CSE446: Blockchain & Cryptocurrencies

Lecture – 7: Bitcoin-1

Inspiring Excellence

Agenda

- Distributed Ledger/Blockchain concept
- Bitcoin
- Bitcoin components
    - Users

Fiat money vs Crypto-currency

- Holder has ownership
  - Like any Fiat money, a crypto-currency is a bearer instrument
  - But provides better security as it is important to prove ownership
- No other records kept as to identify an owner
- Easy to keep anonymous
- Hard or impossible to replace if lost or stolen

https://upload.wikimedia.org/wikipedia/en/9/94/1000_Bangladeshi_taka_Obs_2011.jpg

Bitcoin

- Decentralised, Distributed, Voluntary
- No central issuing or verification authority, no “Bitcoin Corp”
  - Bitcoin Foundation (bitcoinfoundation.org)
  - Growing numbers of of entrepreneurs accepting or basing new business concepts on Bitcoin
- Relative to other bearer instruments (currency or fiat currency)
  - Easier to transport anywhere in the world
  - Easier to secure, even provides better security
- Relative to other electronic currencies
  - Immune to sovereign censorship, shutdown, or confiscation
  - Immune to inflation and bank defaults

Bitcoin challenges

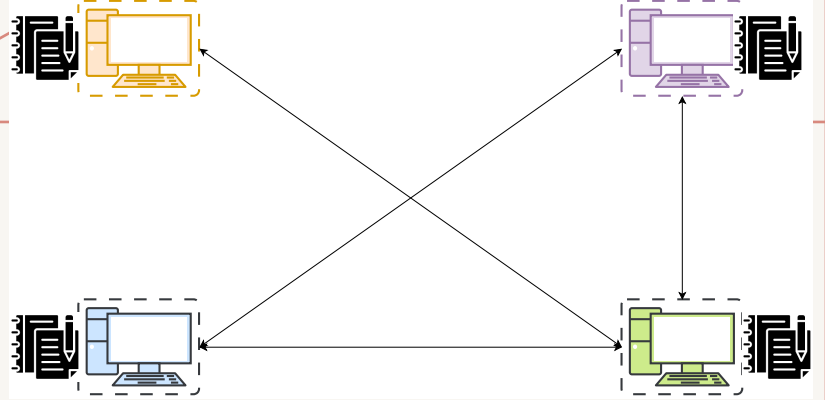
- Creation of a virtual coin/note
  - How is it created in the first place?
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?)
- Validation
  - Is the coin legit?
  - How do you prevent a coin from double-spending?
- Trust on third-parties
  - Rely on proof instead of trust
  - Verifiable by everyone
  - No central bank or clearing house

Bitcoin challenges

- Creation of a virtual coin/note
  - How is it created in the first place?
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?)
  - Is the coin legit?
  - How do you prevent a coin from double-spending?
- Trust on third-parties
  - Rely on proof instead of trust
  - Verifiable by everyone
  - No central bank or clearing house

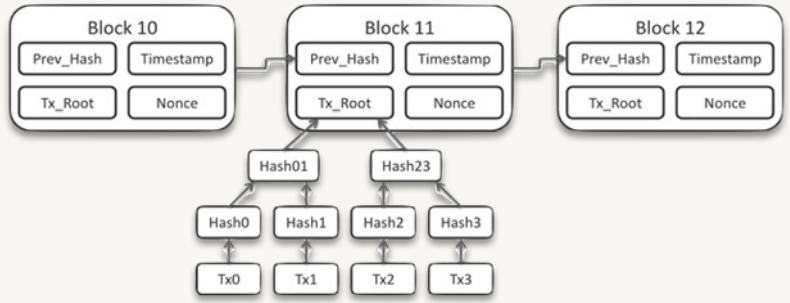
Blockchain/Distributed Ledger is the solution

Distributed Ledger



- A general ledger is the heart of any banking and financial institutions
- To tackle the centralised trust issues
  - dissolve the centralised trust, replace it with a decentralised trust
- One way: distribute the ledger over as many entities as possible
  - Hence the notion of distributed ledger
- Slight difference in meanings between blockchain and distributed ledger
  - A blockchain is just an example of a distributed ledger

