

Bitcoin



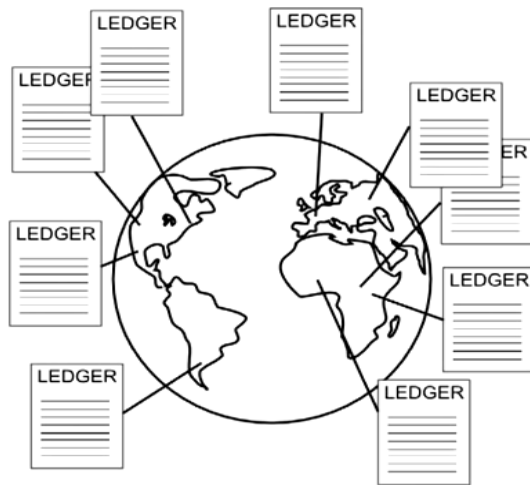
Mikal Vike Villa

High level brief

~~TRUST~~

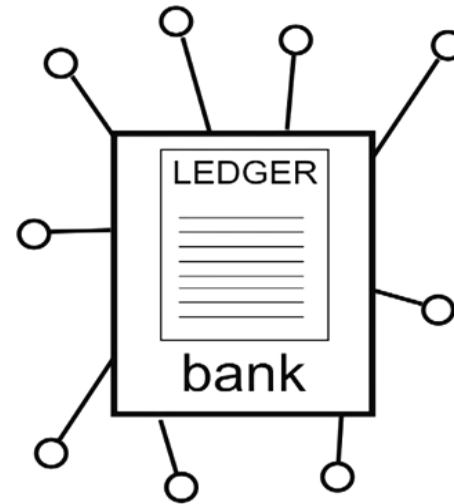
High level brief

- Decentralized ledger
- Each node has it's own copy



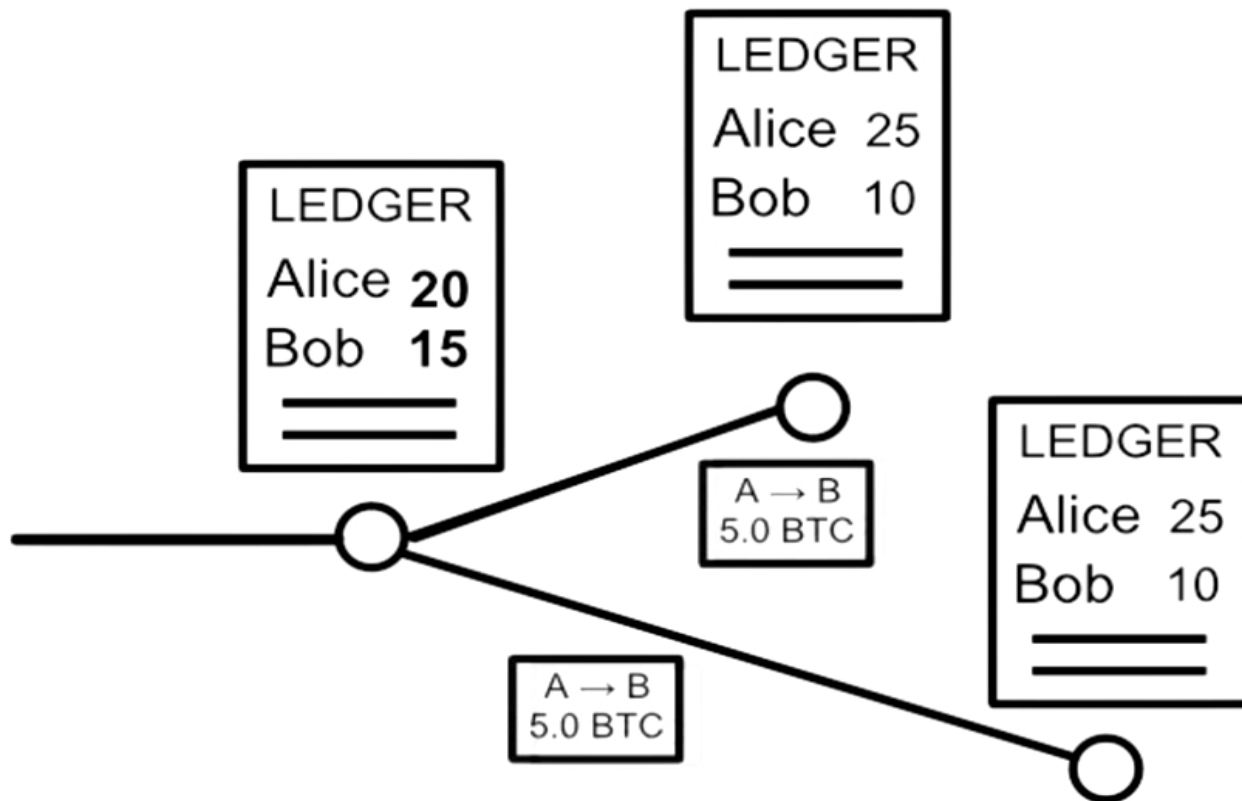
\neq

Centralized Bank
(ex: PayPal)



High level brief

- Nodes applies changes and pass on message



High level brief

- Transactions and balances are public available for all

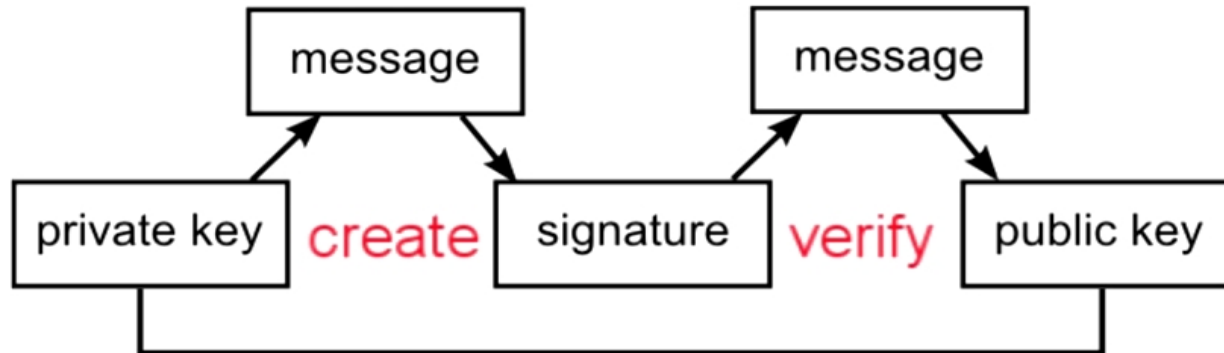
Ledger

Alice	5.3
Bob	100
Frank	700
Carlos	3
Jane	1.3
Charlie	4.645
Scott	.00000001
Kristin	1

...

High level brief

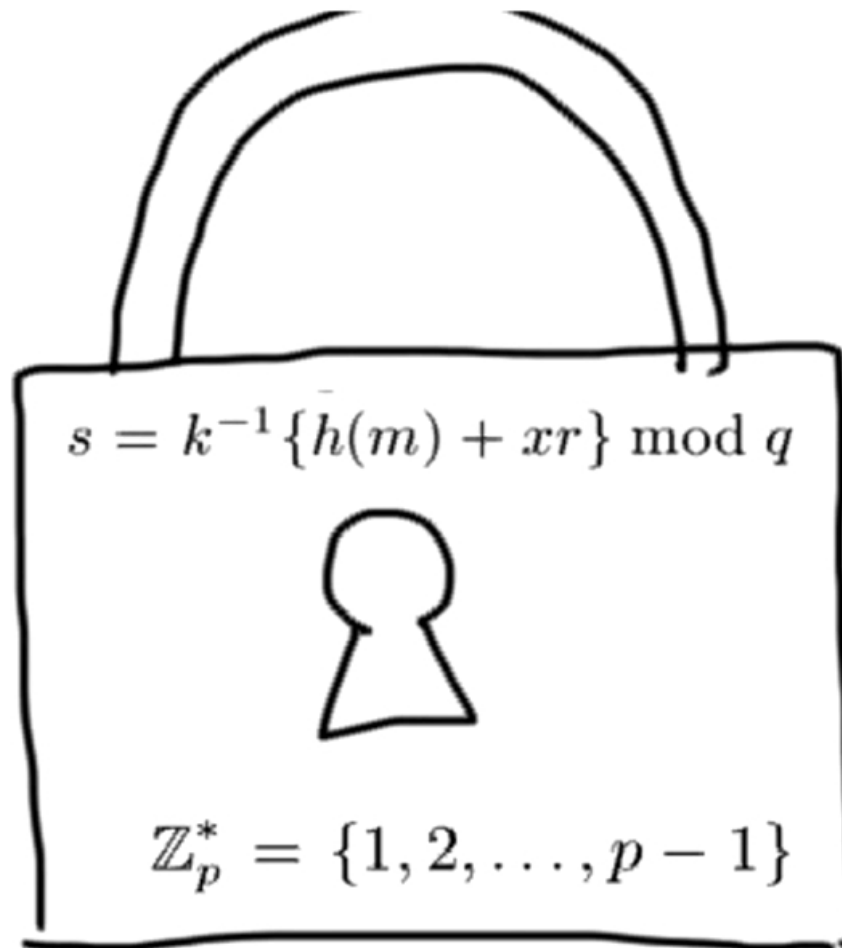
- 160bit hash of an ECDSA public key == “bank account”



→ 13v8NB9ScRa21JDi86GmnZ5d8Z4CjhZMEd
(Alice's Public Key)

High level brief

- Mathematical functions to protect every aspect



High level brief

- No trust
- Decentralized ledger
- Each node has it's own copy
- Nodes applies changes and pass on message
- Transactions and balances are public available for all
- 160bit hash of an ECDSA public key == “bank account”
- Mathematical functions to protect every aspect

... And that's about it!

Hash?

- What is a hash?

Hash?

- What is a hash?
- Often used for checksums (ex. file, password check)

Hash?

- What is a hash?
- Often used for checksums (ex. file, password check)
- In this case, also a 32byte or 256bit number

Hash?

- What is a hash?
- Often used for checksums (ex. file, password check)
- In this case, also a 32byte or 256bit number

SHA256("little me.")

0x

48db362a9723246da3fd21ba423e4c77a4bba95d4f6cbf8c232cb56a3e760df
6

SHA256("This is a longer text, for example some transactions")

0x

27afd01c52c5f1ea8f2f901dfcc94a9099a5a78e7e8c88d143b1120b3708d74d

SHA256("This is a longer text, for example some transactions.")

Bitcoin addresses

- Elliptic curve digital signature algorithm (ECDSA)

Bitcoin addresses

- Elliptic curve digital signature algorithm (ECDSA)
- Base58 (Using non similar characters, ex. 0Oll)

Bitcoin addresses

- Elliptic curve digital signature algorithm (ECDSA)
- Base58 (Using non similar characters, ex. 0Oll)
- Public and private keys (Keypair)

Bitcoin addresses

- Elliptic curve digital signature algorithm (ECDSA)
- Base58 (Using non similar characters, ex. 0Oll)
- Public and private keys (Keypair)
- Generated in “keypool” inside wallet (or 3rdparty)

Bitcoin addresses

- Elliptic curve digital signature algorithm (ECDSA)
- Base58 (Using non similar characters, ex. 0Oll)
- Public and private keys (Keypair)
- Generated in “keypool” inside wallet (or 3rdparty)
- (Alternative) Send Bitcoin to an IP address

Bitcoin addresses

- Elliptic curve digital signature algorithm (ECDSA)
- Base58 (Using non similar characters, ex. 0Oll)
- Public and private keys (Keypair)
- Generated in “keypool” inside wallet (or 3rdparty)
- (Alternative) Send Bitcoin to an IP address
- (Alternative) Not recommended due to MITM attack

Bitcoin addresses

- Elliptic curve digital signature algorithm (ECDSA)
- Base58 (Using non similar characters, ex. 0Oll)
- Public and private keys (Keypair)
- Generated in “keypool” inside wallet (or 3rdparty)
- (Alternative) Send Bitcoin to an IP address
- (Alternative) Not recommended due to MITM attack

Bitcoin address creation

What if the address is already taken?

Like emails

alice@mail , alice1@mail , alicealice@mail ,
alice999@mail, alice420@mail, alice20@mail

Bitcoin address creation

Don't worry.

Possible Bitcoin addresses

1461501637330902918203684832716283019655932542976

1.46×10^{48} or 2^{160}

Bitcoin address creation

- Public key

0478d430274f8c5ec1321338151e9f27f4c676a008bdf8638d07c
0b6be9ab35c71a1518063243acd4dfe96b66e3f2ec8013c8e072
cd09b3834a19f81f659cc3455

