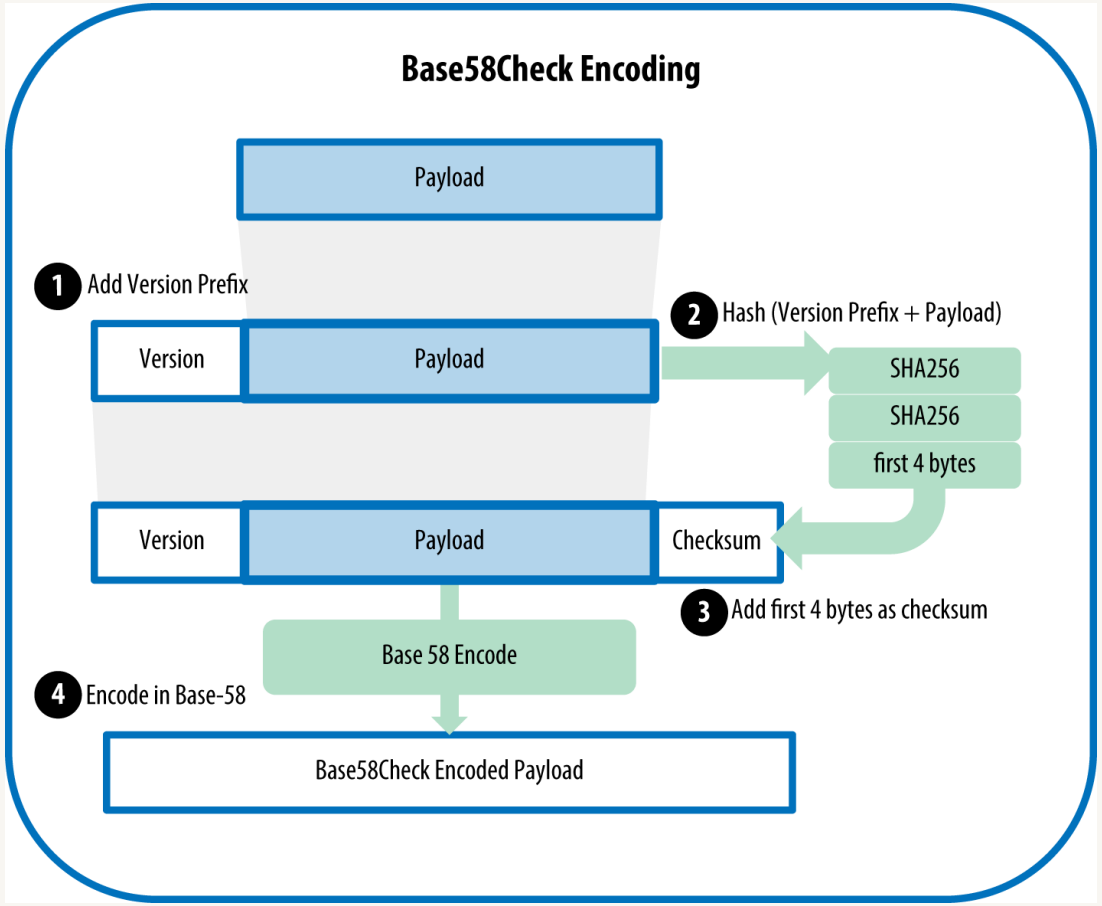
- "Cat" decimal representation: **4415860**

Calculate	Equals	Remainder
4415860 / 58	76135	30
76135 / 58	1312	39
1312 / 58	22	36
22 / 58	0	22

- Remainder values: 22, 36, 39, 30

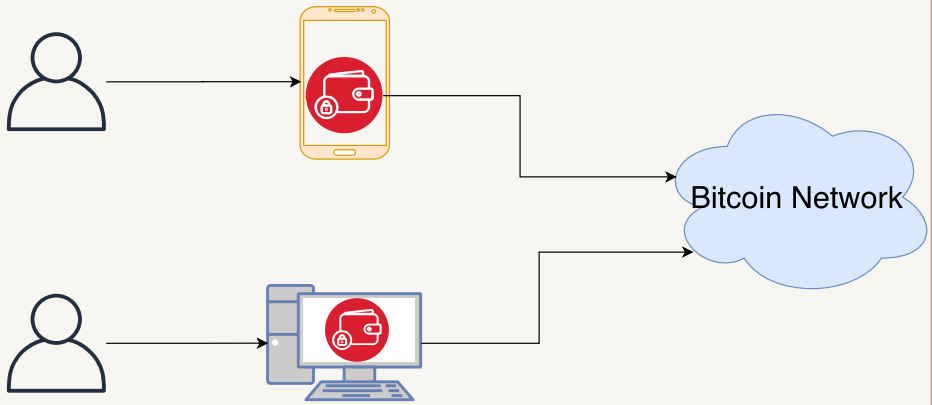
https://www.youtube.com/watch?v=GedV3S9X89c

Bitcoin address



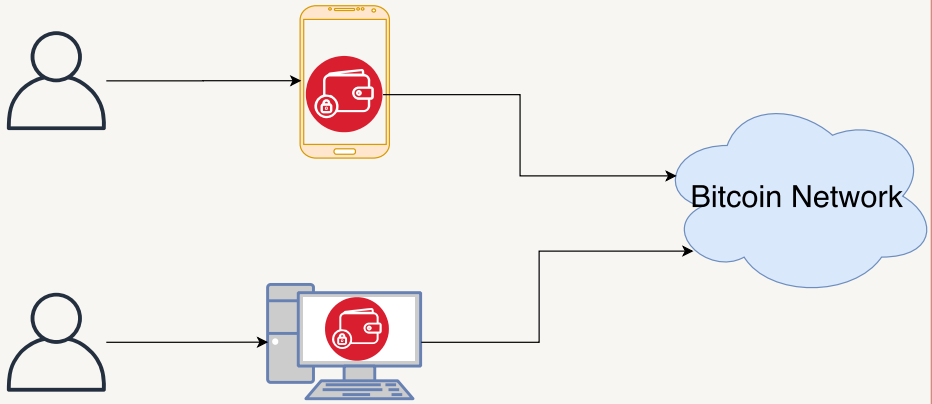
Bitcoin (hot) wallet

- A Bitcoin wallet is a collection of private keys
  - might be used to manage those keys and to make transactions on the Bitcoin network
- It is the entry point for any general users to interact with the bitcoin network
- Can be utilised in a PC, in any smart-device such as a mobile phone or tablet
- Also known as hot wallets as they are always connected to the network
- Examples: Exodus, Electrum, Mycelium