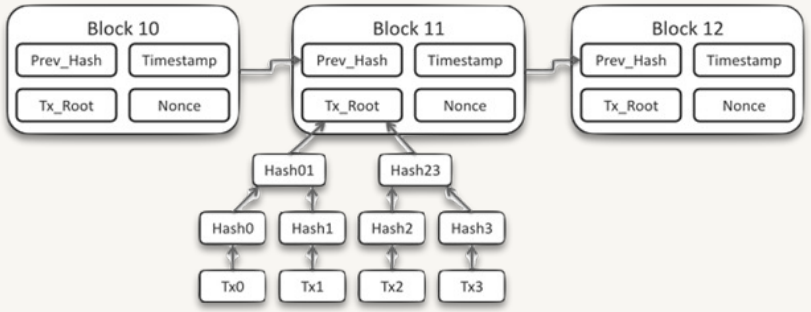
Blockchain

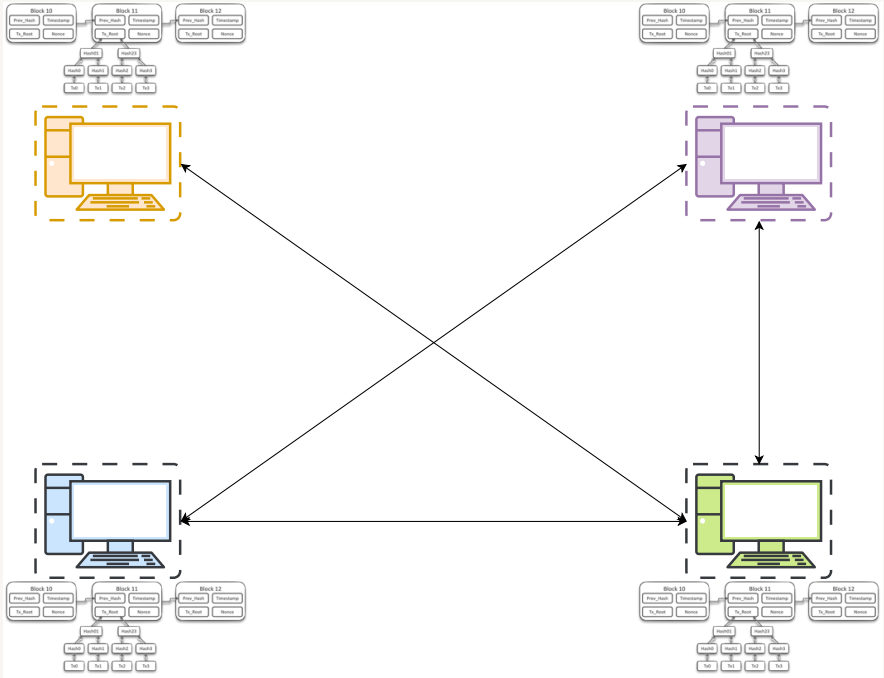


- The blockchain is a distributed record of transactions structured in a specific way
- These transactions are grouped together following specific sets of rules
  - These groups are known as Blocks
- Blocks are the linked together with specific rules, thus forming the chain
- Blockchain is a chain of blocks, where each block maintains a specific data structure

Blockchain

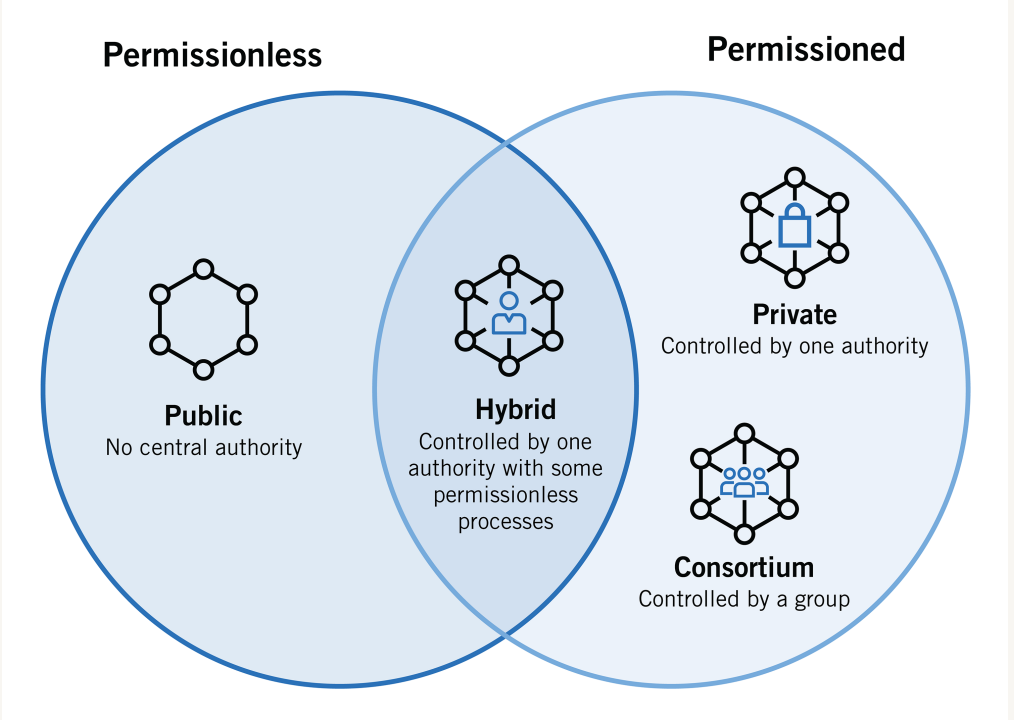
Even though a blockchain is a just a data structure, however, it implies a distributed data structure