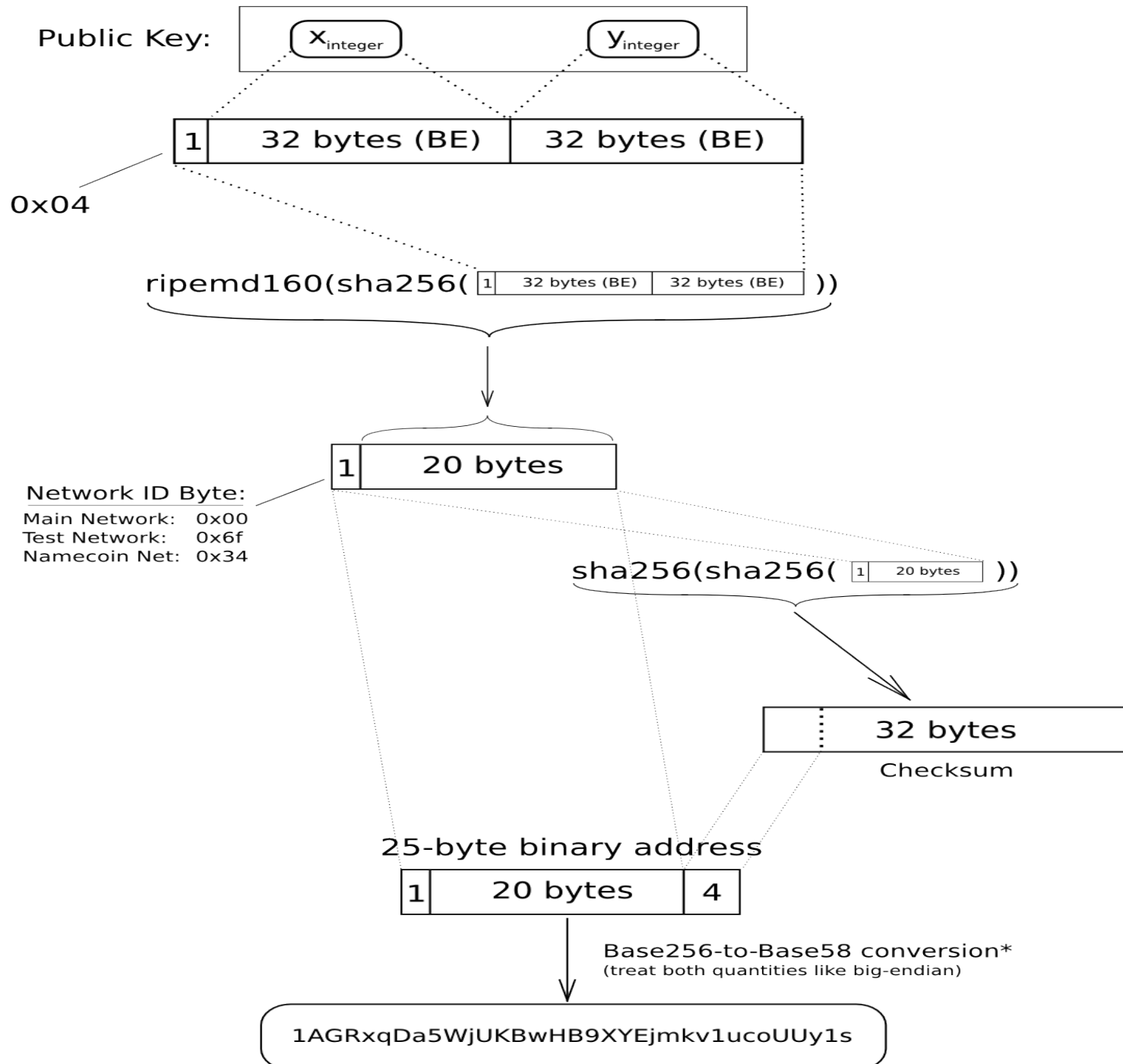
- Private key

5KJvsngHeMpm884wtkJNzQGACErckhHJBGFsvd3VyK5qMZXj
3hS

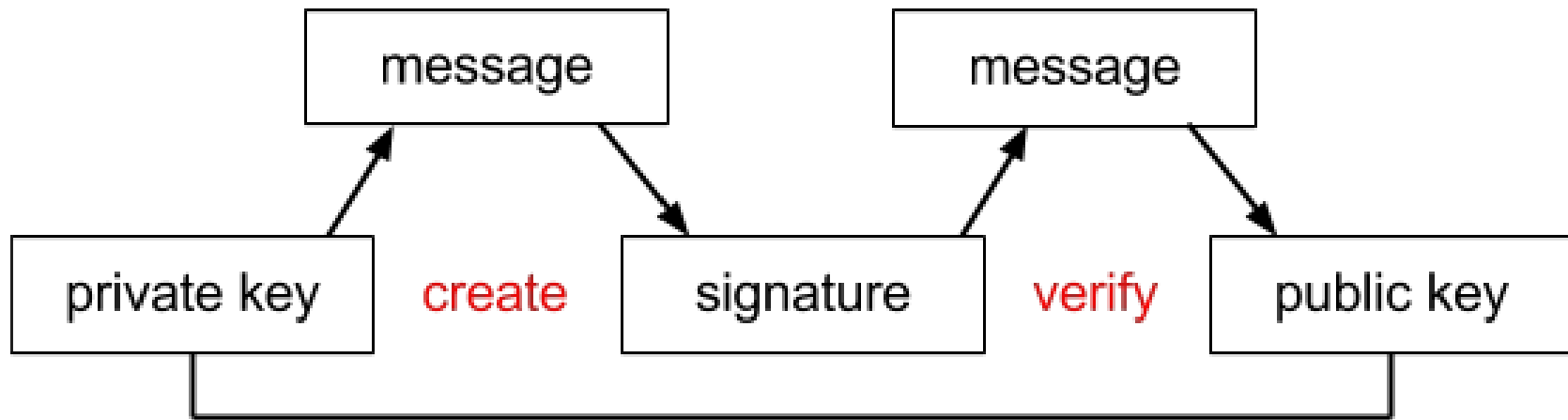
- Address

1JwSSubhmg6iPtRjtyqhUYYH7bZg3Lfy1T

Elliptic-Curve Public Key to BTC Address conversion

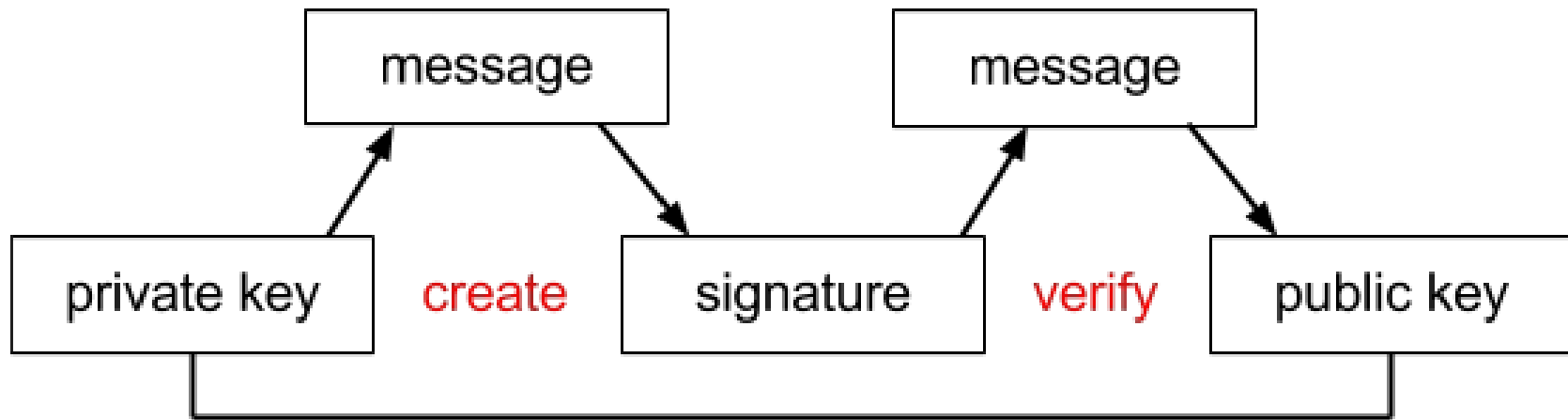


Sending Bitcoins



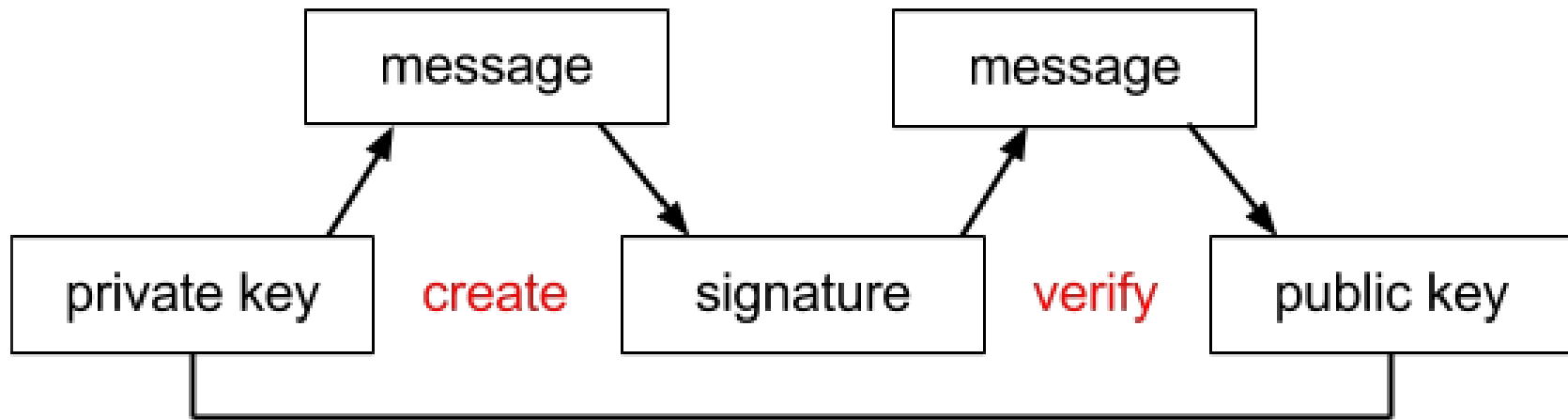
- Send 50.0 BTC from Alice to Bob

Sending Bitcoins



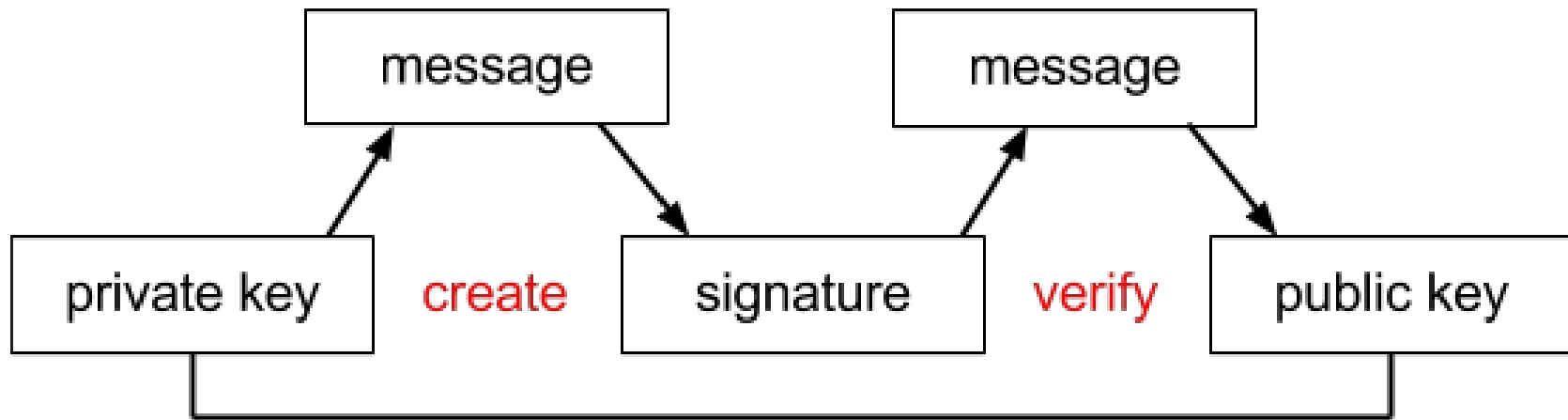
- Send 50.0 BTC from Alice to Bob
- Password check without revealing to network

Sending Bitcoins



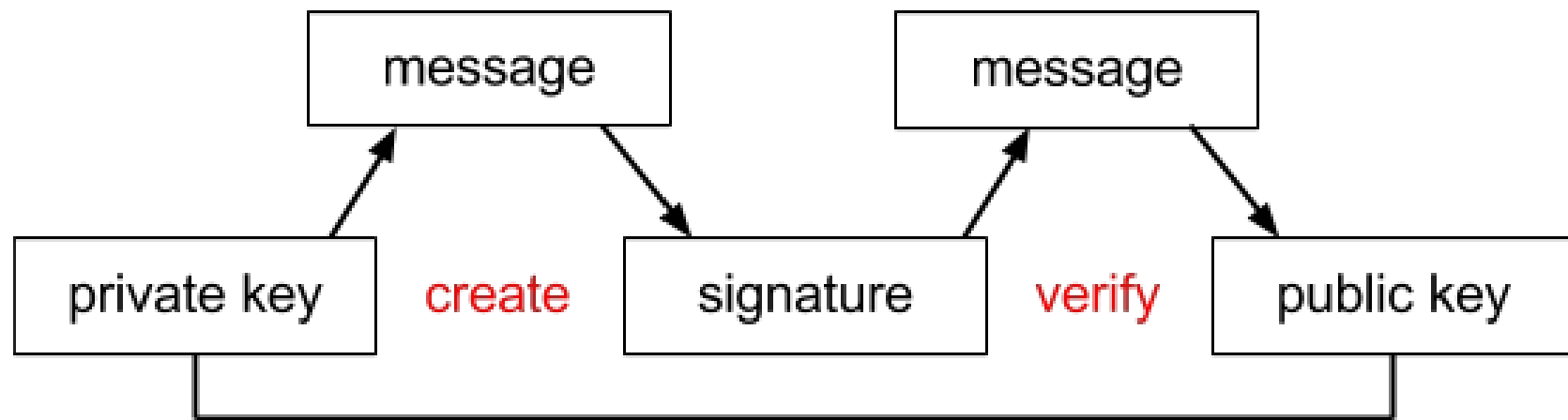
- Send 50.0 BTC from Alice to Bob
- Password check without revealing to network
- Authentic request?

Sending Bitcoins



- Send 50.0 BTC from Alice to Bob
- Password check without revealing to network
- Authentic request?
- Signature!
- Elliptic curve digital signature algorithm (ECDSA)

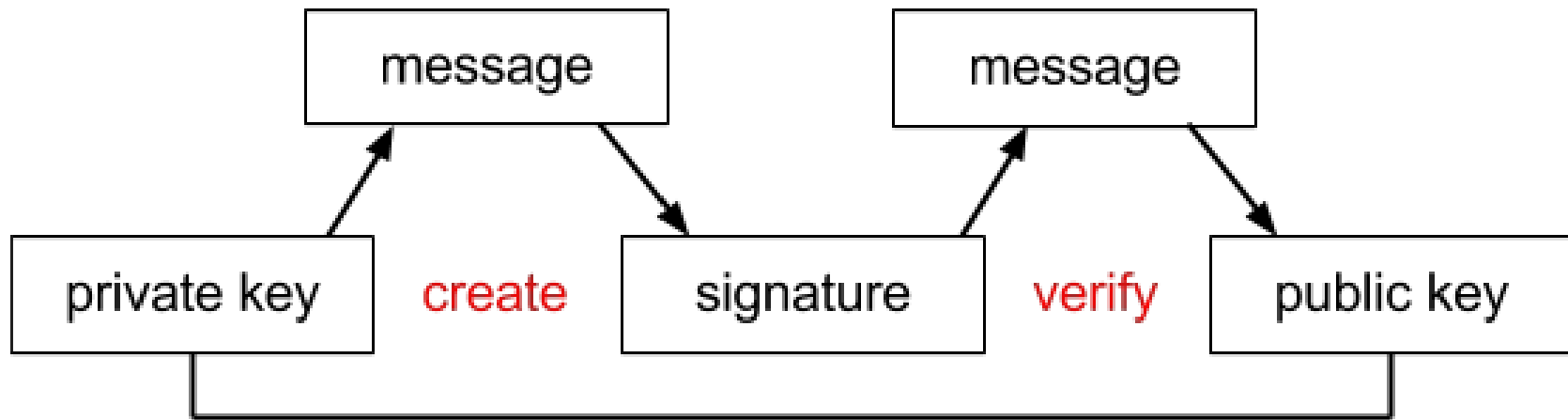
Sending Bitcoins



1427L1ARMZ2AP2oHdUhwY9vuLCfGqfgX2u 50 BTC ➡ 15ijJSSPMw9wkCnaUoXuwxFLexAtoW4C4

- Send 50.0 BTC from Alice to Bob
- Signature = $f(\text{message}, \text{private key})$

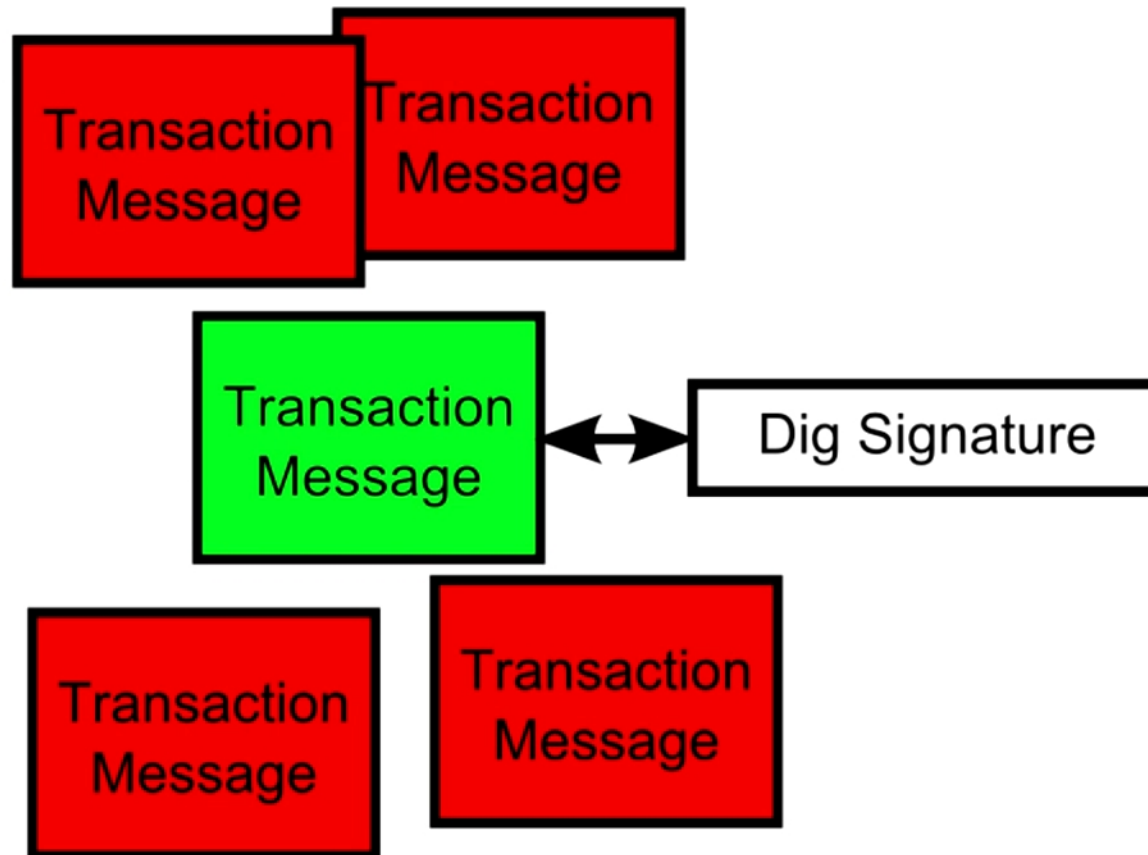
Sending Bitcoins



1427L1ARMZ2AP2oHdUhwY9vuLCfGqfgX2u 50 BTC → 15ijJSSPMw9wkCnaUoXuwCxFLeXAtoW4C4

- Send 50.0 BTC from Alice to Bob
- Signature = $f(\text{message}, \text{private key})$
- $1 = ? v(\text{message}, \text{public key}, \text{signature})$
- Other nodes verify transaction without revealing private key

Sending Bitcoins



Sending Bitcoins

Transaction Messages

		Digital Signature
Alice → Bob	5.0 BTC	04323784...
Alice → Dave	12 BTC	88432738...
Alice → Juan	2000 BTC	00328434...
Alice → Bob	14 BTC	19382637...