Bitcoin (hot) wallet

- Private keys are kept in encrypted (with a password) formats to ensure their security
- If password is forgotten, there is no way to recover funds attached to that private address
  - unlike other password enabled services, there is no account recovery option
- Strong usability issue
- Advantageous for daily trading or continuous usage
- Less secure (e.g. prone to malware attack)



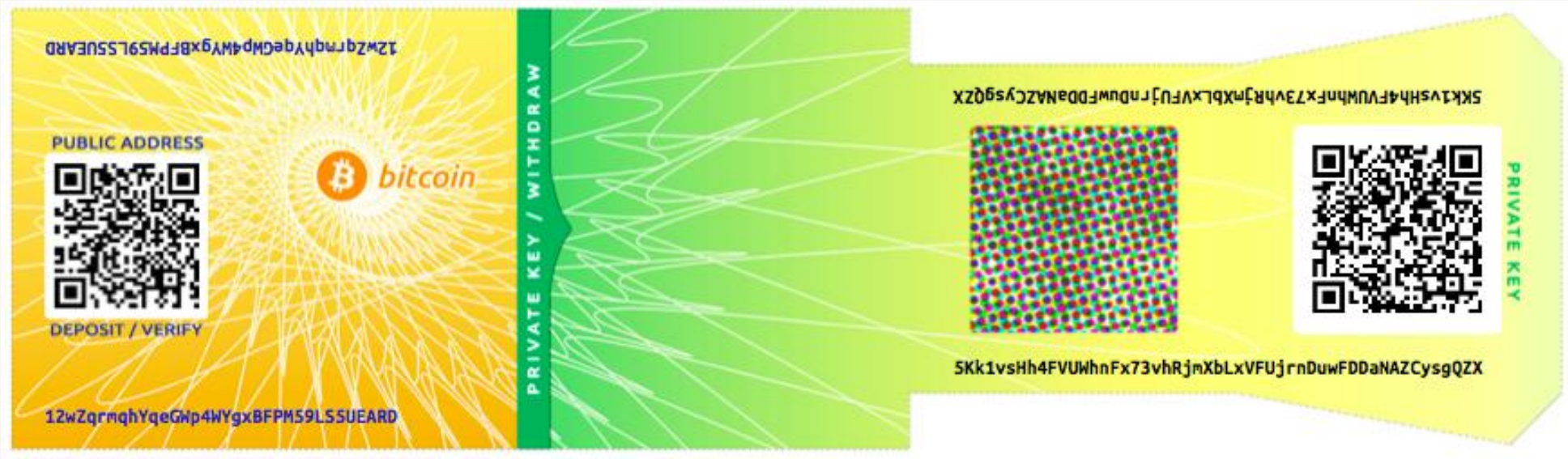
Cold wallet: paper wallet/cold wallet

- Paper wallets are bitcoin private keys printed on paper
  - might include the corresponding bitcoin address for convenience, but this is not necessary because it can be derived from the private key
- They are a very effective way to create backups or offline bitcoin storage, also known as *cold storage/wallet*

Cold wallet: paper wallet/cold wallet

- As a backup mechanism, a paper wallet can provide security
  - against the loss of key due to a computer mishap such as a hard-drive failure, theft, or accidental deletion
  - store it offline in a secret & secure place, even in a bank vault
- As a "cold storage" mechanism, if the paper wallet keys are generated offline
  - never stored on a computer system
- Hence, they are much more secure against hackers, keyloggers, and other online computer threats

Cold wallet: paper wallet/cold wallet



https://raw.githubusercontent.com/bitcoinbook/bitcoinbook/develop/images/mbc2_0410.png

Hardware wallet

- A **hardware wallet** is a special type of bitcoin wallet which stores the user's private keys in a secure hardware device
- They have major advantages over standard software wallets:
  - private keys are often stored in a protected area of a microcontroller, and cannot be transferred out of the device in plaintext
  - immune to computer viruses that steal from software wallets
  - can be used securely and interactively, as opposed to a paper wallet which must be imported to software at some point
  - much of the time, the software is open source, allowing a user to validate the entire operation of the device