Blockchain types

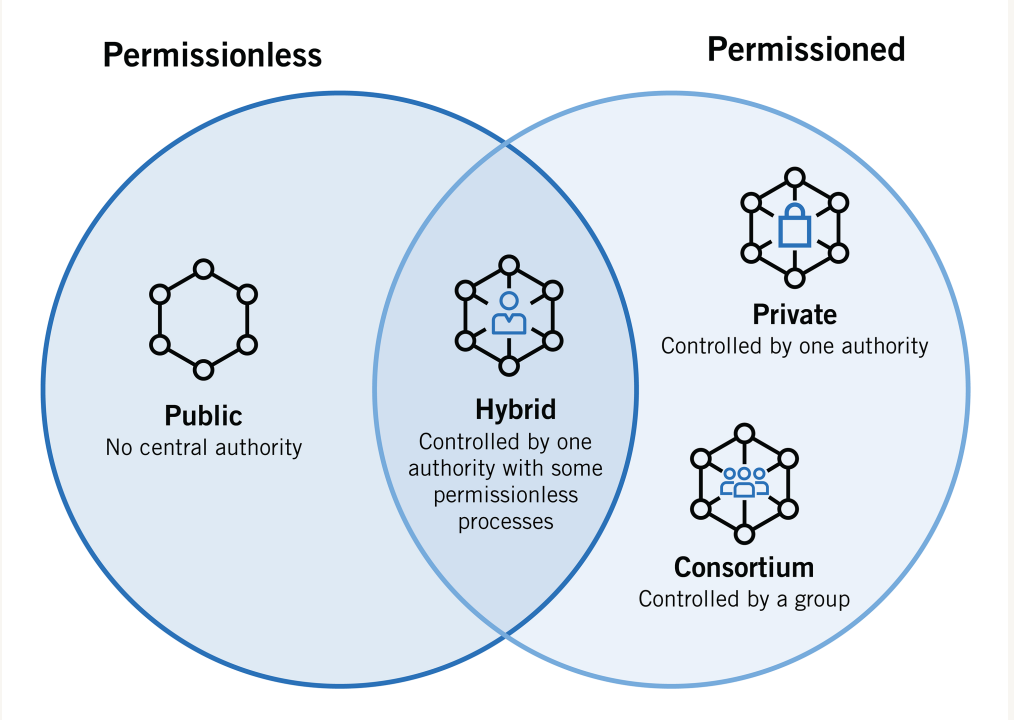
- Depending who can access (read) or write data from/to a blockchain, there could be four types of blockchain
  - Public (permissionless) blockchain
  - Private (permissioned) blockchain
  - Hybrid blockchain
  - Consortium blockchain



https://www.foley.com/en/insights/publications/2021/08/-/media/images/insights/publications/2021/08/22mc35029-blockchain-graphic--permissions06.png

Public blockchain

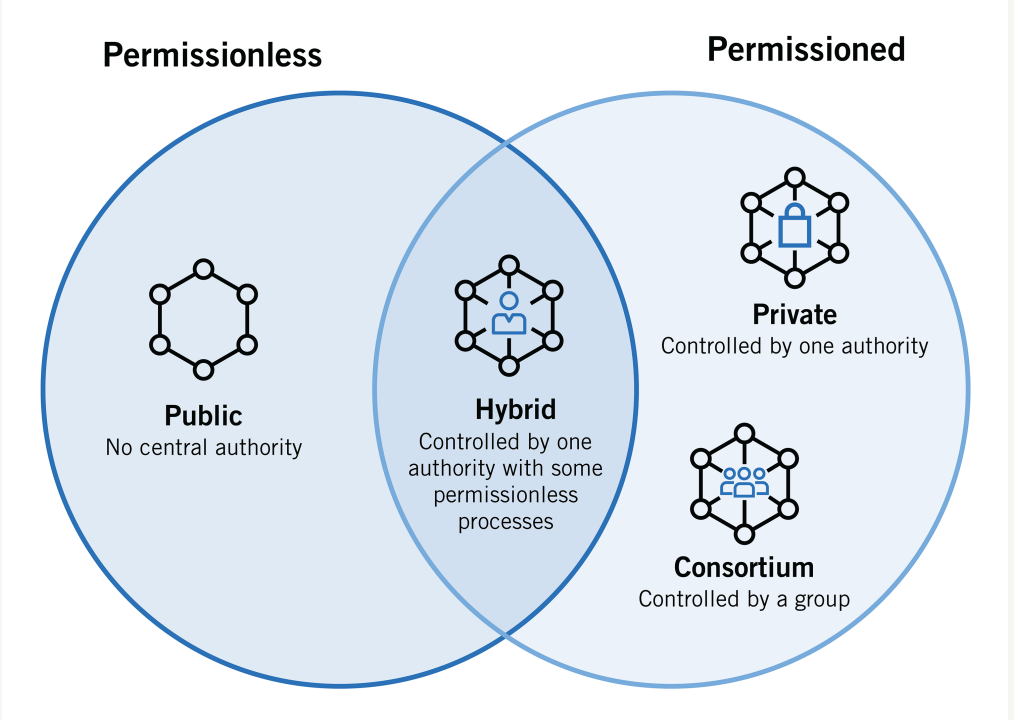
- A public blockchain is an open blockchain which allows everyone to join in the network
- Everyone can write into the blockchain following specific rules
- All data can be read by all
- Everyone can verify all data in the blockchain
- No one is trusted & there is no central authority
- Almost all crypto-currency blockchains are public, e.g. Bitcoin, Ethereum, Solana, Cardano



https://www.foley.com/en/insights/publications/2021/08/-/media/images/insights/publications/2021/08/22mc35029-blockchain-graphic--permissions06.png