^

different every time

Signatures can't be altered.

So far we're covered
how transactions are made and the ledger

Bitcoin address balances

Ledger

Alice	5.3
Bob	100
Frank	700
Carlos	3
Jane	1.3
Charlie	4.645
Scott	.00000001
Kristin	1

...

Bitcoin address balances

Ledger

Alice
Bob
Frank
Carlos
Jane
Charlie
Scott
Kristin

...

Ledger

Transaction List

Accounts and Balances

Alice	5.3
Bob	100
Frank	700
Carlos	3
Jane	1.3
Charlie	4.645
Scott	.00000001
Kristin	1

...

[illegible]

Ledger (All Transactions)

from to amount

1b874A...	16BZZe8...	1.0
167sdu...	13kjhfg...	15.0
1lkj382S	1238fhdj...	6.0
1398fda...	1lkj382S...	500.0
1348dd...	1SD48sd...	34.0
1354sd...	13kjhfg...	1.0
148958...	1asdytrr...	0.0001
1598fjk...	154gkeR...	3.0
13kjhfg...	16BZZe8...	2.0
167sdu...	1487djhk...	5.0
13kjhfg...	1238fhdj...	2445.0

My balance



0.0

Ledger (All Transactions)

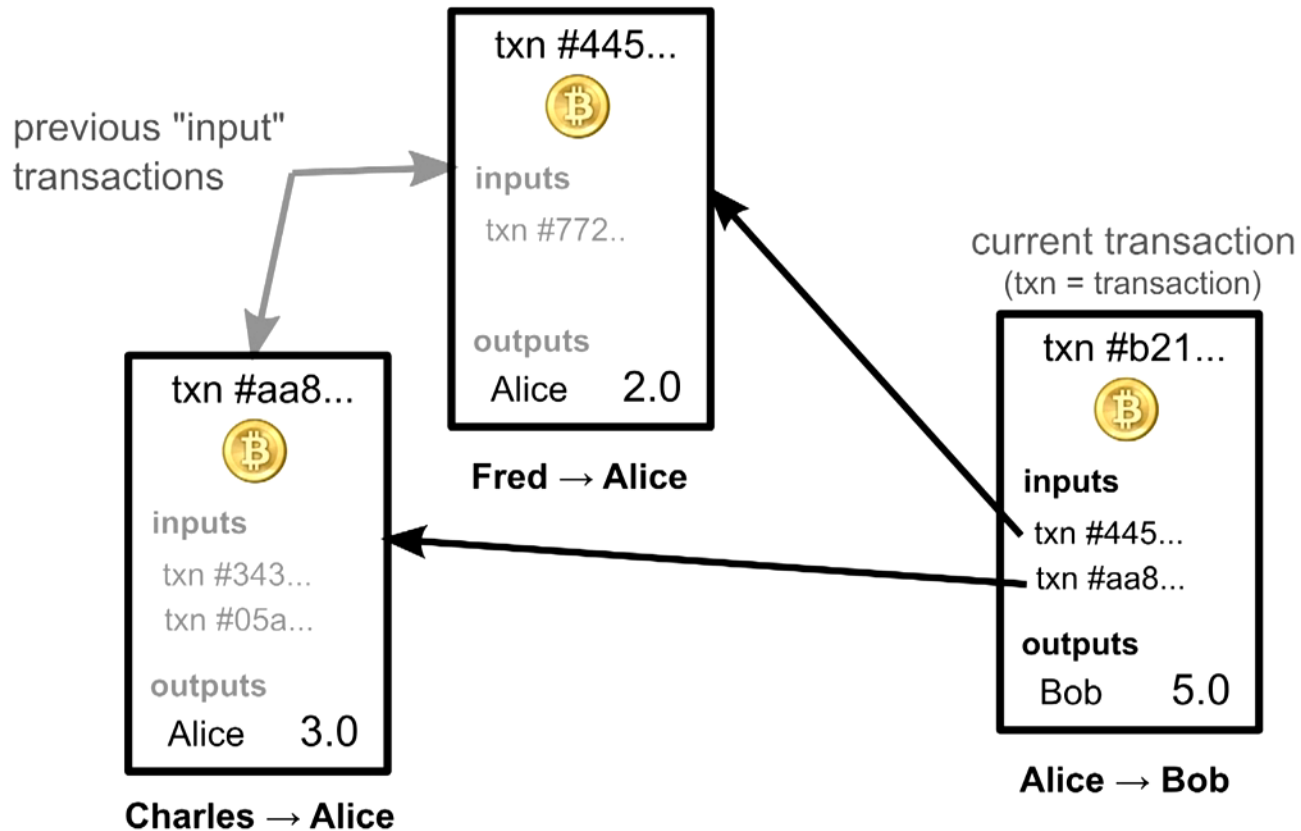
from	to	amount
1348dd...	1SD48sd...	34.0
1354sd...	13kjhfg...	1.0
148958...	1asdytrr...	0.0001
1598fjk...	154gkeR...	3.0
13kjhfg...	16BZZe8...	2.0
167sdu...	1487djhk...	5.0
13kjhfg...	1238fhdj...	2445.0
1398fda...	1lkj382S...	7.0
1348dd...	13kjhfg.....	10.0
1354sd...	1aa5dfdf...	1.0
148958...	1asdytrr...	56.0
1598fjk...	154gkeR...	3.0

My balance

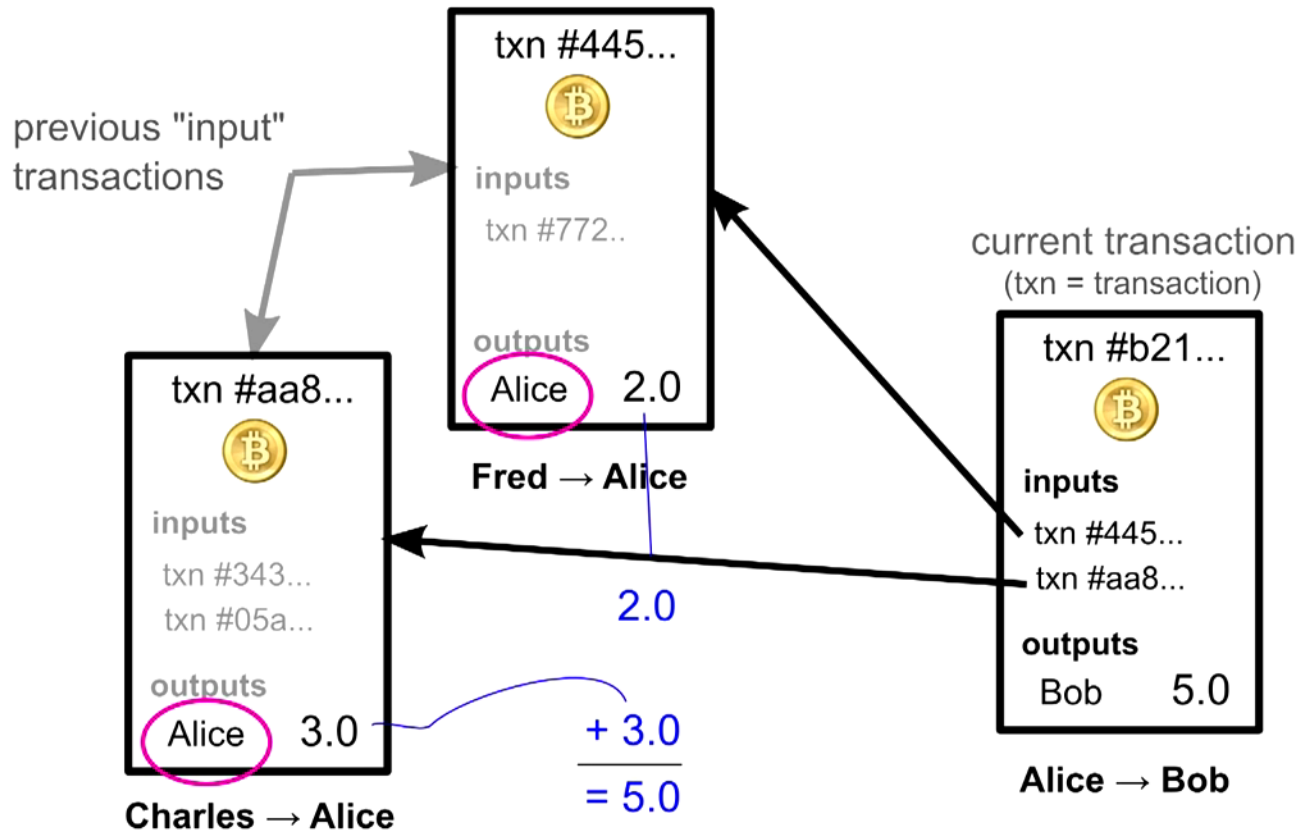


15.0

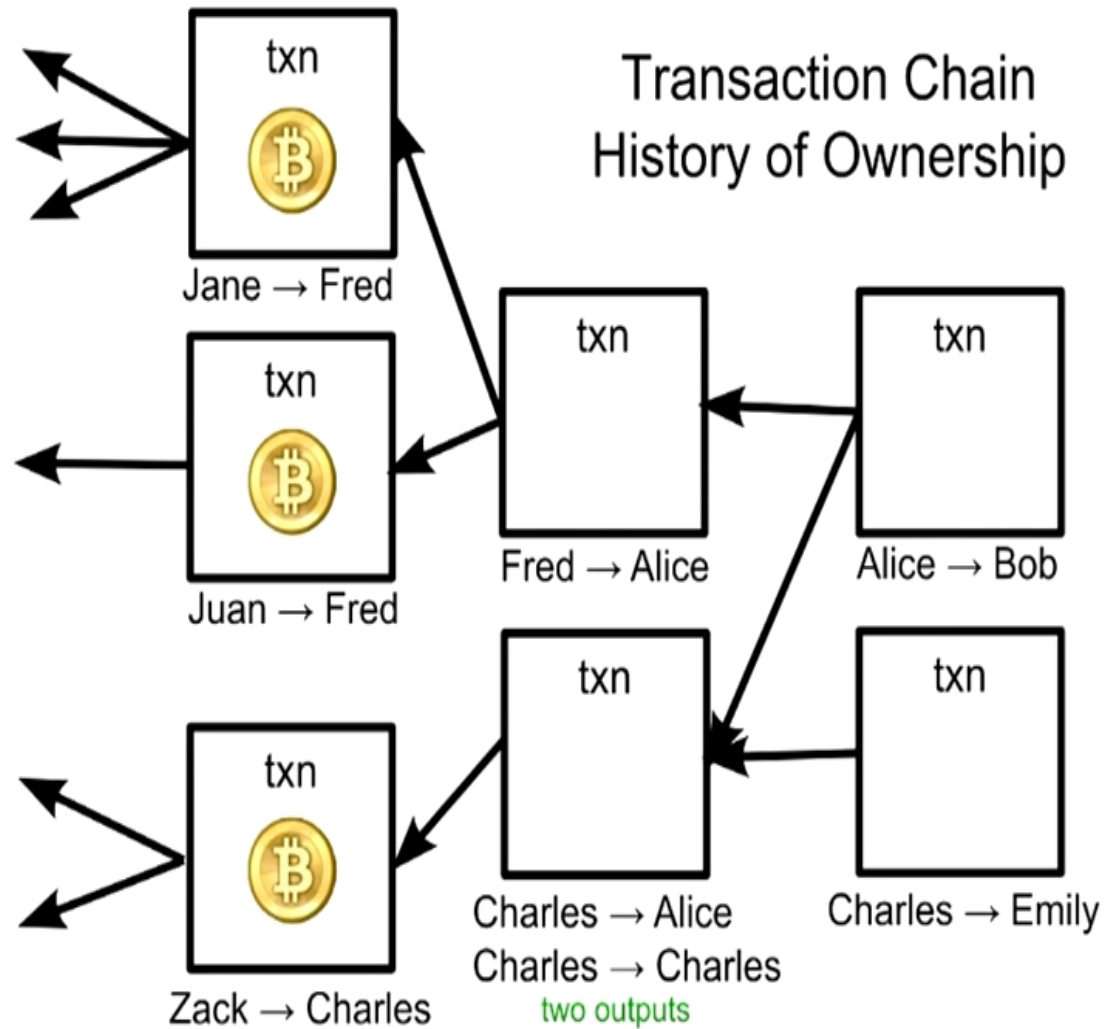
Bitcoin address balances



Bitcoin address balances



Transaction Chain History of Ownership



Real transactions

Inputs

Previous output (index) ²	Amount ²	From address ²	Type ²	ScriptSig ²
eb38f77560ca...1	8	1P9SgqzjFWgWVAuZBFwinNPV7LunaJpgTj	Address	30450220078df7c48ed152bd40eae4a73afefc3l 044760639da2c0d6158484e1a4dab332fefc4bb! ◀ [] ▶
b912994fca58...1	0.03	18Mk65wV1E5kCVHFSHvUTU6zt4yVEKM5Ft	Address	304502204e877fc5ca3783e165052e64c4788dd 04769bbfc55cbd412784e024c8624f8c4f42d7ct ◀ [] ▶
58379d94fe85...15	1	1G4hfmM2ufAPEECdawg5gtvUTBB2PxyLr2	Address	3044022075d23fd4a8004866777210f51f46c96i 046dd45b37fe3ff33f1563458cfbdfb7f922d1b4a- ◀ [] ▶
fc9d1cd1c2ac...1	130	1LpQVnJSMgqqibQBGZwbobdX2Ghn9YWYc7	Address	3046022100a65a188b89a4e5ae2eaa5ba387503 04ba81a1a538c5ddf7e0c76884497ab522456b9 ◀ [] ▶
7b6f7d4a521c...1	0.55357267	16Kb6XppHUBigmYQDpRvxx9jNE9Az5Xvcb	Address	3045022100eeb76e61abe62d38fd462eafd1d11f 04f4fa1d3e26f3e7058038871a31b8bf63fd127f6 ◀ [] ▶
544097a30e09...0	0.03270607	1JnsDx1g6c757z8AnJUemj46YQgCTw54QN	Address	3045022100859df2ced47493e86a849cce10615 04de257fe6490bd16188be6d06ca7b34816fa4b- ◀ [] ▶

Outputs²

Outputs

Index ²	Redeemed at input ²	Amount ²	To address ²	Type ²	ScriptPubKey ²
0	8baaca27d158...	0.01071174	1F7BgZQbyWTWzEMUKNzzLdkbjaQT9K96m	Address	OP_DUP OP_HASH160 9abd2e0c0a63dea36b75c3128fe15d82f274e39- OP_EQUALVERIFY OP_CHECKSIG ◀ [] ▶
1	1bb973b4ccc8...	139.605567	1NT2zFMa11NiCZydt4kqgXRZPF3iS6ZPGZ	Address	OP_DUP OP_HASH160 eb471d7a903e538cb94c1f2faf20eaadad8479af OP_EQUALVERIFY OP_CHECKSIG

Real transactions

Inputs

Previous output (index) ²	Amount ²	From address ²	Type ²	ScriptSig ²
eb38f77560ca...1	8	1P9SgqzjFWgWVAuZBFwimNPV7LuuajpgTj	Address	30450220078df7c48ed152bd40eae4a73afefc3l 044760639da2c0d6158484e1a4dab332fefc4bb! ◀ [] ▶
b912994fca58...1	0.03	18Mk65wV1E5kCVHFSbvUTU6zt4yVFKM5Ft	Address	304502204e877fc5ca3783e165052e64c4788dd 04769bbfc55cbd412784e024c8624f8c4f42d7cb ◀ [] ▶
58379d94fe85...15	1	1G4hfmM2ufAPEECdawg5gtvUTBB2PxxLr2	Address	3044022075d23fd4a8004866777210f51f46c96l 046dd45b37fe3ff33f1563458cfbdfb7f922d1b4a- ◀ [] ▶
fc9d1cd1c2ac...1	130	1LpQVnJSMgqqibQBGZwbobdX2Ghm9YWYc7	Address	3046022100a65a188b89a4e5ae2eaa5ba387503 04ba81a1a538c5ddf7e0c76884497ab522456b9 ◀ [] ▶
7b6f7d4a521c...1	0.55357267	16Kb6XppHUbignYQDpRvzx9jNE9Az5Xvcb	Address	3045022100eeb76e61abe62d38fd462eafd1d11f 04f4fa1d3e26f3e7058038871a31b8bf63fd127f6 ◀ [] ▶
544097a30e09...0	0.03270607	1JnsDx1g6c757z8AnJUemj46YQgCTw54QN	Address	3045022100859df2ced47493e86a849cce10615 04de257fe6490bd16188be6d06ca7b34816fa4b- ◀ [] ▶