https://www.ledgerwallet.com/images/products/lns/ledger-nano-s-fold-medium.png

https://en.bitcoin.it/w/images/en/d/de/Trezor-tx.jpg

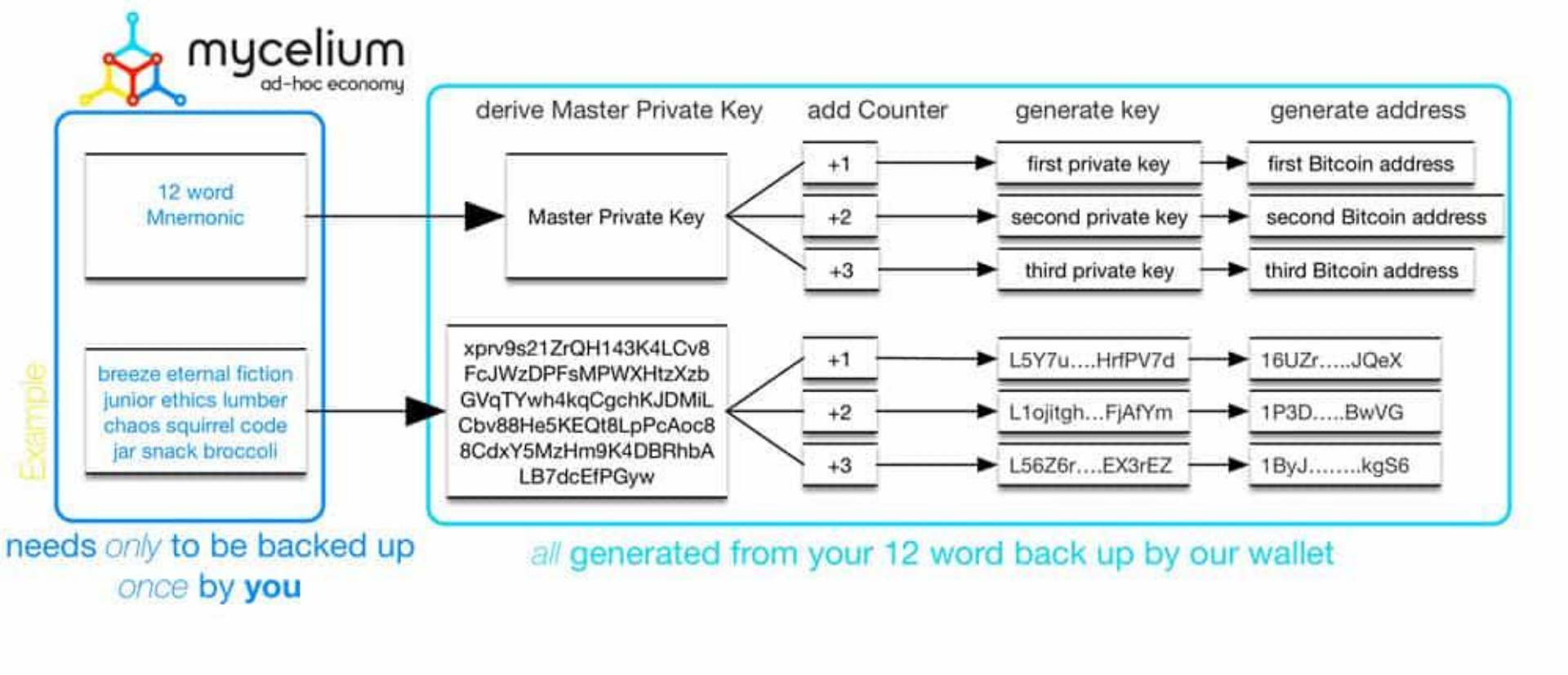
HD wallet

- A Hierarchical Deterministic (HD) is a key creation and transfer protocol which allows creating child keys from a parent key in a hierarchical way
  - Wallets using the HD protocol are called HD wallets
  - The single starting parent key is known as a seed
- The seed allows a user to easily back up and restore a wallet without needing any other information

HD wallet

- Seeds are typically serialised into human-readable words in a **Mnemonic** phrase
- A mnemonic phrase, mnemonic recovery phrase or mnemonic seed is a list of words which store all the information needed to recover a Bitcoin wallet
- Such Mnemonic words must be stored securely and must never be typed on any website