Private blockchain

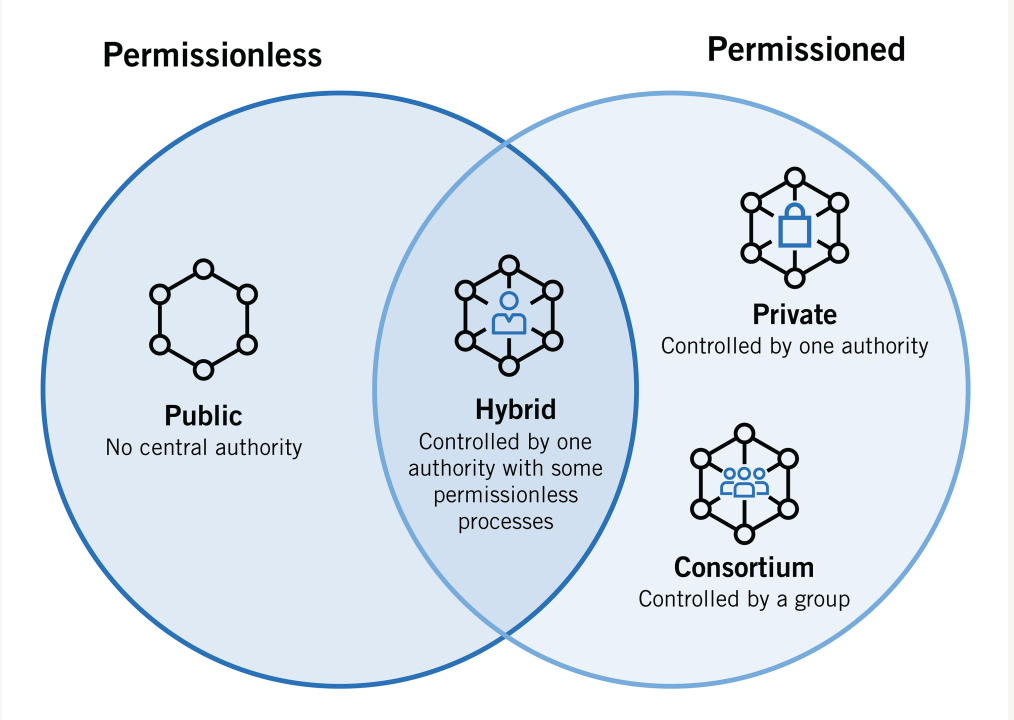
- A private blockchain is controlled by a single authority (e.g. a bank or an org)
- The network is private and set up between trusted partners (e.g. different bank branches)
- Sets own rules and regulations
- Restricted read/write access so that only authorised parties can participate
- Examples: Hyperledger Fabric, Hyperledger Sawtooth, Corda, etc.



https://www.foley.com/en/insights/publications/2021/08/-/media/images/insights/publications/2021/08/22mc35029-blockchain-graphic--permissions06.png

Hybrid blockchain

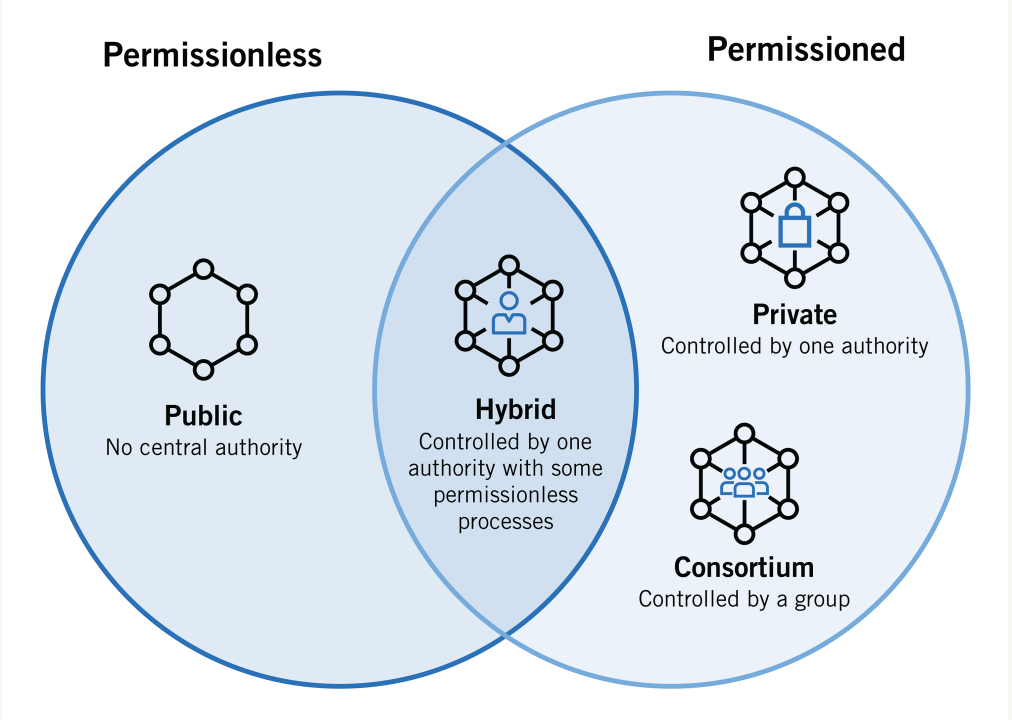
- A hybrid is a combination of public and private blockchain
- It is usually controlled by a central authority
- The authority sets up the rules
- Everyone can read data from the blockchain
- Write access is restricted
- Examples: LTO Network, Sovrin