Outputs²

139.616

Outputs

Index ²	Redeemed at input ²	Amount ²	To address ²	Type ²	ScriptPubKey ²
0	8baaca27d158... 0.011	0.01071174	1F7BgzQbyWTWzEMUKNzzLdjkbjaQT9K96m	Address	OP_DUP OP_HASH160 9abd2e0c0a63dea36b75c3128fe15d82f274e394 OP_EQUALVERIFY OP_CHECKSIG ◀ [] ▶
1	1bb973b4ccc8... 139.606	139.605567	1NT2zFMa11NiCZydt4kqgXRZPf3iS6ZPGZ	Address	OP_DUP OP_HASH160 eb471d7a903e538cb94c1f2faf20eaadad8479af OP_EQUALVERIFY OP_CHECKSIG

back to sender

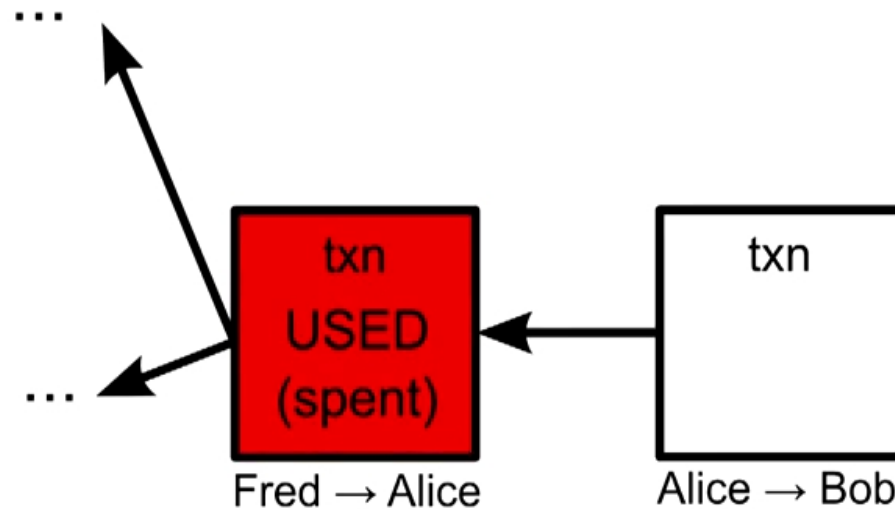
Real transactions

Block 245795, July 10th, 2013 (blockexplorer.com)

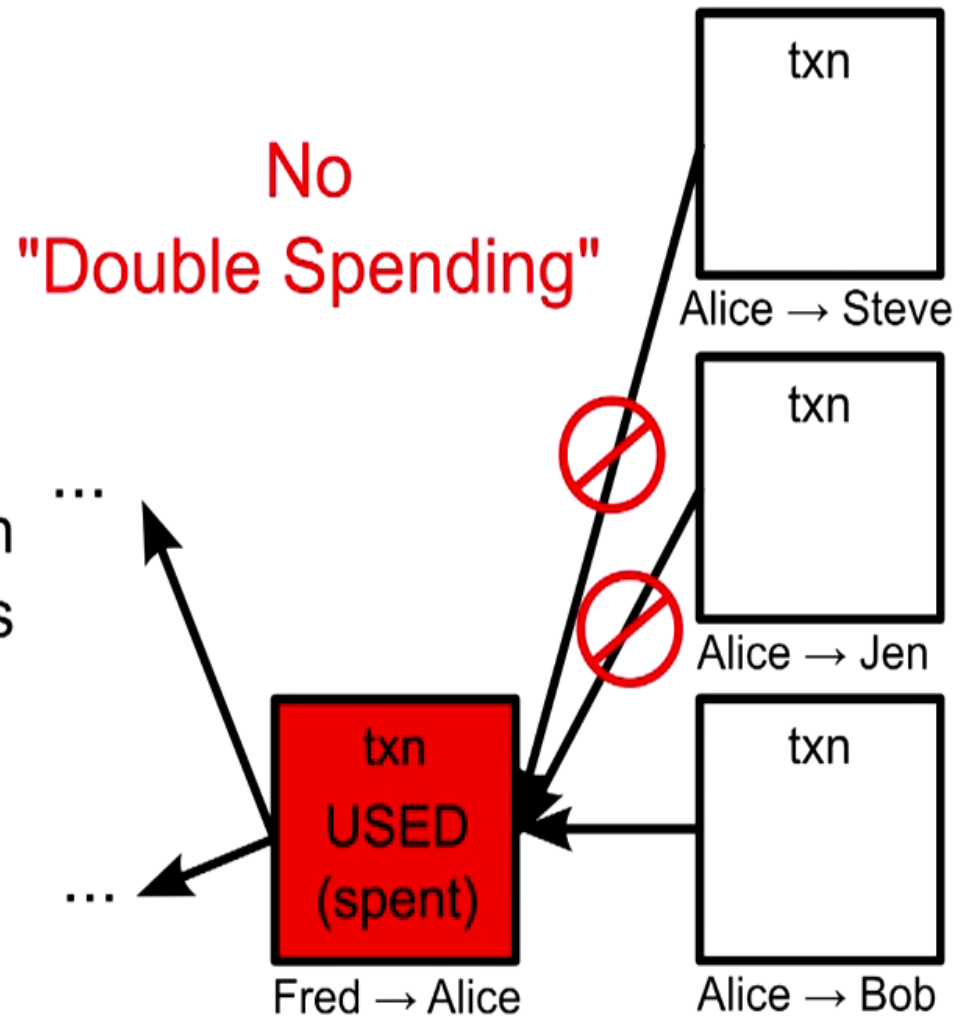
Transaction ²	Fees	Size (kB) ²	From (amount) ²	To (amount) ²
5b8abf9b7c...	0	0.104	Generation: 25 + 0.22670701 total fees	17bZK6PaC813v7sgRzmEZGeXKupp15J6: 25.22670701
b4d3e68059...	0 0	1.116	1wrQkR9ShehDnjDuJdAar9ikQwTeAWFiP: 27.16289 15TeGQW9SnXGqZLMxKRQKC7aKF1ezYJRuz: 400 1wrQkR9ShehDnjDuJdAar9ikQwTeAWFiP: 16.30322 1wrQkR9ShehDnjDuJdAar9ikQwTeAWFiP: 62.01666822 1wrQkR9ShehDnjDuJdAar9ikQwTeAWFiP: 1.1498 1wrQkR9ShehDnjDuJdAar9ikQwTeAWFiP: 44.86013 1wrQkR9ShehDnjDuJdAar9ikQwTeAWFiP: 2.44169	1MJnVuvz8PQbd66dtZW5FSkTLwcBpkHS4h: 0.58452822 1GAmvSbcugxoPcnoDGmnvosAE92LNWVvxN: 553.34987
2be12dfb3c...	0 0	0.437	16vZKzn7NSrWLBLoV1mS5EVnoyBFcCUyUY: 1.28 1APXHgo37zXYrTNRJ7pwg9yeDRyoacSaD1: 0.12096168	152DAXR8HQ7eAprZYPIvDWo1MYqcfXRCe: 0.07656168 19KQzTt7wmCn87ocy8op5cd2BHpozMZZ2D: 1.3244
b81b66dc39...	0.0005 .0005	0.258	1PYw3w37XKqa3NXzt94sBZHe78BRhi5v2x: 705.42113185	17d1BNKSaVt5DswzvuVDugwpczKBzwAEuU: 705.40728813 1ChY3gi9v376V9rf73BY23GQhbx3fguoWS: 0.01334372
a716d71690...	0.0003 .0003	0.259	1KDpGZ2ZNU7UjJf7HUsa7wmDDvy9w6nvn: 238.42376903	1HMBUMzQXHM2csdL3DKJ4Y9pWRo2gWSSmb: 232.23066347 1G56C8Gcon1KneNJK61GTVfsHeNgtBjH: 6.19280556

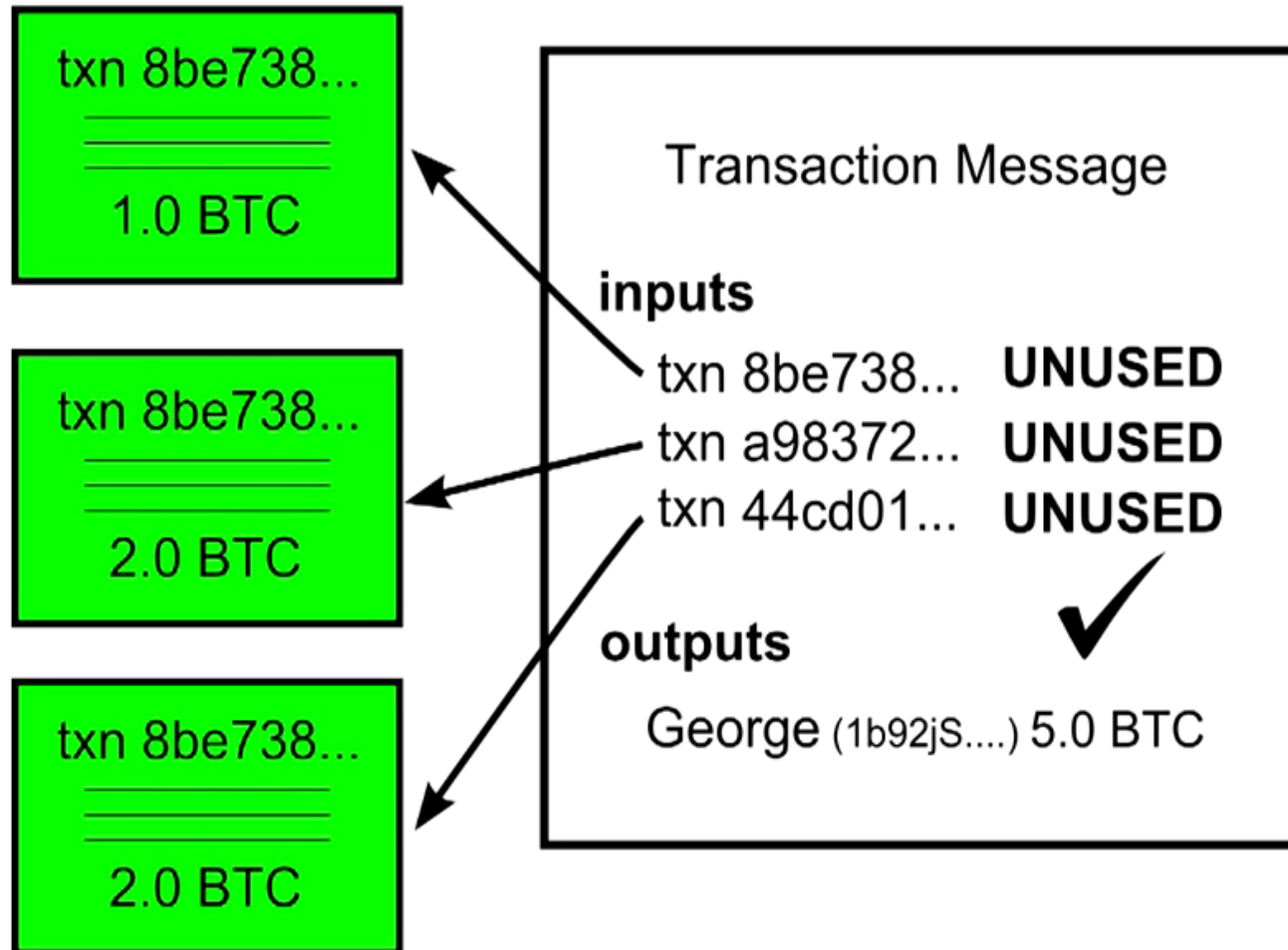
Back to transactions

Each Transaction Can
Only be used Once as
an Input.



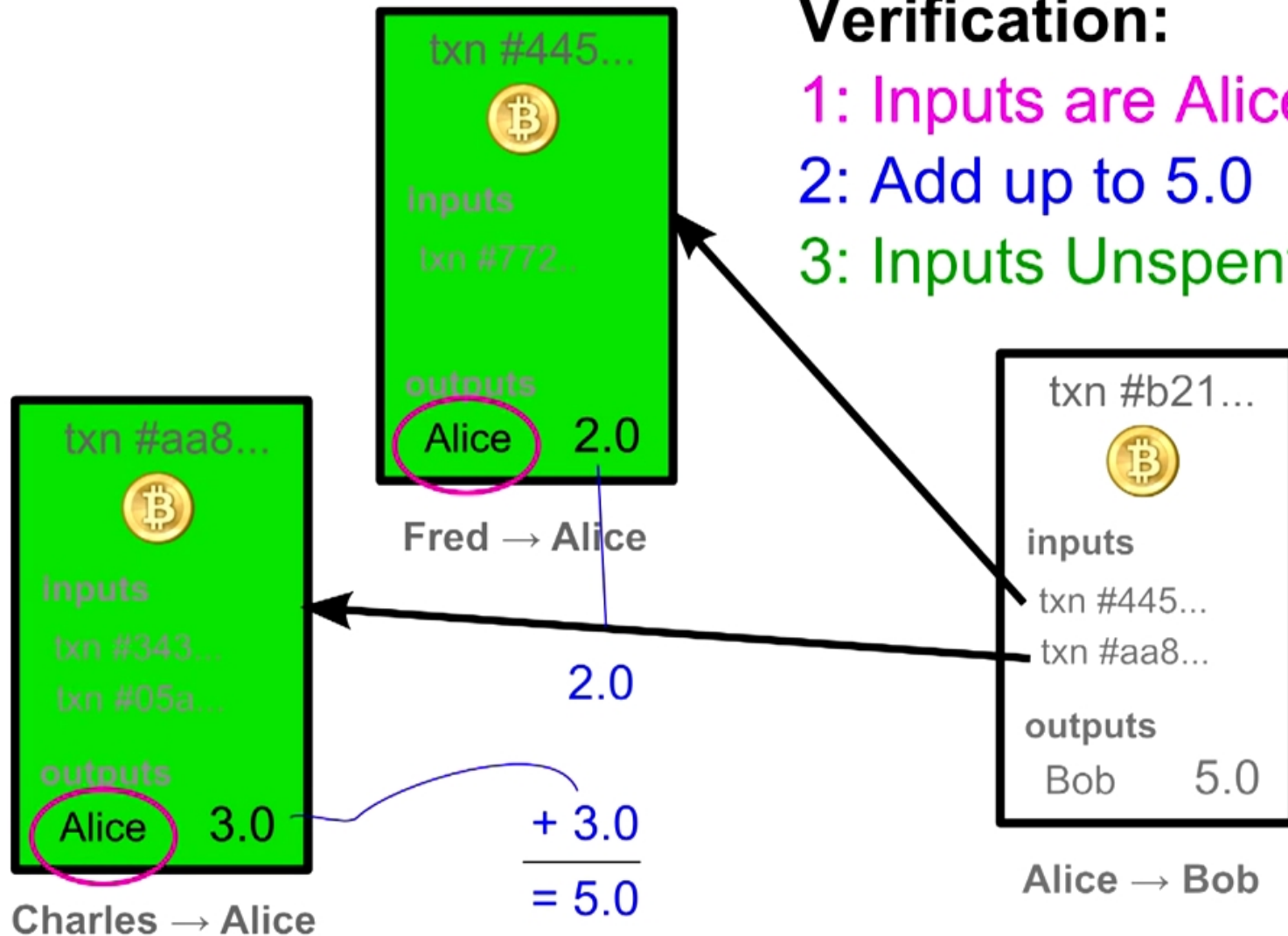
Each Transaction Can
Only be used Once as
an Input.