HD wallet



https://coinsutra.com/wp-content/uploads/2017/07/HD_Wallets.jpg

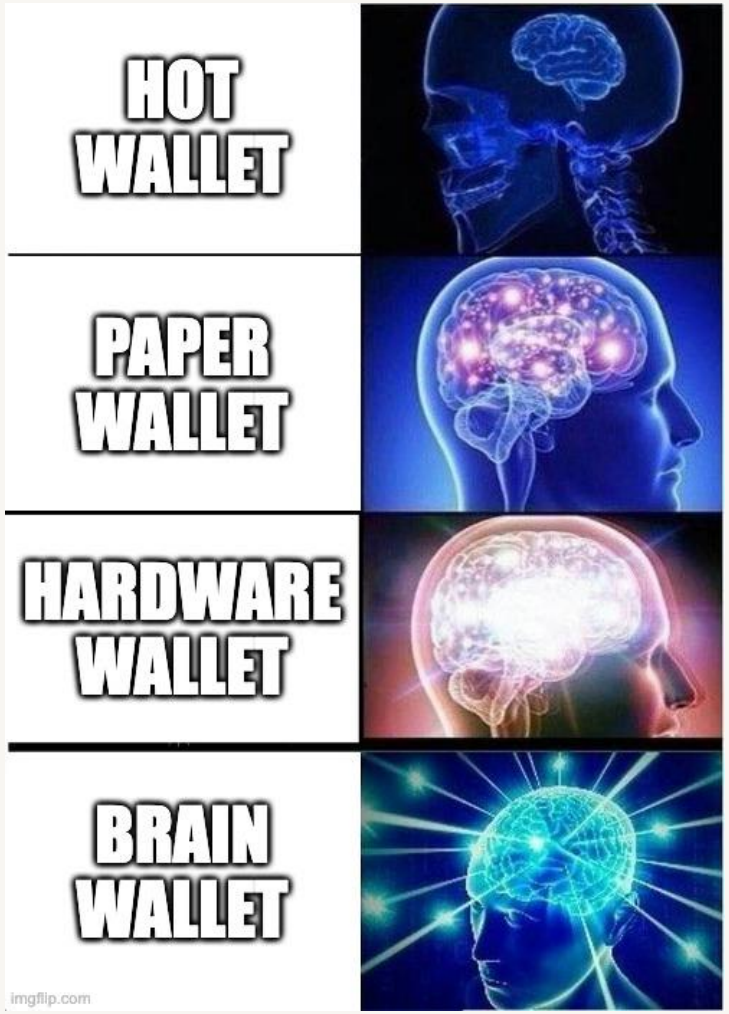
HD wallet

2048 Words, all private keys are generated from these words!!

abandon ability able about above absent absorb abstract absurd abuse access accident account accuse achieve acid acoustic acquire across act action actor actress actual adapt add addict address adjust admit adult advance advice aerobic affair afford afraid again age agent agree ahead aim air airport aisle alarm album alcohol alert alien all alley allow almost alone alpha already also alter always amateur amazing among amount amused analyst anchor ancient anger angle angry animal ankle announce annual another answer antenna antique anxiety any apart apology appear apple approve april arch arctic area arena argue arm armed armor army around arrange arrest arrive arrow art artefact artist artwork ask aspect assault asset assist assume asthma athlete atom attack attend attitude attract auction audit august aunt author auto autumn average avocado avoid awake aware away awesome awful awkward axis baby bachelor bacon badge bag balance balcony ball bamboo banana banner bar barely bargain barrel base basic basket battle beach bean beauty because become beef before begin behave behind believe below belt bench benefit best betray better between beyond bicycle bid bike bind biology bird birth bitter black blade blame blanket blast bleak bless blind blood blossom blouse blue blur blush board boat body boil bomb bone bonus book boost border boring borrow boss bottom bounce box boy bracket brain brand brass brave bread breeze brick bridge brief bright bring brisk broccoli broken bronze broom brother brown brush bubble buddy budget buffalo build bulb bulk bullet bundle bunker burden burger burst bus business busy butter buyer buzz cabbage cabin cable cactus cage cake call calm camera camp can canal cancel candy cannon canoe canvas canyon capable capital captain car carbon card cargo carpet carry cart case cash casino castle casual cat catalog catch category cattle caught cause caution cave ceiling celery cement census century cereal certain chair chalk champion change chaos chapter charge chase chat cheap check cheese chef cherry chest chicken chief child chimney choice choose chronic chuckle chunk churn cigar cinnamon circle citizen city civil claim clap clarify claw clay clean clerk clever click client cliff climb clinic clip clock clog close cloth cloud clown club clump cluster clutch coach coast coconut code coffee coil coin collect color column combine come comfort comic common company concert conduct confirm congress connect consider control convince cook cool copper copy coral core corn correct cost cotton couch country couple course cousin cover coyote crack cradle craft cram crane crash crater crawl crazy cream credit creek crew cricket crime crisp critic crop cross crouch crowd crucial cruel cruise crumble crunch crush cry crystal cube culture cup cupboard curious current curtain curve cushion custom cute cycle dad damage damp dance danger daring dash daughter dawn day deal debate debris decade december decide decline decorate decrease deer defense define defy degree delay deliver demand demise denial dentist deny depart depend deposit depth deputy derive describe desert design desk despair destroy detail detect develop device devote diagram dial diamond diary dice diesel diet differ digital dignity dilemma dinner dinosaur direct dirt disagree discover disease dish dismiss disorder display distance divert divide divorce dizzy doctor document dog doll dolphin domain donate donkey donor door dose double dove draft dragon drama drastic draw dream dress drift drill drink drip drive drop drum dry duck dumb dune during dust dutch duty dwarf dynamic eager eagle early earn earth easily east easy echo ecology economy edge edit educate effort egg eight either elbow elder electric elegant element elephant elevator elite else embark embody embrace emerge emotion employ empower empty enable enact end endless endorse enemy energy enforce engage engine enhance enjoy enlist enough enrich enroll ensure enter entire entry envelope episode equal equip era erase erode erosion error erupt escape essay essence estate eternal ethics evidence evil evoke evolve exact example excess exchange excite exclude excuse execute exercise exhaust exhibit exile exist exit exotic expand expect expire explain expose express extend extra eye eyebrow fabric face faculty fade faint faith fall false fame family famous fan fancy fantasy farm fashion fat fatal father fatigue fault favorite feature february federal fee feed feel female fence festival fetch fever few fiber fiction field figure file film filter final find fine finger finish fire firm first fiscal fish fit fitness fix flag flame flash flat flavor flee flight flip float flock floor flower fluid flush fly foam focus fog foil fold follow food foot force forest forget fork fortune forum forward fossil foster found fox fragile frame frequent fresh friend fringe frog front frost frown frozen fruit fuel fun funny furnace fury future gadget gain galaxy gallery game gap garage garbage garden garlic garment gas gasp gate gather gauge gaze general genius genre gentle genuine gesture ghost giant gift giggle ginger giraffe girl give glad glance glare glass glide glimpse globe gloom glory glove glow glue goat goddess gold good goose gorilla gospel gossip govern gown grab grace grain grant grape grass gravity great green grid grief grit grocery group grow grunt guard guess guide guilt guitar gun gym habit hair half hammer hamster hand happy harbor hard harsh harvest hat have hawk hazard head health heart heavy hedgehog height hello helmet help hen hero hidden high hill hint hip hire history hobby hockey hold hole holiday hollow home honey hood hope horn horror horse hospital host hotel hour hover hub huge human humble humor hundred hungry hunt hurdle hurry hurt husband hybrid ice icon idea identify idle ignore ill illegal illness image imitate immense immune impact impose improve impulse inch include income increase index indicate indoor industry infant inflict inform inhale inherit initial inject injury inmate inner innocent input inquiry insane insect inside inspire install intact interest into invest invite involve iron island isolate issue item ivory jacket jaguar jar jazz jealous jeans jelly jewel job join joke journey joy judge juice jump jungle junior junk just kangaroo keen keep ketchup key kick kid kidney kind kingdom kiss kit kitchen kite kitten kiwi knee knife knock know lab label labor ladder lady lake lamp language laptop large later latin laugh laundry lava law lawn lawsuit layer lazy leader leaf learn leave lecture left leg legal legend leisure lemon lend length lens leopard lesson letter level liar liberty library license life lift light like limb limit link lion liquid list little live lizard load loan lobster local lock logic lonely long loop lottery loud lounge love loyal lucky luggage lumber lunar lunch luxury lyrics machine mad magic magnet maid mail main major make mammal man manage mandate mango mansion manual maple marble march margin marine market marriage mask mass master match material math matrix matter maximum maze meadow mean measure meat mechanic medal media melody melt member memory mention menu mercy merge merit merry mesh message metal method middle midnight milk million mimic mind minimum minor minute miracle mirror misery miss mistake mix mixed mixture mobile model modify mom moment monitor monkey monster month moon moral more morning mosquito mother motion motor mountain mouse move movie much muffin mule multiply muscle museum mushroom music must mutual myself mystery myth naive name napkin narrow nasty nation nature near neck need negative neglect neither nephew nerve nest net network neutral never news next nice night noble noise nominee noodle normal north nose notable note nothing notice novel now nuclear number nurse nut oak obey object oblige obscure observe obtain obvious occur ocean october odor off offer office often oil okay old olive olympic omit once one onion online only open opera opinion oppose option orange orbit orchard order ordinary organ orient original orphan ostrich other outdoor outer output outside oval oven over own owner oxygen oyster ozone pact paddle page pair palace palm panda panel panic panther paper parade parent park parrot party pass patch path patient patrol pattern pause pave payment peace peanut pear peasant pelican pen penalty pencil people pepper perfect permit person pet phone photo phrase physical piano picnic picture piece pig pigeon pill pilot pink pioneer pipe pistol pitch pizza place planet plastic plate play please pledge pluck plug plunge poem poet point polar pole police pond pony pool popular portion position possible post potato pottery poverty powder power practice praise predict prefer prepare present pretty prevent price pride primary print priority prison private prize problem process produce profit program project promote proof property prosper protect proud provide public pudding pull pulp pulse pumpkin punch pupil puppy purchase purity purpose purse push put puzzle pyramid quality quantum quarter question quick quit quiz quote rabbit raccoon race rack radar radio rail rain raise rally ramp ranch random range rapid rare rate rather raven raw razor ready real reason rebel rebuild recall receive recipe record recycle reduce reflect reform refuse region regret regular reject relax release relief rely remain remember remind remove render renew rent reopen repair repeat replace report require rescue resemble resist resource response result retire retreat return reunion reveal review reward rhythm rib ribbon rice rich ride ridge rifle right rigid ring riot ripple risk ritual rival river road roast robot robust rocket romance roof rookie room rose rotate rough round route royal rubber rude rug rule run runway rural sad saddle sadness safe sail salad salmon salon salt salute same sample sand satisfy satoshi sauce sausage save say scale scan scare scatter scene scheme school science scissors scorpion scout scrap screen script scrub sea search season seat second secret section security seed seek segment select sell seminar senior sense sentence series service session settle setup seven shadow shaft shallow share shed shell sheriff shield shift shine ship shiver shock shoe shoot shop short shoulder shove shrimp shrug shuffle shy sibling sick side siege sight sign silent silk silly silver similar simple since sing siren sister situate six size skate sketch ski skill skin skirt skull slab slam sleep slender slice slide slight slim slogan slot slow slush small smart smile smoke smooth snack snake snap sniff snow soap soccer social sock soda soft solar soldier solid solution solve someone song soon sorry sort soul sound soup source south space spare spatial spawn speak special speed spell spend sphere spice spider spike spin spirit split spoil sponsor spoon sport spot spray spread spring spy square squeeze squirrel stable stadium staff stage stairs stamp stand start state stay steak steel stem step stereo stick still sting stock stomach stone stool story stove strategy street strike strong struggle student stuff stumble style subject submit subway success such sudden suffer sugar suggest suit summer sun sunny sunset super supply supreme sure surface surge surprise surround survey suspect sustain swallow swamp swap swarm swear sweet swift swim swing switch sword symbol symptom syrup system table tackle tag tail talent talk tank tape target task taste tattoo taxi teach team tell ten tenant tennis tent term test text thank that theme then theory there they thing this thought three thrive throw thumb thunder ticket tide tiger tilt timber time tiny tip tired tissue title toast tobacco today toddler toe together toilet token tomato tomorrow tone tongue tonight tool tooth top topic topple torch tornado tortoise toss total tourist toward tower town toy track trade traffic tragic train transfer trap trash travel tray treat tree trend trial tribe trick trigger trim trip trophy trouble truck true truly trumpet trust truth try tube tuition tumble tuna tunnel turkey turn turtle twelve twenty twice twin twist two type typical ugly umbrella unable unaware uncle uncover under undo unfair unfold unhappy uniform unique unit universe unknown unlock until unusual unveil update upgrade uphold upon upper upset urban urge usage use used useful useless usual utility vacant vacuum vague valid valley valve van vanish vapor various vast vault vehicle velvet vendor venture venue verb verify version very vessel veteran viable vibrant vicious victory video view village vintage violin virtual virus visa visit visual vital vivid vocal voice void volcano volume vote voyage wage wagon wait walk wall walnut want warfare warm warrior wash wasp waste water wave way wealth weapon wear weasel weather web wedding weekend weird welcome west wet whale what wheat wheel when where whip whisper wide width wife wild will win window wine wing wink winner winter wire wisdom wise wish witness wolf woman wonder wood wool word work world worry worth wrap wreck wrestle wrist write wrong yard year yellow you young youth zebra zero zone zoo