https://www.foley.com/en/insights/publications/2021/08/-/media/images/insights/publications/2021/08/22mc35029-blockchain-graphic--permissions06.png

Consortium blockchain

- It is a private blockchain controlled by a set of private entities (e.g. a consortium of banks in Bangladesh)
- They set up their own rules and regulations
- Read and write access are controlled and are only allowed to authorised entities
- Can be set up with private blockchains

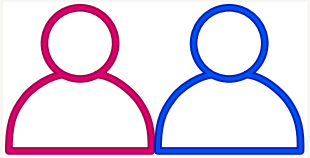


https://www.foley.com/en/insights/publications/2021/08/-/media/images/insights/publications/2021/08/22mc35029-blockchain-graphic--permissions06.png

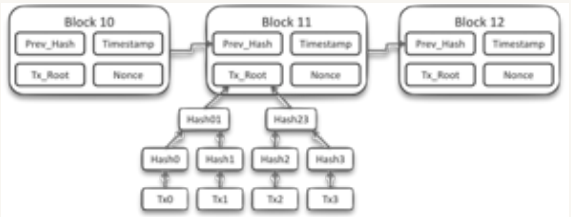
Summary

Types	Read	Write
Public	All	All
Private	Restricted	Restricted
Hybrid	All	Restricted
Consortium	Restricted	Restricted

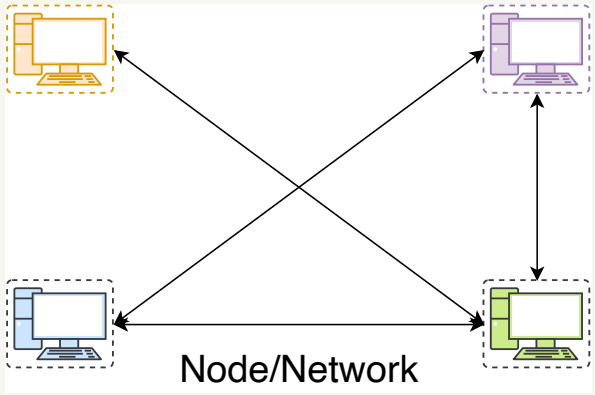
Blockchain components



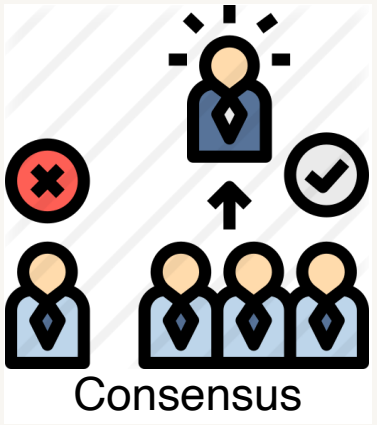
Users



Blockchain



Node/Network



Consensus

Decentralised Identity

- Identity 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
- 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