Verification:

- 1: Inputs are Alice's
- 2: Add up to 5.0
- 3: Inputs Unspent



Complex transactions

Typical output:

```
OP_DUP OP_HASH160
9abd2e0c0a63dea36b75c3128fe15d82f274e394
OP_EQUALVERIFY OP_CHECKSIG
```


Complex transactions

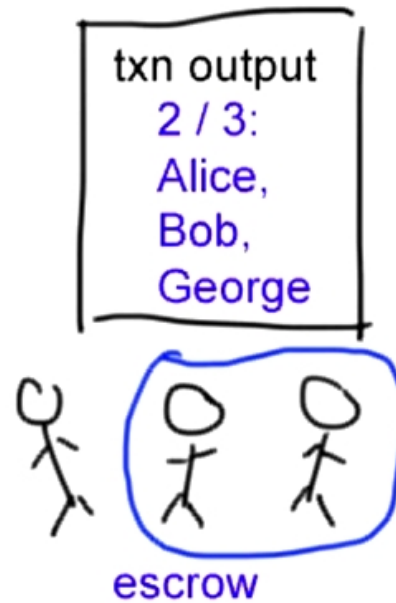
OP_IF	99	0x63	<expression> if [statements] [else [statements]]* endif		If the top stack value is not 0, the statements are executed. The top stack value is removed.
OP_NOTIF	100	0x64	<expression> if [statements] [else [statements]]* endif		If the top stack value is 0, the statements are executed. The top stack value is removed.
OP_ELSE	103	0x67	<expression> if [statements] [else [statements]]* endif		If the preceding OP_IF or OP_NOTIF or OP_ELSE was not executed then these statements are and if the preceding OP_IF or OP_NOTIF or OP_ELSE was executed then these statements are not.
OP_ENDIF	104	0x68	<expression> if [statements] [else [statements]]* endif		Ends an if/else block.
OP_VERIFY	105	0x69	True / false	Nothing / False	Marks transaction as invalid if top stack value is not true. True is removed, but false is not.
OP_RETURN	106	0x6a	Nothing	Nothing	Marks transaction as invalid.

Stack

Word	Opcode	Hex	Input	Output	Description
OP_TOALTSTACK	107	0x6b	x1	(alt)x1	Puts the input onto the top of the alt stack. Removes it from the main stack.
OP_FROMALTSTACK	108	0x6c	(alt)x1	x1	Puts the input onto the top of the main stack. Removes it from the alt stack.
OP_IFDUP	115	0x73	x	x / x x	If the top stack value is not 0, duplicate it.
OP_DEPTH	116	0x74	Nothing	<Stack size>	Puts the number of stack items onto the stack.
OP_DROP	117	0x75	x	Nothing	Removes the top stack item.
OP_DUP	118	0x76	x	x x	Duplicates the top stack item.
OP_NIP	119	0x77	x1 x2	x2	Removes the second-to-top stack item.
OP_OVER	120	0x78	x1 x2	x1 x2 x1	Copies the second-to-top stack item to the top.
OP_PICK	121	0x79	xn ... x2 x1 x0 <n>	xn ... x2 x1 x0 xn	The item <i>n</i> back in the stack is copied to the top.
OP_ROLL	122	0x7a	xn ... x2 x1 x0 <n>	... x2 x1 x0 xn	The item <i>n</i> back in the stack is moved to the top.
OP_ROT	123	0x7b	x1 x2 x3	x2 x3 x1	The top three items on the stack are rotated to the left.

Complex transactions

Transactions: Mathematical Puzzles



First Transaction: 2009, Jan 3

50 BTC

04678afdb0fe5548271967f1a67130b7105cd6a828e0390
9a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec11
2de5c384df7ba0b8d578a4c702b6bf11d5f
OP_CHECKSIG

Complex transactions

Typical output:

```
OP_DUP OP_HASH160
9abd2e0c0a63dea36b75c3128fe15d82f274e394
OP_EQUALVERIFY OP_CHECKSIG
```

Money erased via invalid transactions

2011, Oct 28th, cerca block 150951

amount	transaction ref (hash)
24.31	111291fcf8ab84803d42ec59cb4eaceadd661185242a1e8f4b7e49b79ecbe5f3
100.00	81f591582b436c5b129f347fe7e681afd6811417973c4a4f83b18e92a9d130fd
37.000	ddddf9f04b4c1d4e1185cacf5cf302f3d11dee5d74f71721d741fbb507062e9e
98.48055	305fbc2ec7f7f2bc5a21d2dfb01a5fc52ab5d064a7278e2ecbab0d2a27b8c392
39.8100	f0137a6b31947cf7ab367ae23942a263272c41f36252fcd3460ee8b6e94a84c1
65.0	633acf266c913523ab5ed9fcc4632bae18d2a7efc1744fd43dd669e5f2869ce5
100.00	5bd88ab32b50e4a691dcfd1fff9396f512e003d7275bb5c1b816ab071beca5ba

...

Trust?

- How can you trust previous transactions?

Trust?

- How can you trust previous transactions?
- You can! That's the “block chain”

Trust?

- How can you trust previous transactions?
- You can! That's the “block chain”
- Downloaded on initial launch

Trust?

- How can you trust previous transactions?
- You can! That's the “block chain”
- Downloaded on initial launch
- As of 15 Jan 2014, 18Gb

Bitcoin transaction security

Digital signatures
Referenced transactions

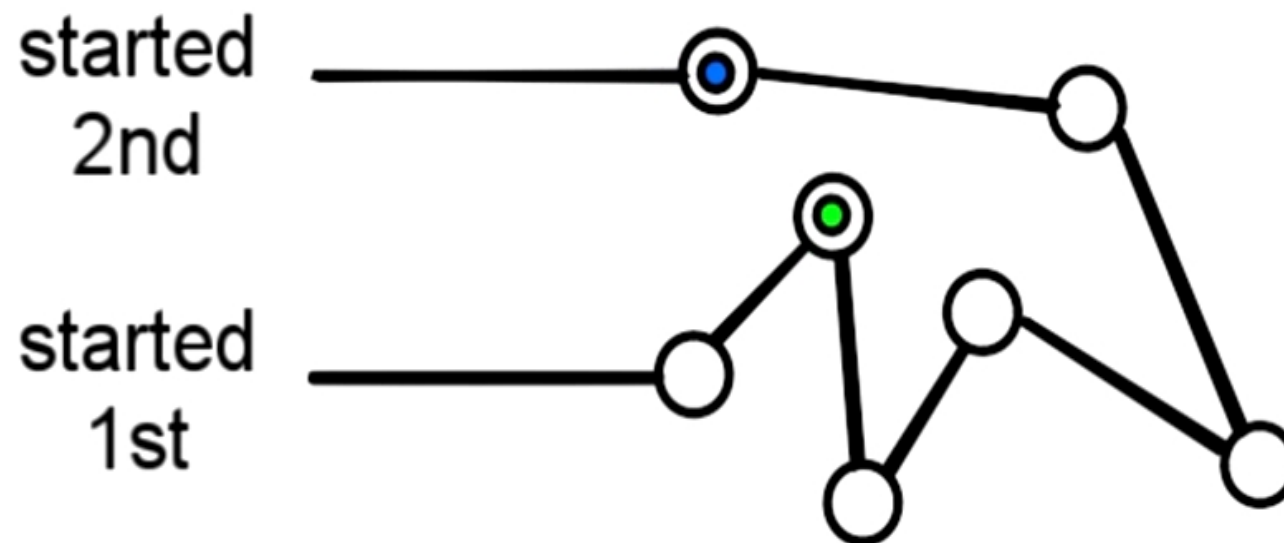
Security Hole: Transaction Order

txn msg

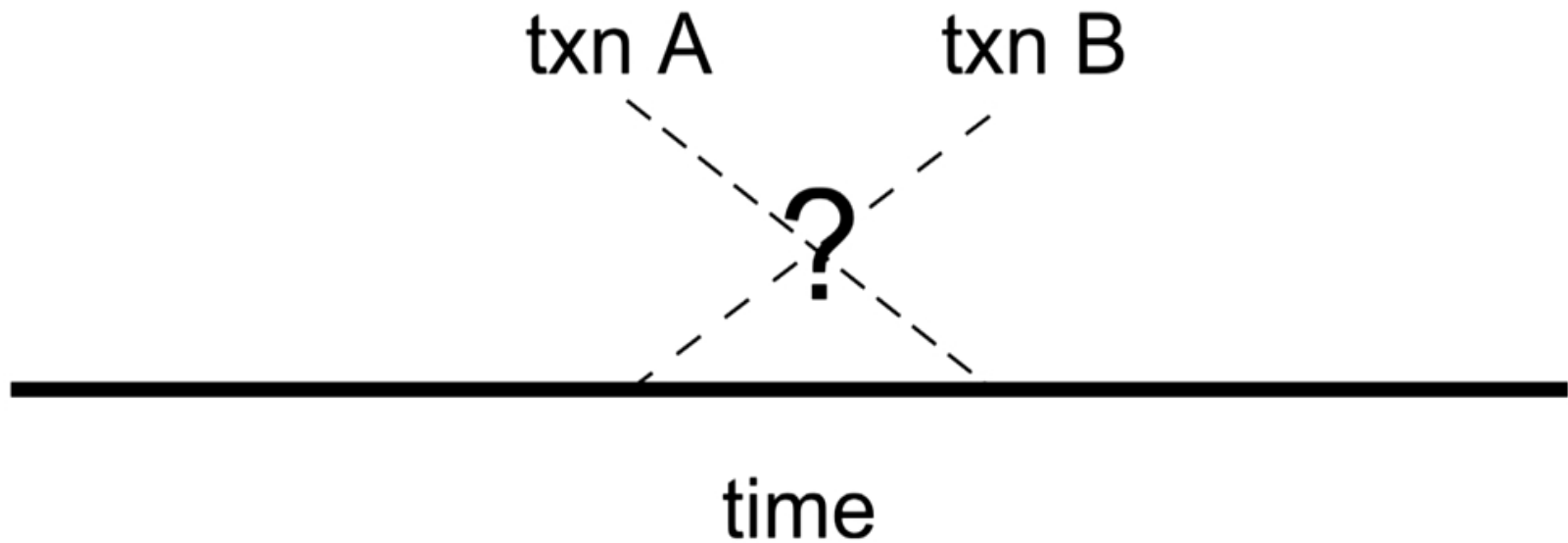
time:

Aug 3rd, 1492

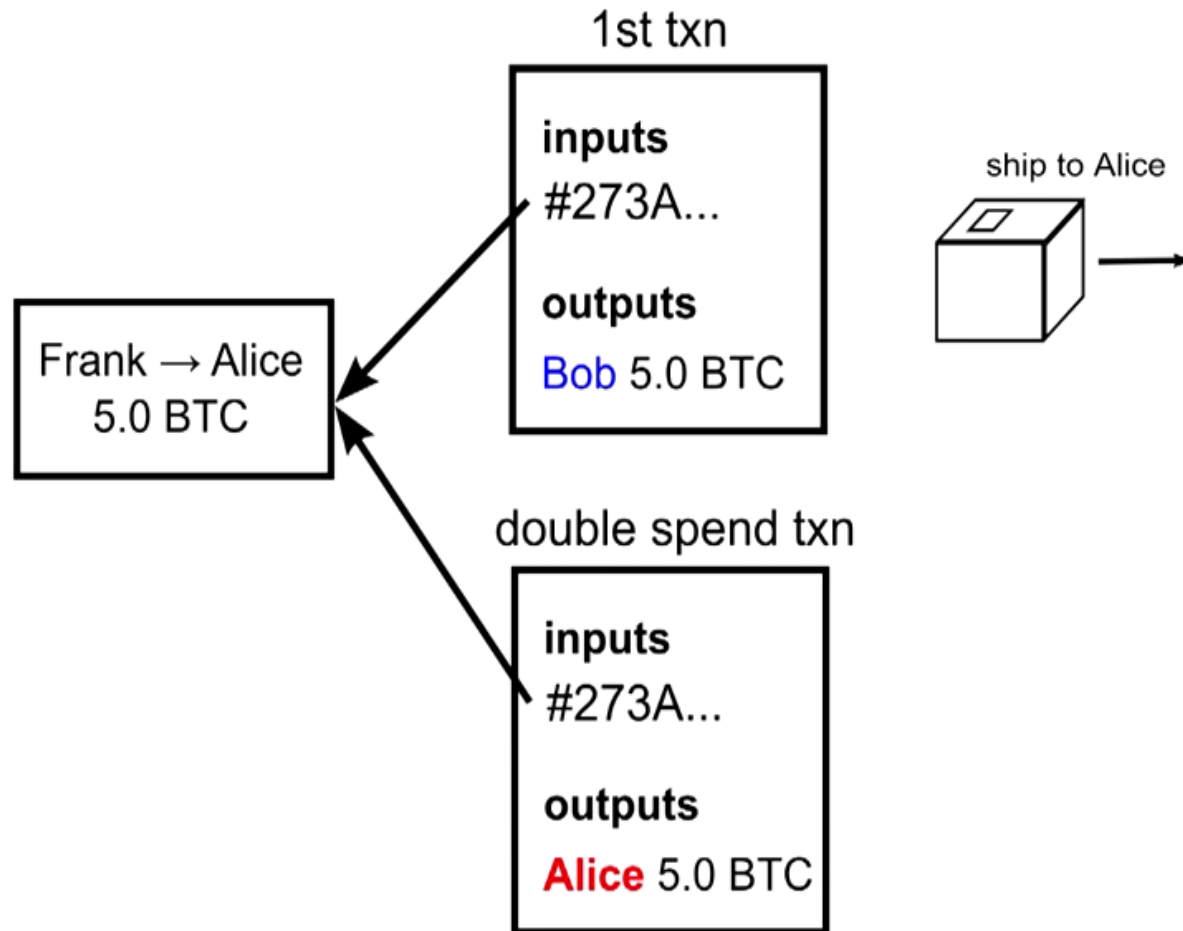
Security Hole: Transaction Order



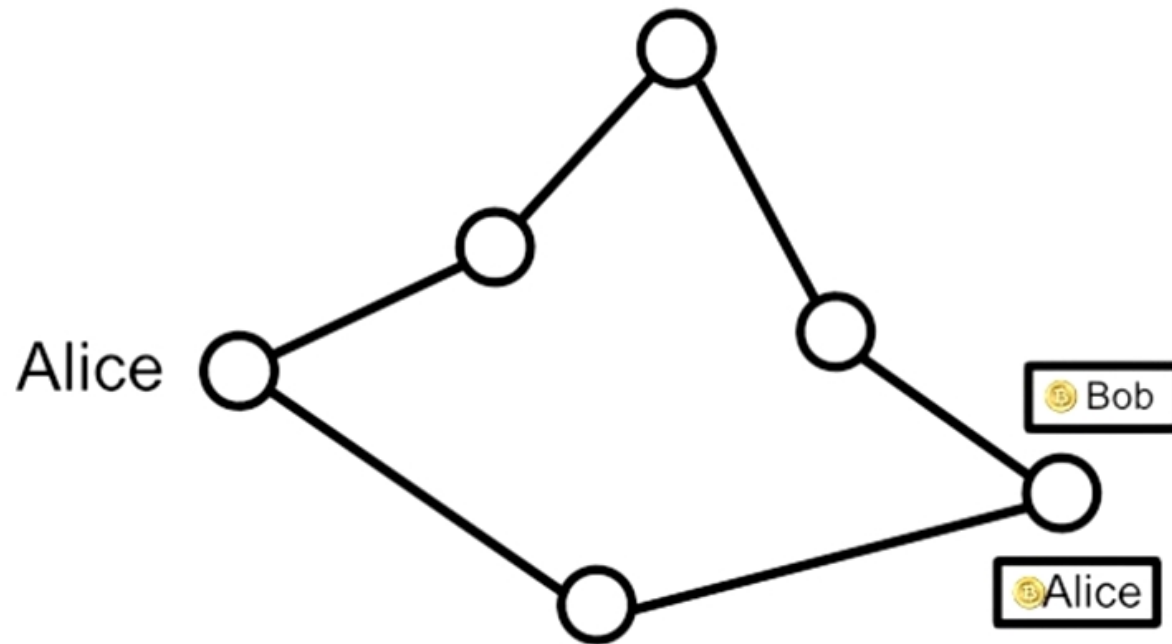
Security Hole: Transaction Order



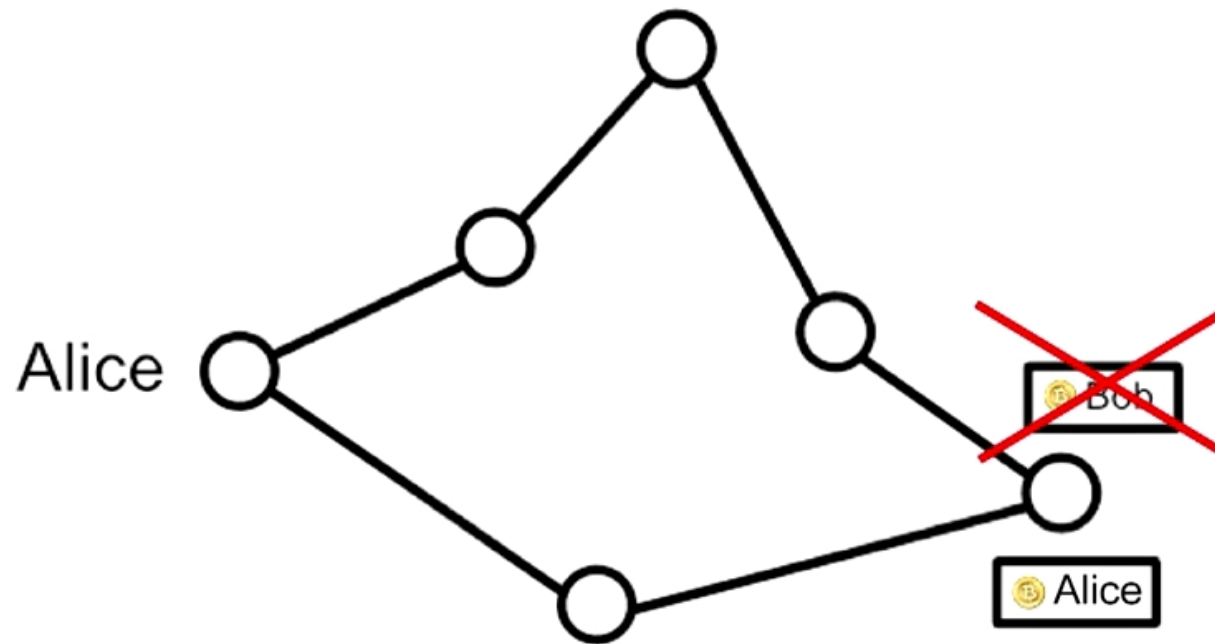
Double Spending Fraud



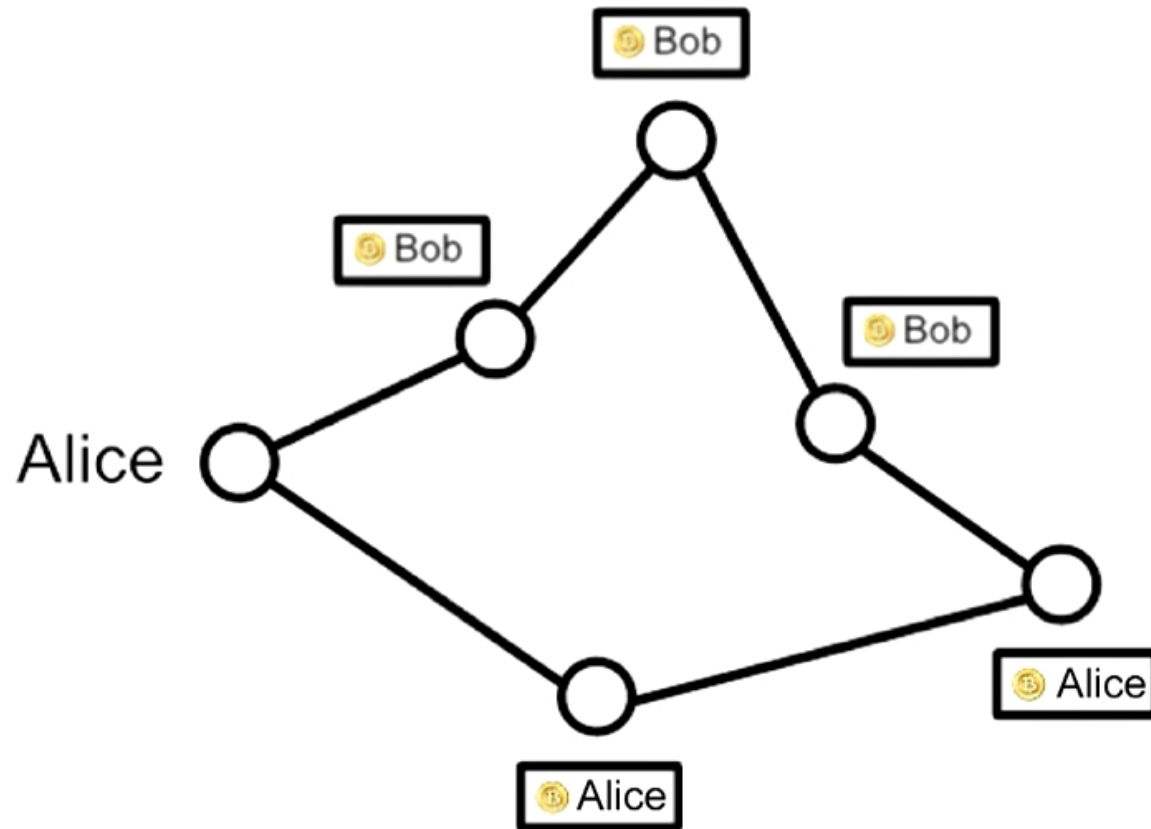
Double Spending Fraud



Double Spending Fraud



Double Spending Fraud



Solution

- Nodes need to agree on transaction order

Solution

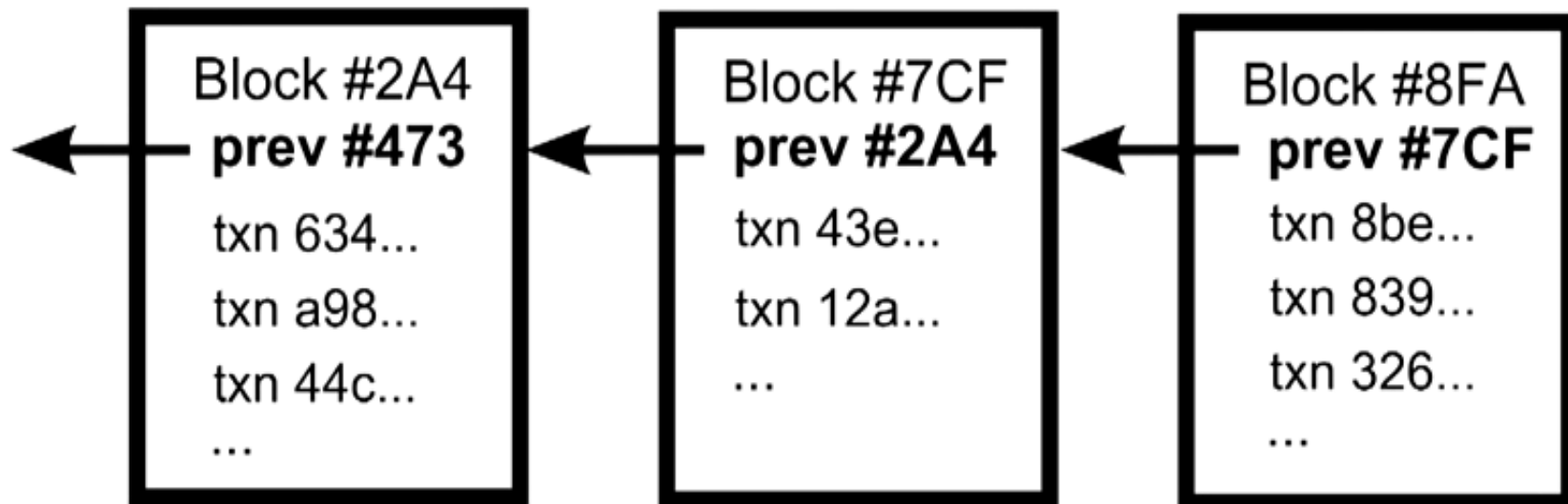
- Nodes need to agree on transaction order
- Not easy in a decentralized system

Solution

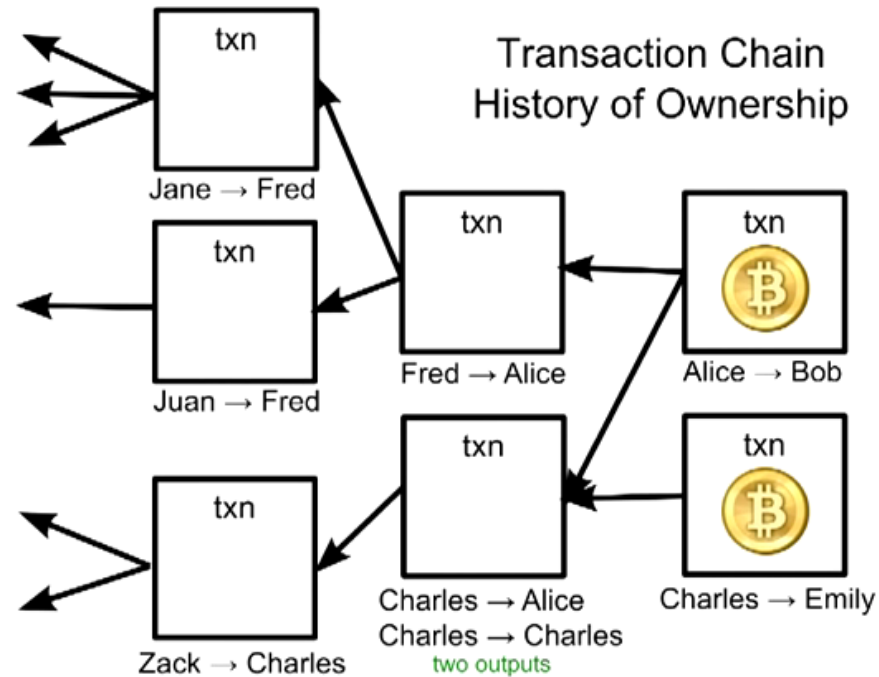
- Nodes need to agree on transaction order
- Not easy in a decentralized system
- Ordering solution: The block chain

Solution

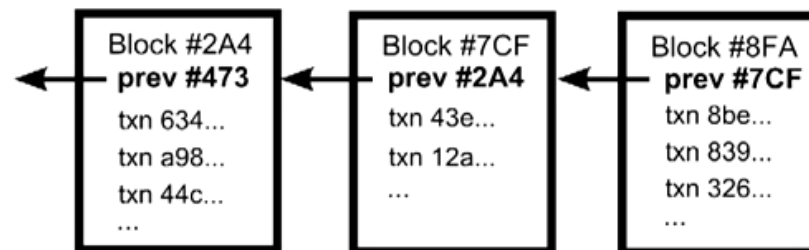
- Nodes need to agree on transaction order
- Not easy in a decentralized system
- Ordering solution: The block chain



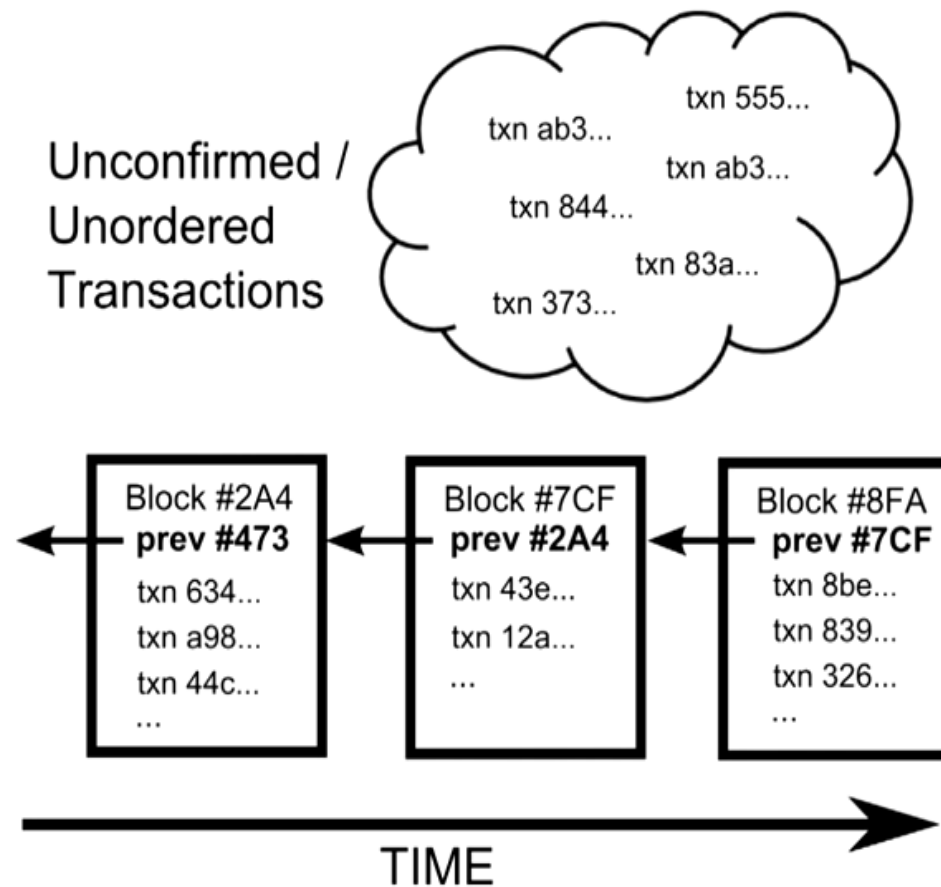
Transaction Chain: History of Ownership



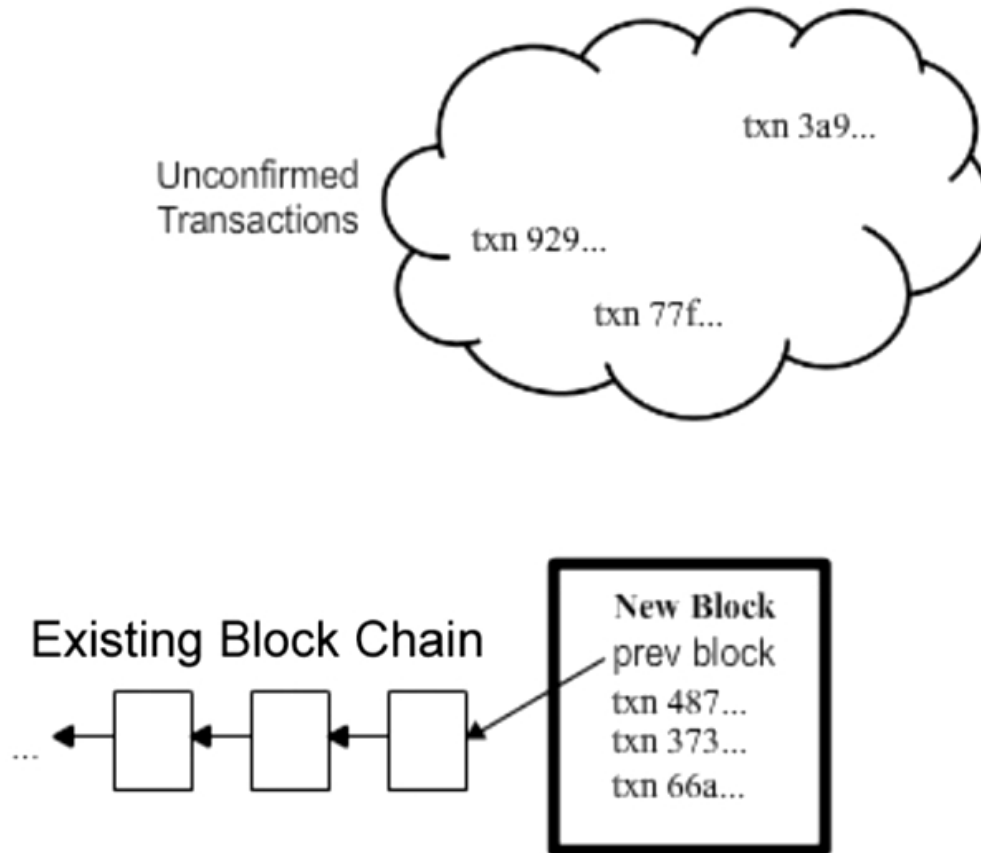
Block Chain: Transaction Ordering



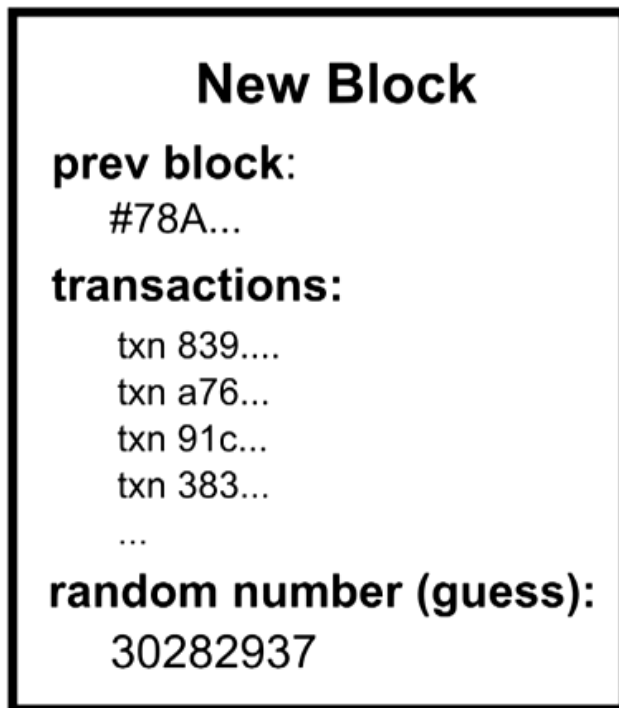
Ordering Solution: The Block Chain




Block Creation



Block Puzzle




$$f(\text{block}) < ? \text{target}$$

Cryptographic Hash (SHA256)