Brain wallet

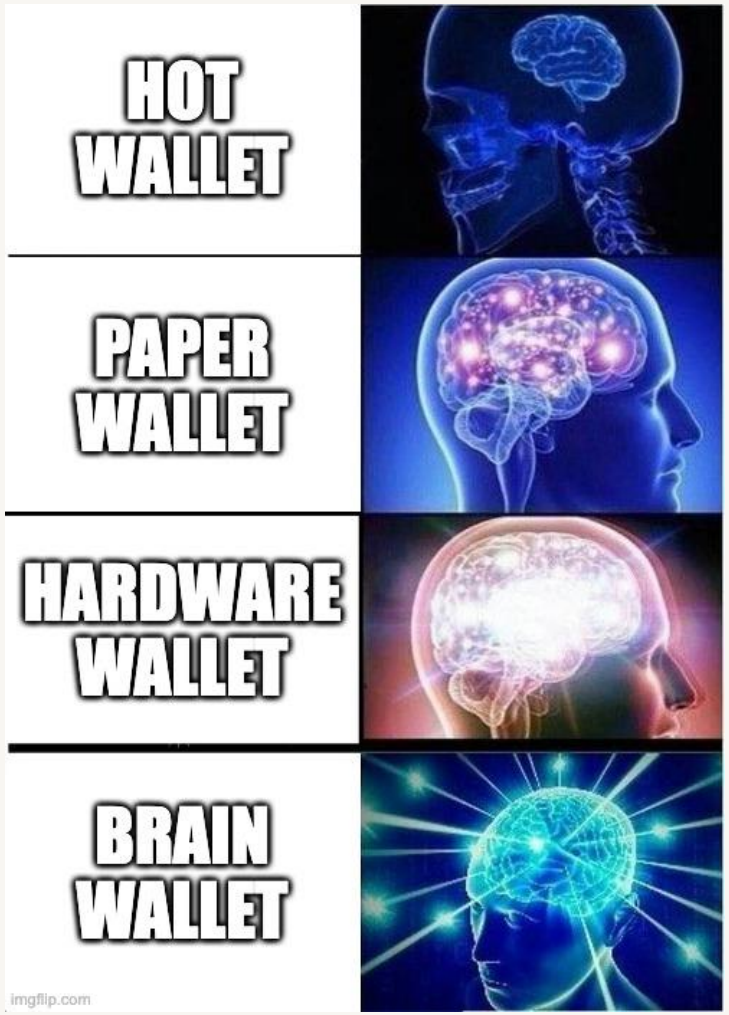
- A brain wallet refers to the concept of storing Bitcoin’s private key in one's own mind by memorising a seed phrase
- If the private key is not recorded anywhere, the Bitcoins can be thought of as being held only in the mind of the owner
- Using memory techniques allow them to be memorised and recalled easily
- If a brain wallet is forgotten or the person dies or is permanently incapacitated, the Bitcoins are lost forever



https://i.imgflip.com/6x41nq.jpg

Brain wallet

- Private keys will be generated from a seed (mnemonic words/passphrase)
  - E.g. hashing the passphrase
- Then generate the public key from the private key using a standard algorithm
- The passphrase needs to be securely created, otherwise an adversary could easily guess
- If the passphrase is long, it will be difficult to memorise