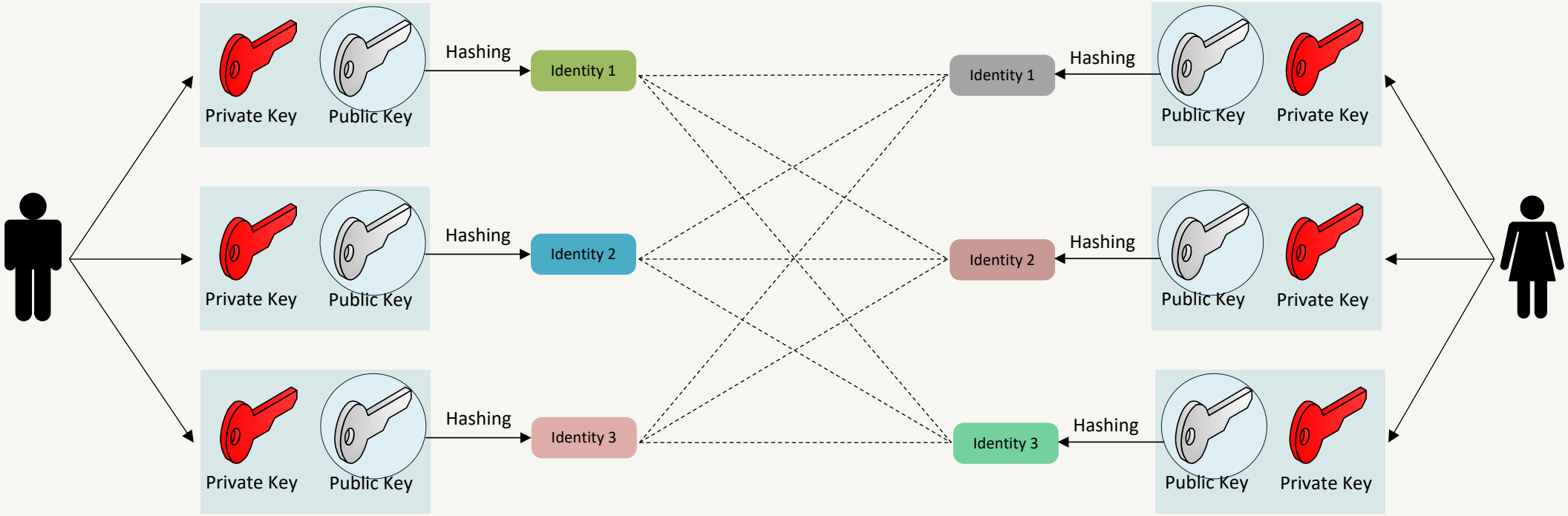
Decentralised Identity

- Decentralised identity is the solution using digital signature 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

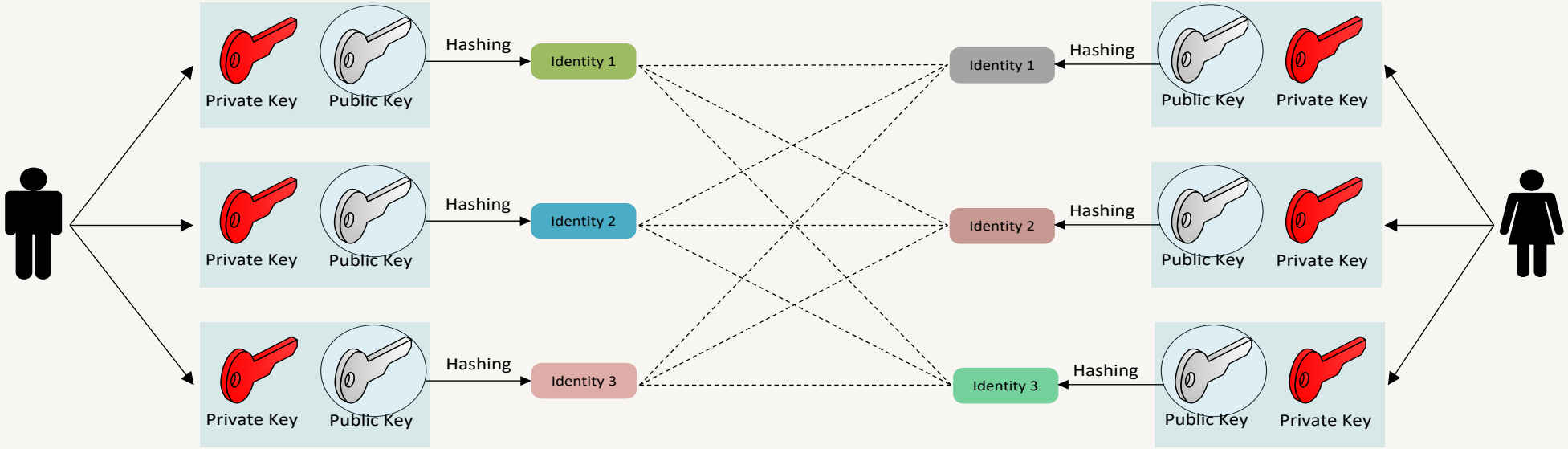
- Public keys are very large
  - You want to hash your public key pk in order to receive an “identity”
- To validate a statement, one has to check
  1. if the pk hashes to the identity and
  2. if the message verifies under the public key pk

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

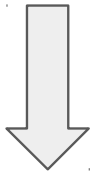
Users

- 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

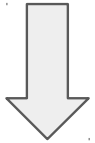
Private key:

5JXesisRRU2Z7HMmwMpNtoiYk1QDMVjV3HLoYMd1PTKEkJhJT1z



Public key:

045a5f526dfe5d5995bf95f1229e70e21818190883c40ab3590458476ad34aaae5
9bc772b98a587035b452638b59238e2a39e954b43ab7a4f32408664d36ec1575