Cyrpto Hash Locks Blocks in Place

block contents		random guess (nonce)	hash result	?	target
prev block ID	transactions				

$$f(\text{\#78A...}, \text{tx\#839}, \text{tx\#a76,...}, \text{3001}) = 438... < 100...$$

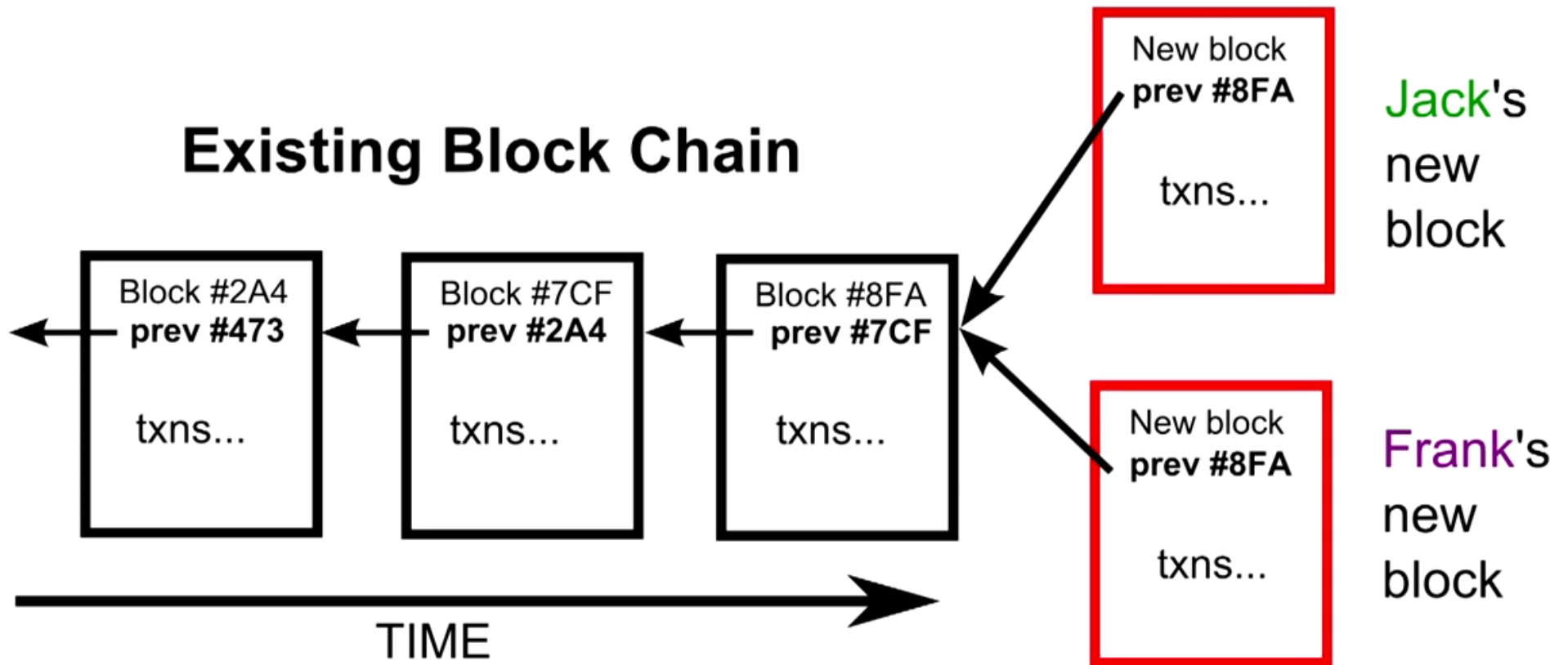
Cyrpto Hash Locks Blocks in Place

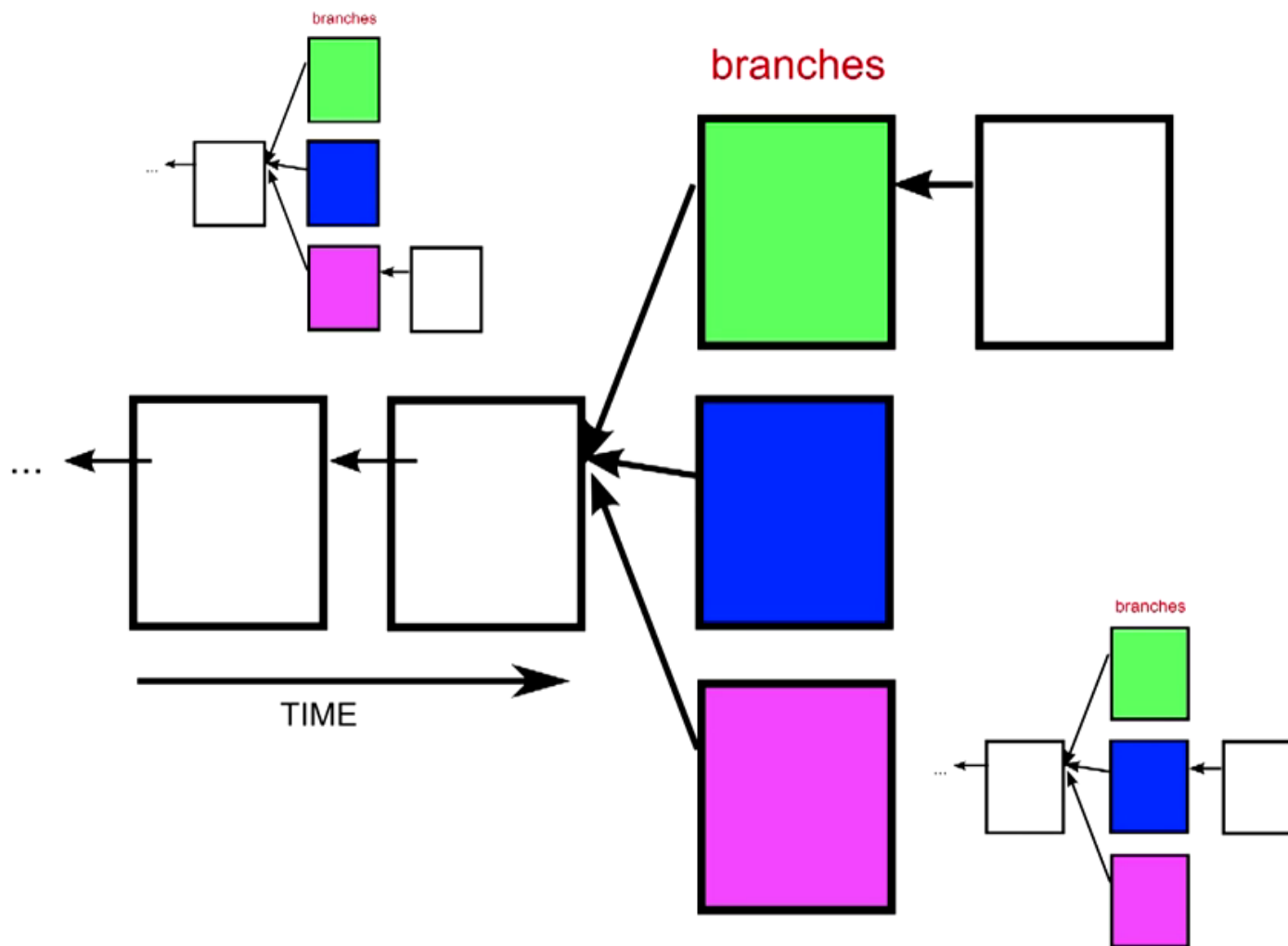
prev block ID		block contents transactions		random guess (nonce)	hash result	? target
f(#78A..., tx#839, tx#a76,...,				3001	= 438...	< 100...
f(#78A..., tx#839, tx#a76,...,				3002	= 988...	< 100...
f(#78A..., tx#839, tx#a76,...,				3003	= 587...	< 100...
f(#78A..., tx#839, tx#a76,...,				3004	= 087...	< 100...