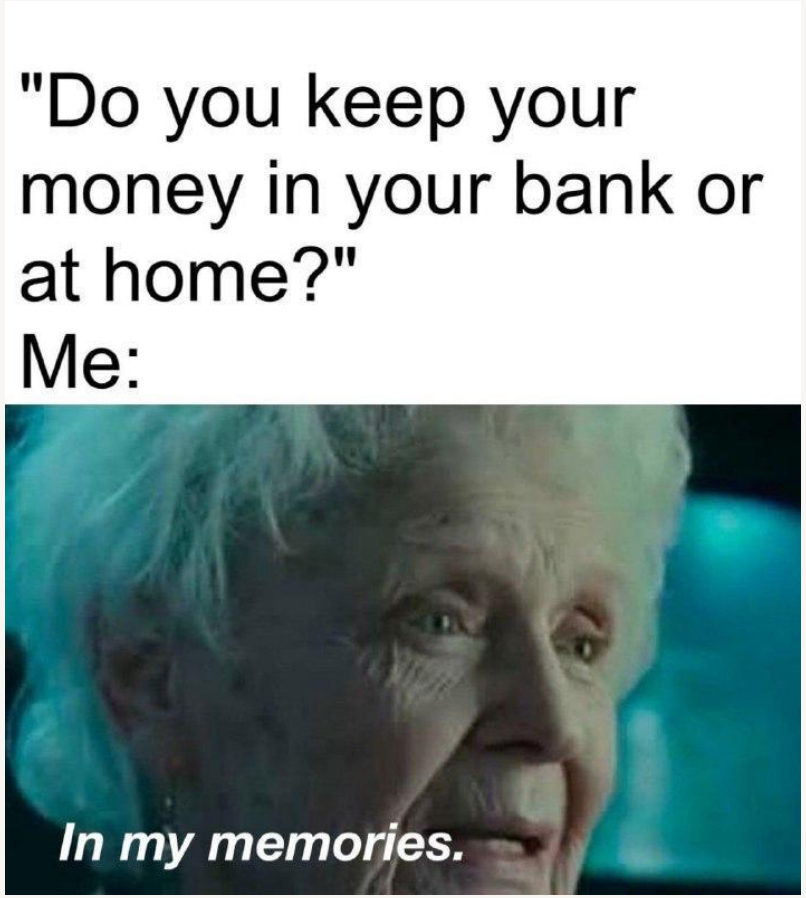


https://i.imgflip.com/6x41nq.jpg

Brain wallet

- To memorise a seed with this method you must invent a story which hits the words as "keynotes”
- Let the key phrases are the following
  - witch collapse practice feed shame open despair creek road again ice least
- “Imagine going through a room and seeing your sister dressed as a **witch**, playing the jenga boardgame until the tower **collapses** and so on”

Brain wallet



Custodial wallet

- Let other people / companies store your bitcoins / cryptocurrencies for you
- No access to the private key, coins can only be used through a certain interface / website
- Very common within most exchanges
  - The money is sent to the exchange, the account on the platform has now a new balance which can be traded or paid out
- However: Very dangerous!
- Many exchanges got hacked, users lost their funds. Be careful!

Bitcoin Node & Network

- All nodes are connected to a common p2p network
- Every node runs a bitcoin implementation (bitcoind, bcoin, etc.)
  - implementations are open source
- Anyone can freely join the network
- Nodes do not have to trust the network!
- Everybody assumes that neighbours may lie (byzantine behaviour)
- Every node receives messages, acts on them and passes these messages to its known neighbours according to protocols
  - malicious nodes can suppress messages and behave beyond protocols rules

Bitcoin Node & Network

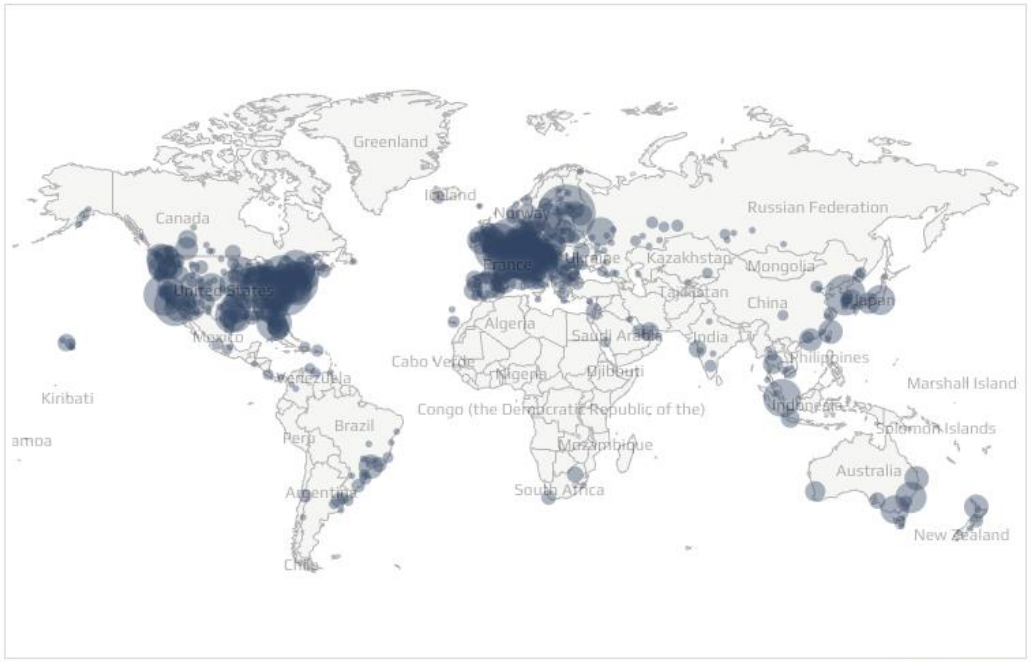
REACHABLE BITCOIN NODES
Updated: Tue Nov 4 16:16:56 2025 +06

23106 NODES CHARTS

IPv4: +4.0% / IPv6: +7.7% / .onion: -4.6%

Top 10 countries with their respective number of reachable nodes are as follows.