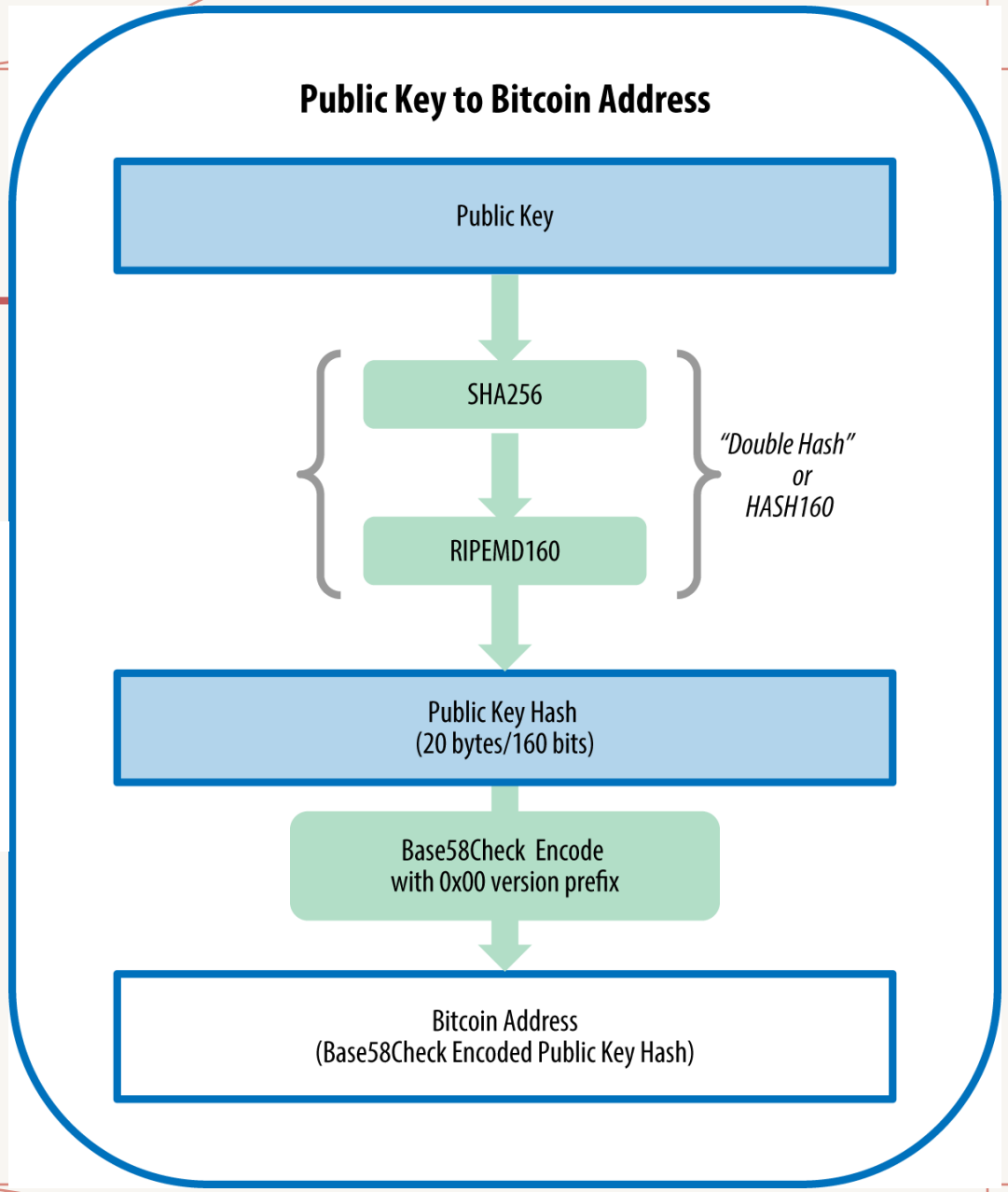
Address: **133GT5661q8RuSKrrv8q2Pb4RwSpUTQU1Z**

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				46			
Base64-encoded	T				W				F				u			
encoded octets	84 (0x54)				87 (0x57)				70 (0x46)				117 (0x75)			