RANK	COUNTRY	NODES
1	n/a	14599 (63.18%)
2	United States	2461 (10.65%)
3	Germany	1274 (5.51%)
4	France	726 (3.14%)
5	Canada	416 (1.80%)
6	Finland	380 (1.64%)
7	Netherlands	352 (1.52%)
8	United Kingdom	302 (1.31%)
9	Switzerland	248 (1.07%)
10	Russian Federation	193 (0.84%)



Map shows concentration of reachable Bitcoin nodes found in countries around the world. LIVE MAP

https://bitnodes.io/

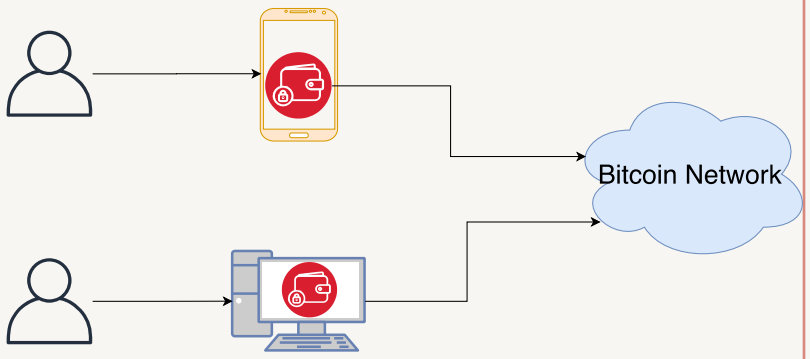
Live map available: https://bitnodes.io/nodes/live-map/

Bitcoin Node

- Bitcoin has four types of nodes:
  - Wallet node
  - Light node
  - Full node
  - Miner node

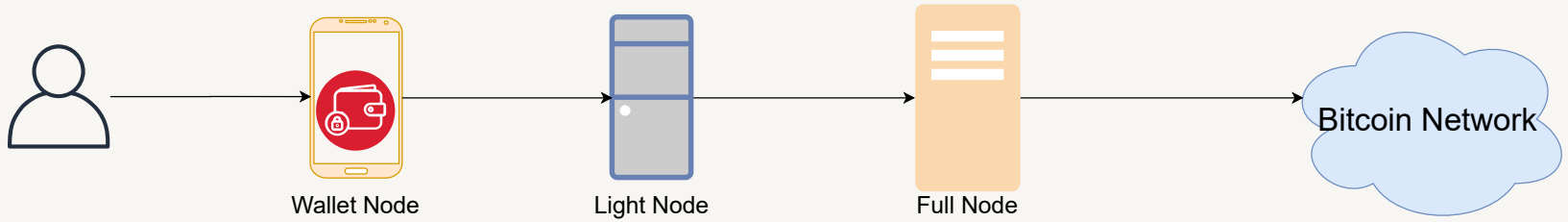
Bitcoin Node types: wallet node (user)

- The wallet owner owns different private keys
- He is the owner of all stored currencies on these addresses
- He sends money by signing and publishing new transactions to a connected light node, full node or miner node



Bitcoin Node types: light node (software)

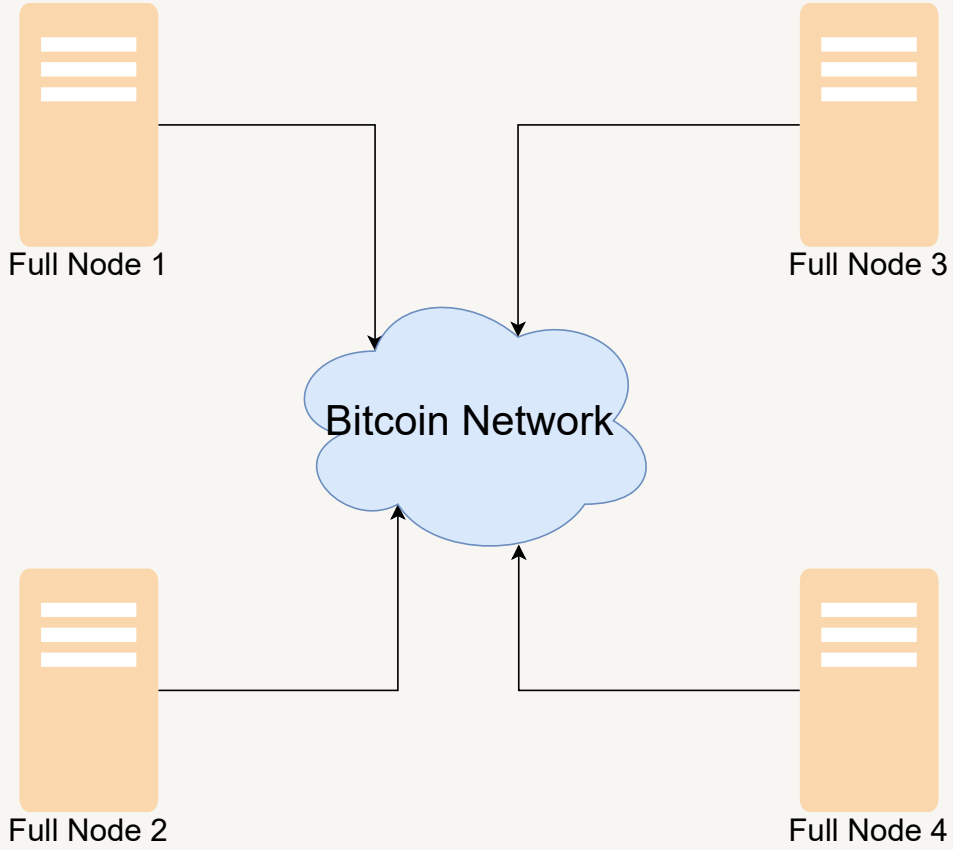
- The light node can act as a relay for transactions of one wallet owner
- It validates whether a single transaction of the wallet owner was executed correctly
- The light node also requires a full node to connect to the network
- Almost no relevance in practice today
- Today, centralised services are used to create transactions



Bitcoin Basics- Gallersdörfer, U., Holl, P., & Matthes, F. (2020). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Bitcoin Node types: full node (software)

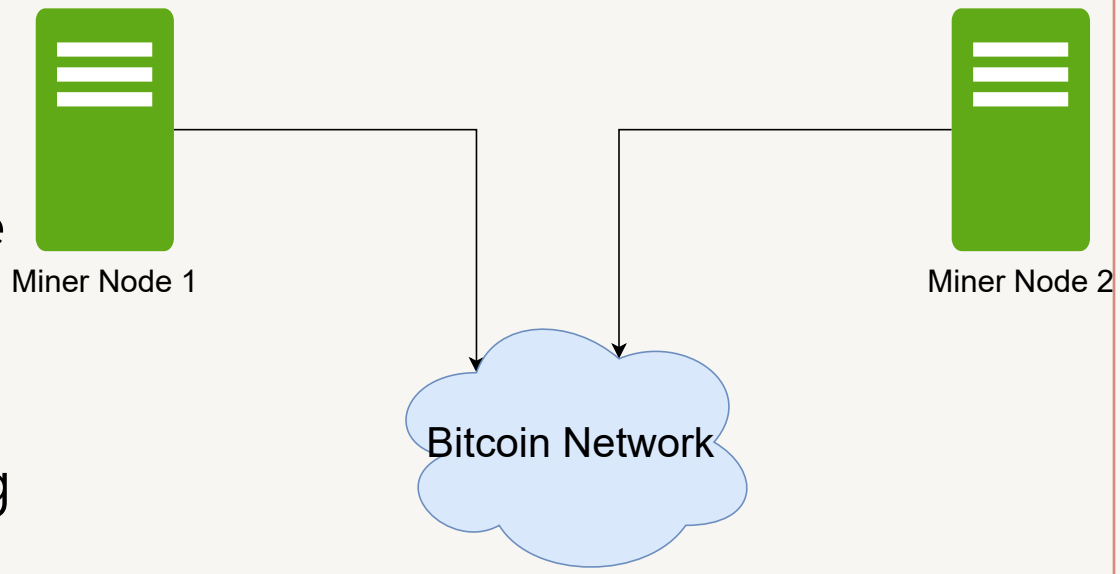
- The full node maintains the complete blockchain
- Its record of the chain is complete
  - it contains every single transaction and block until the genesis (first) block
- Is connected to other full nodes and exchanges information
- Namely:
  - Validates every transaction and block it receives
  - Relays all new transactions and blocks



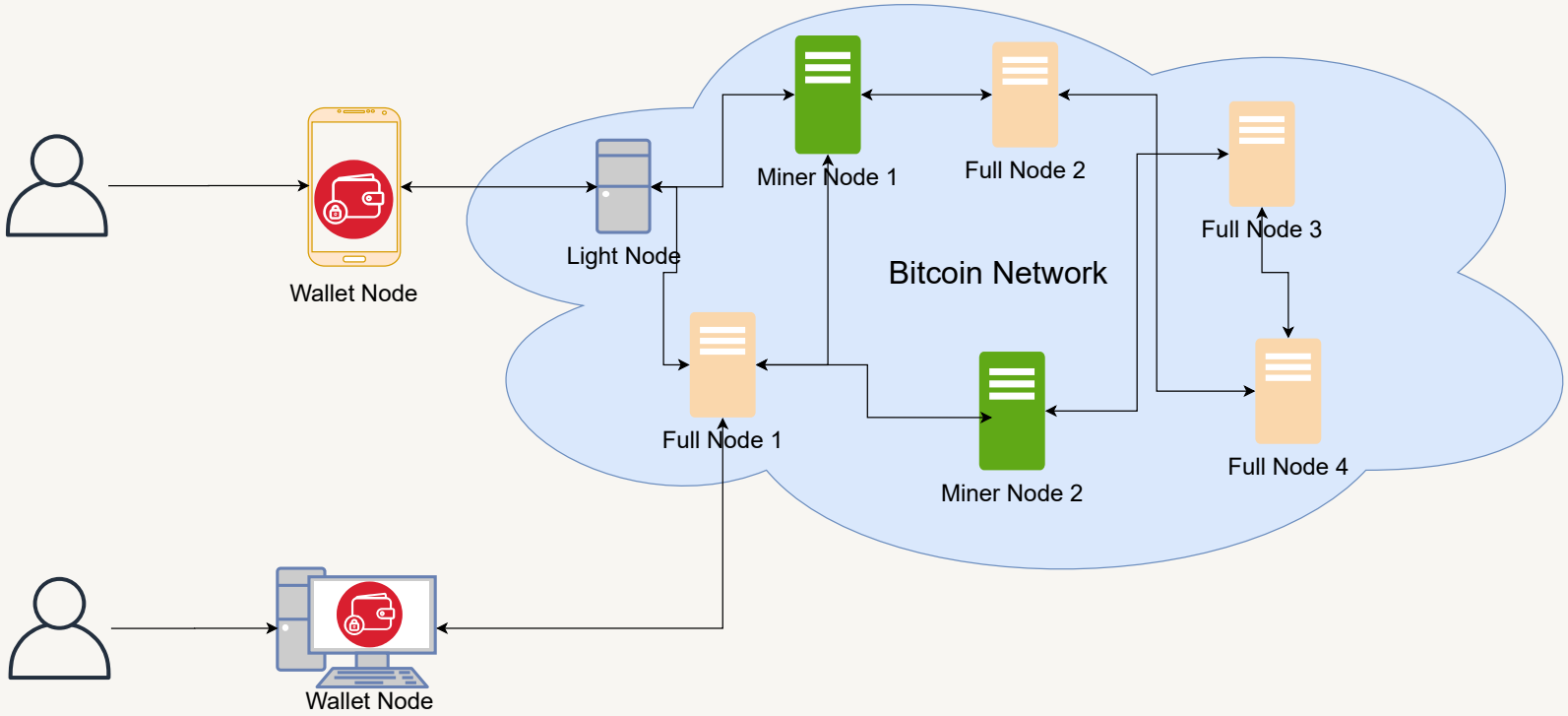
Bitcoin Basics- Gallersdörfer, U., Holl, P., & Matthes, F. (2020). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Bitcoin Node types: miner node (software)

- The miner needs the same record as a full node to work properly
- It also is connected with other nodes and maintains the network
- Additionally, the miner is responsible for creating new blocks by trying to solve the mining puzzle
- The miner gets rewarded for creating new blocks



Bitcoin network




THANK YOU
QUESTIONS?