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				

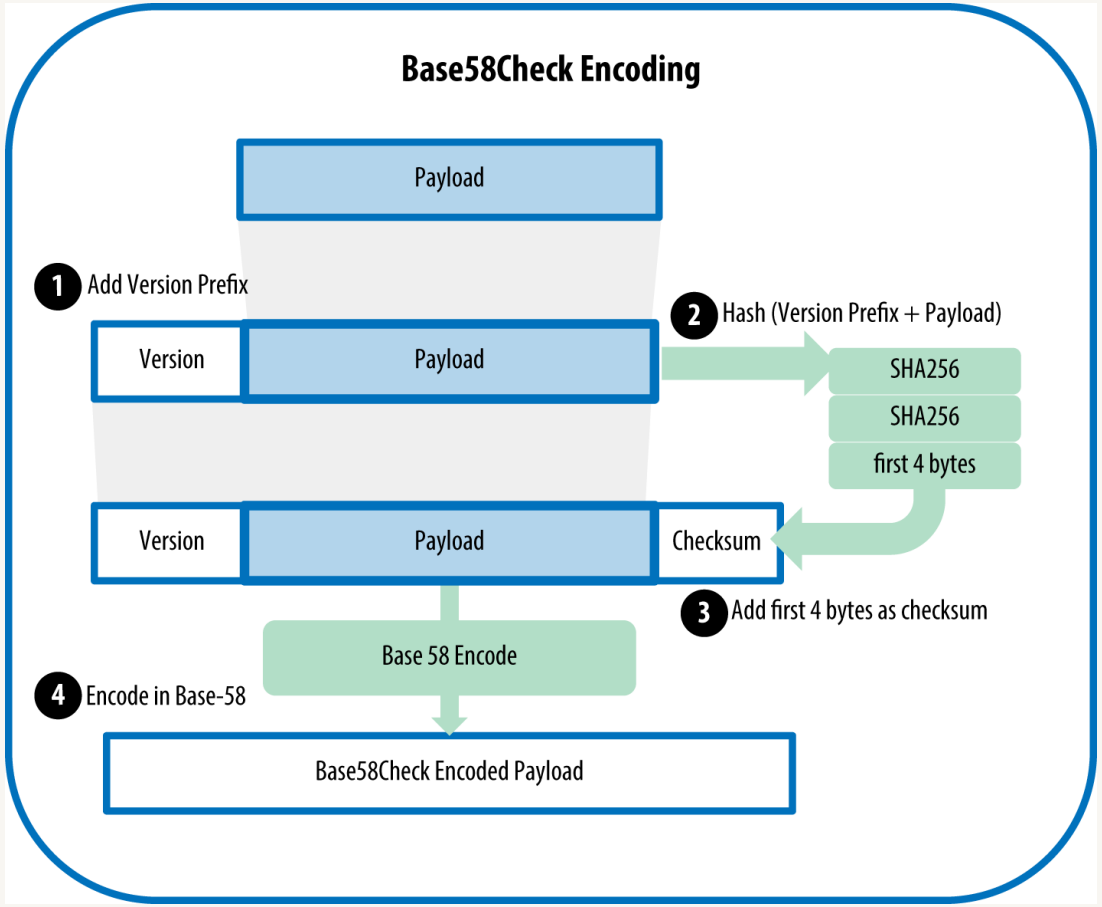
- "Cat" decimal representation: **4415860**

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

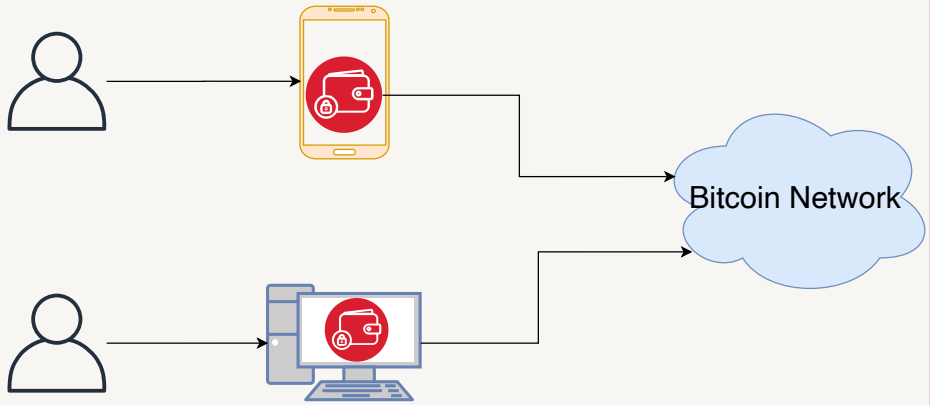
https://www.youtube.com/watch?v=GedV3S9X89c

Bitcoin address



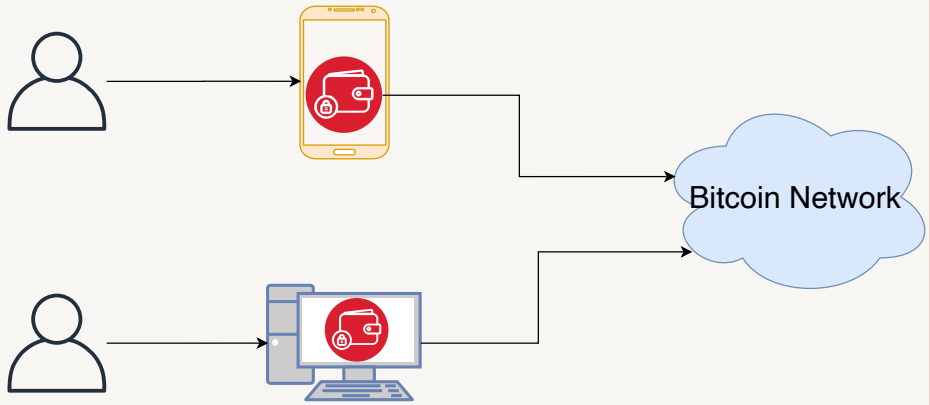
Bitcoin (hot) wallet

- 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)




THANK YOU
QUESTIONS?