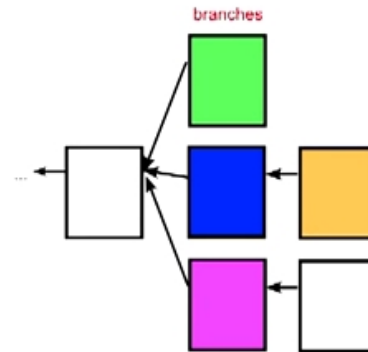
potential next blocks

Existing Block Chain

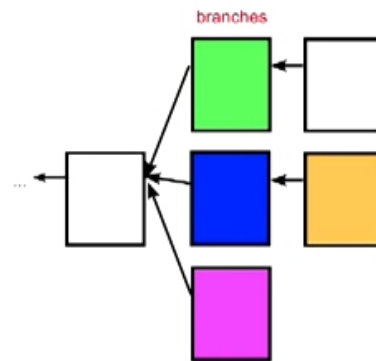




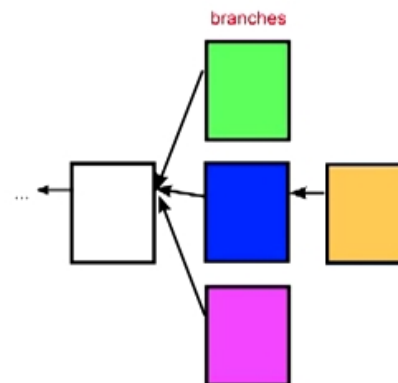
Travis's Block Chain



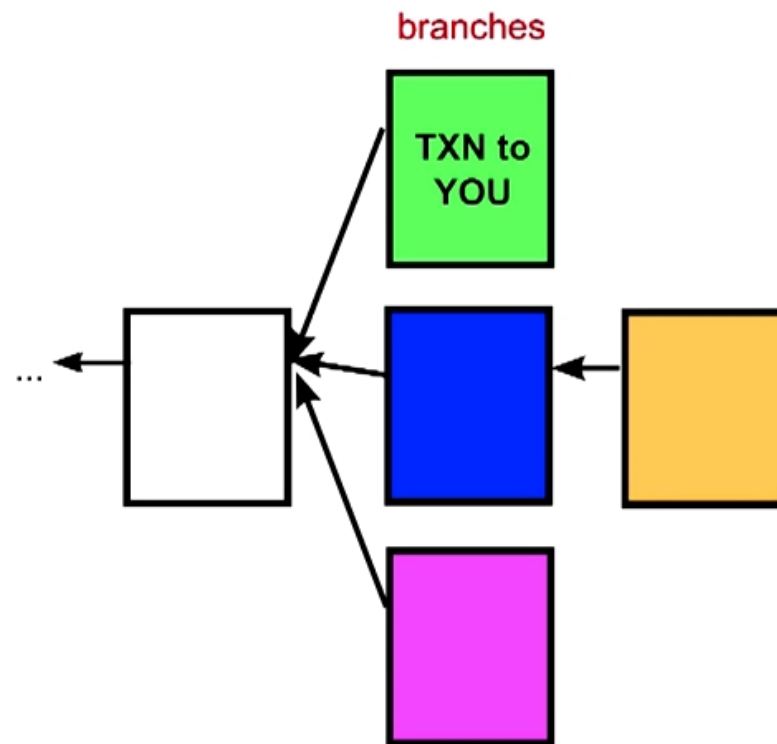
Your Block Chain



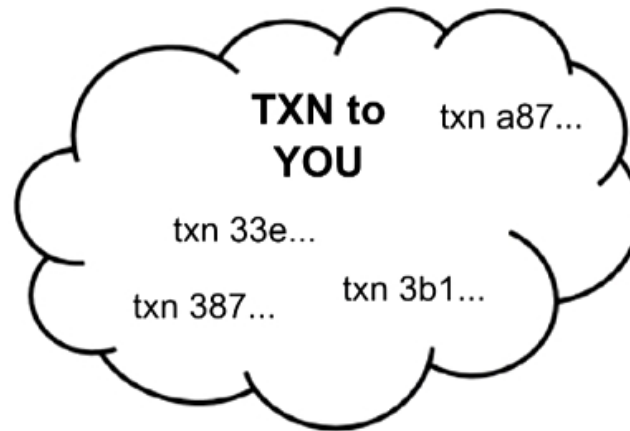
Carol's Block Chain



End of Chain Insecurity

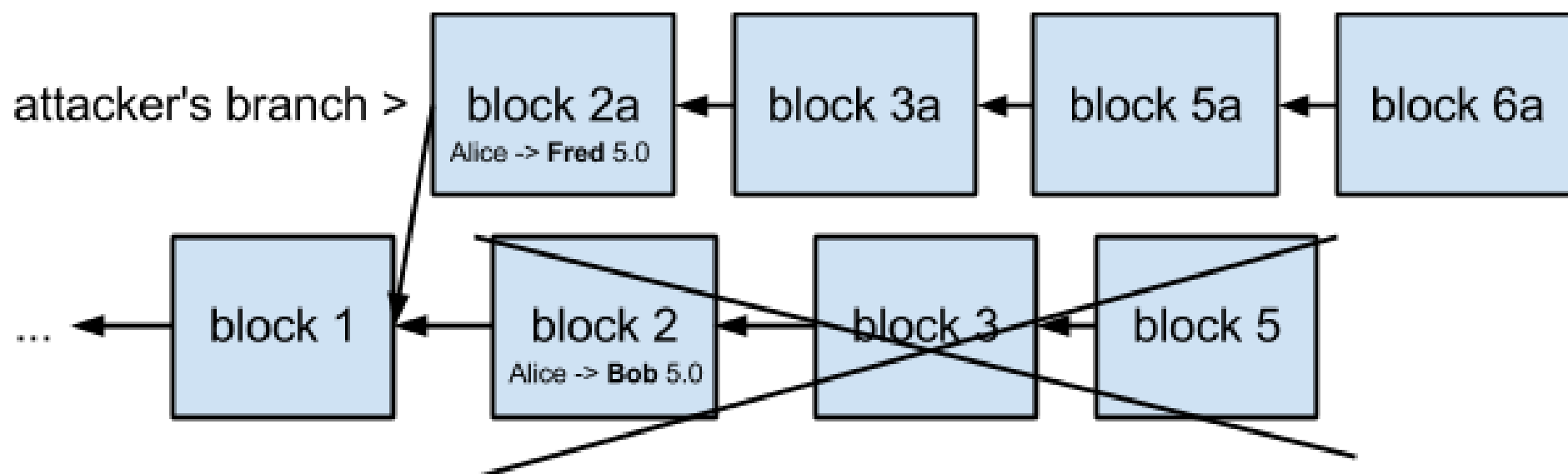


End of Chain Insecurity



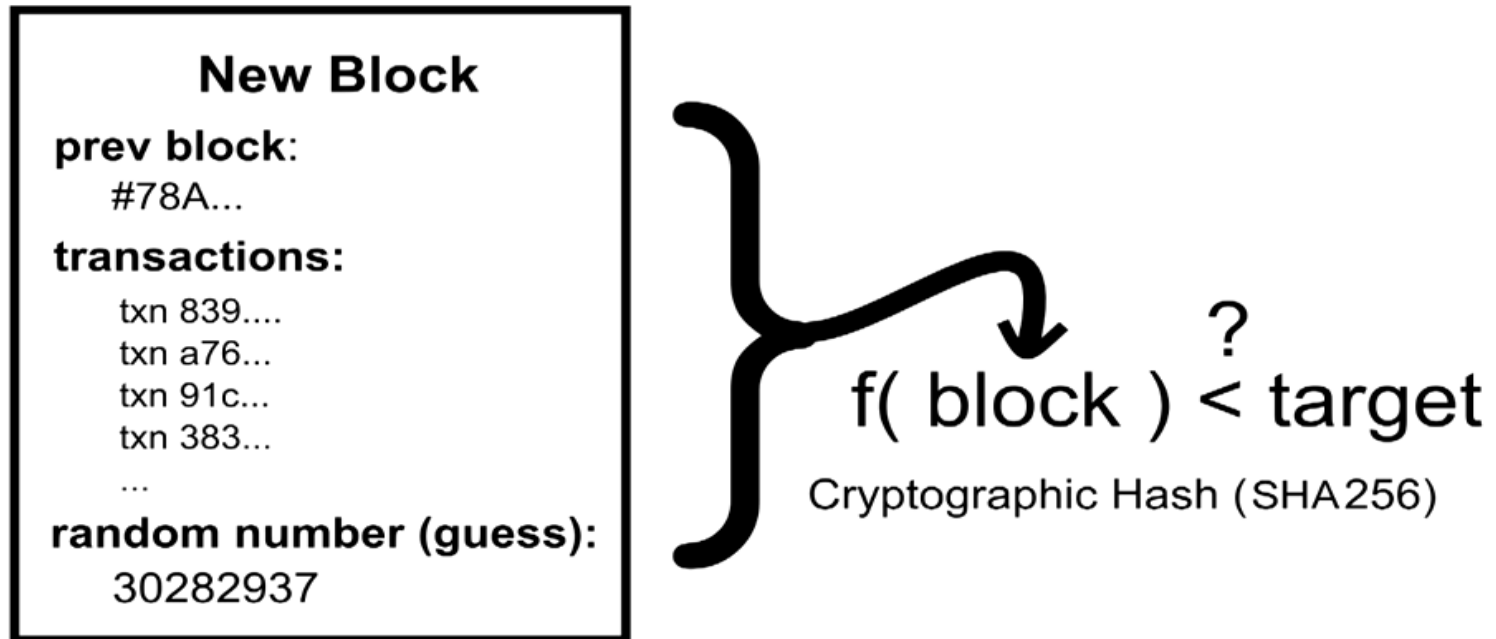
Unconfirmed / Unordered Transactions

Double spend attack



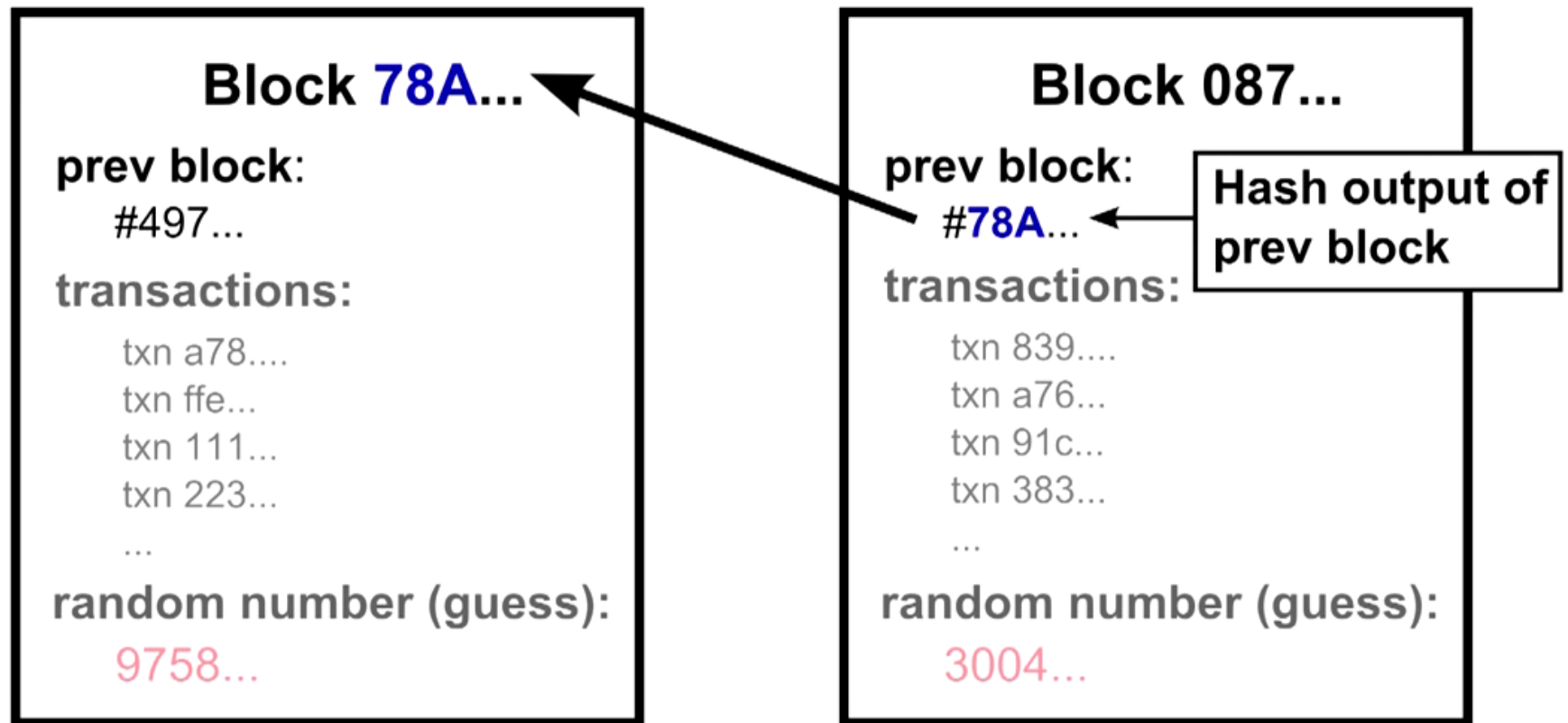
Double spend attack

Cyrpto Hash Locks Blocks in Place

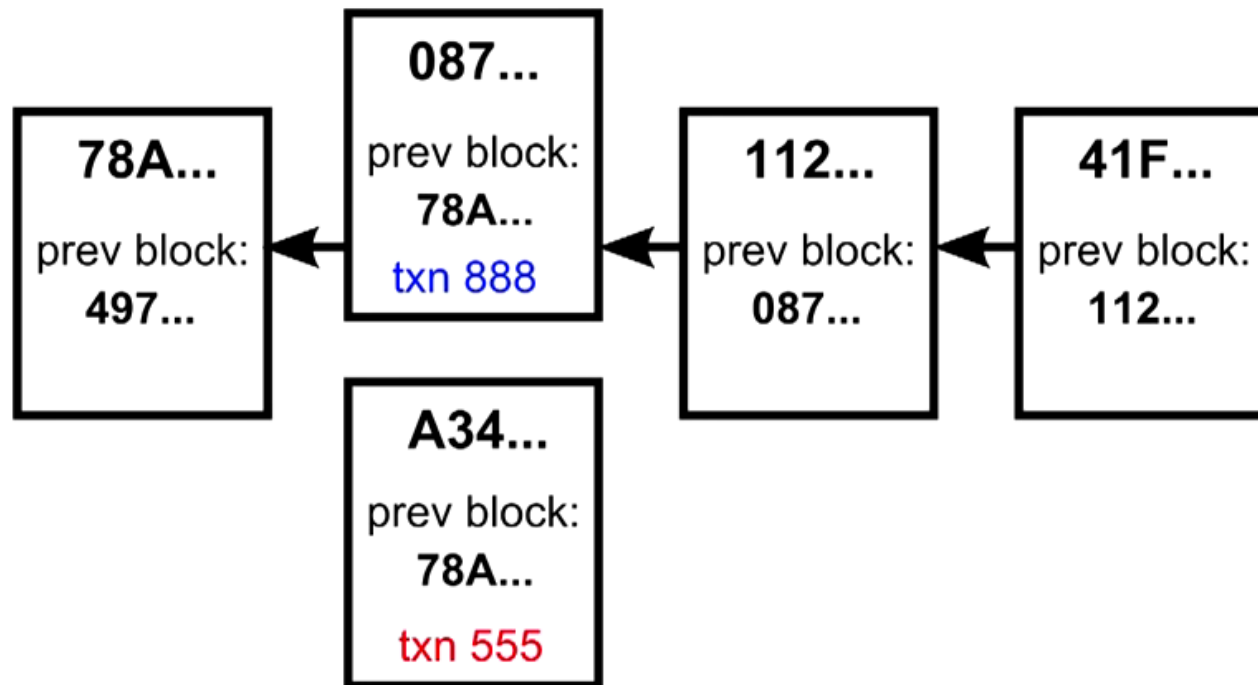


Double spend attack

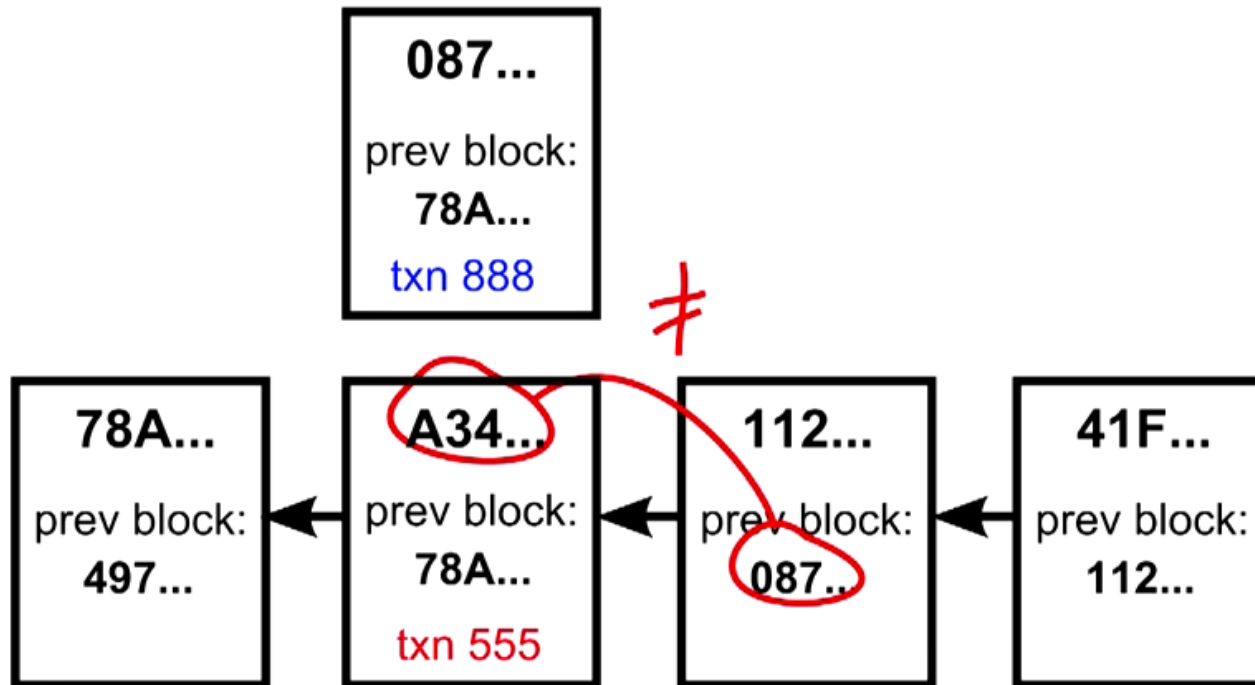
Hash outputs = Block IDs



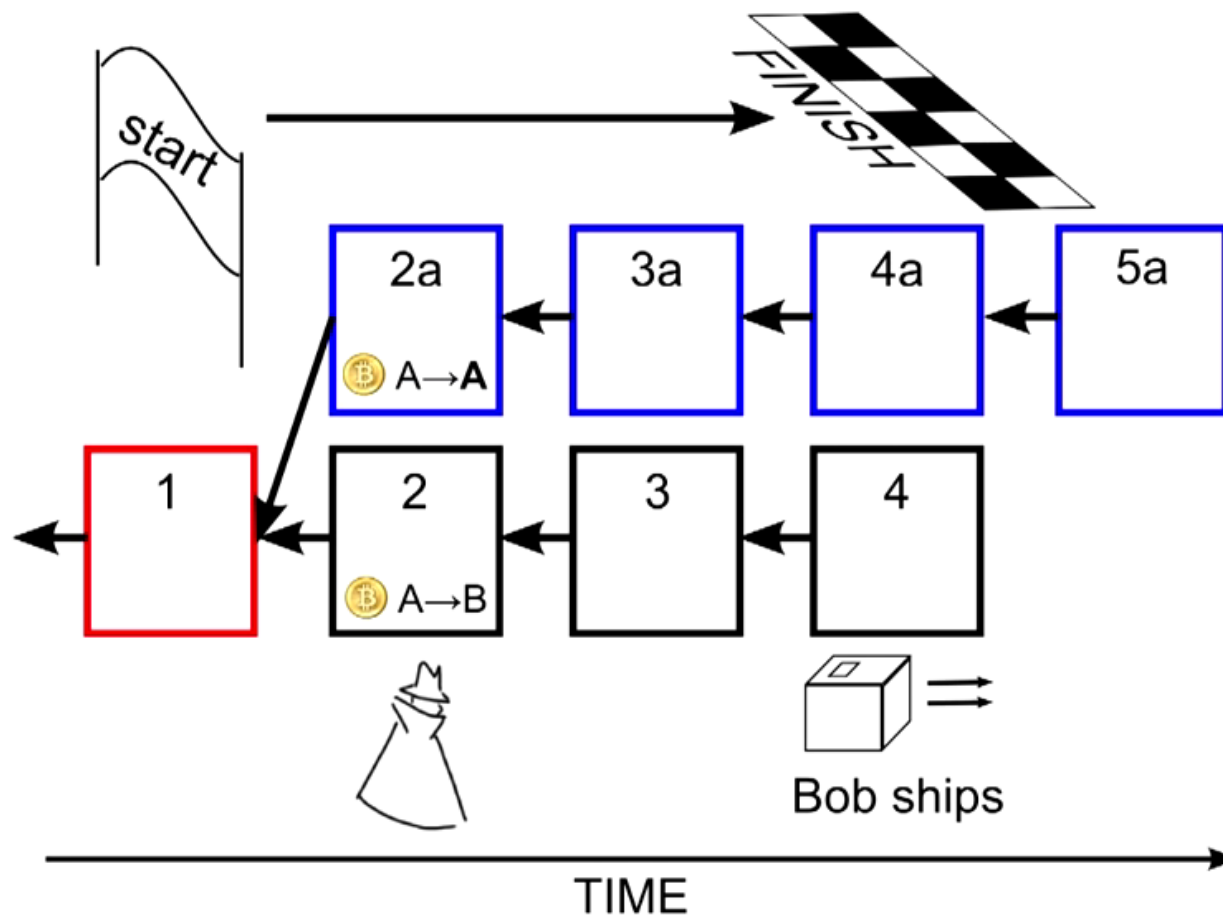
Double spend attack



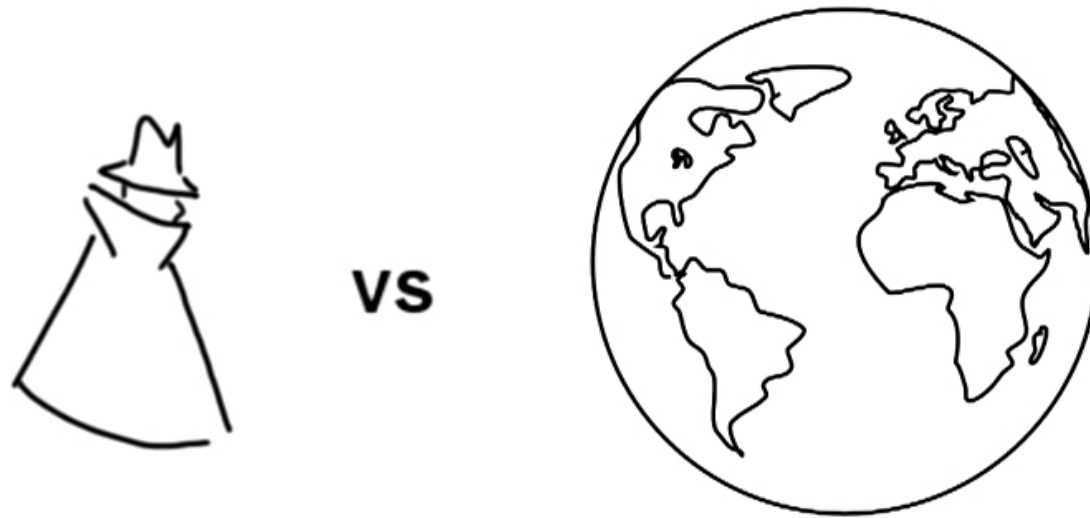
Double spend attack



Double spend attack

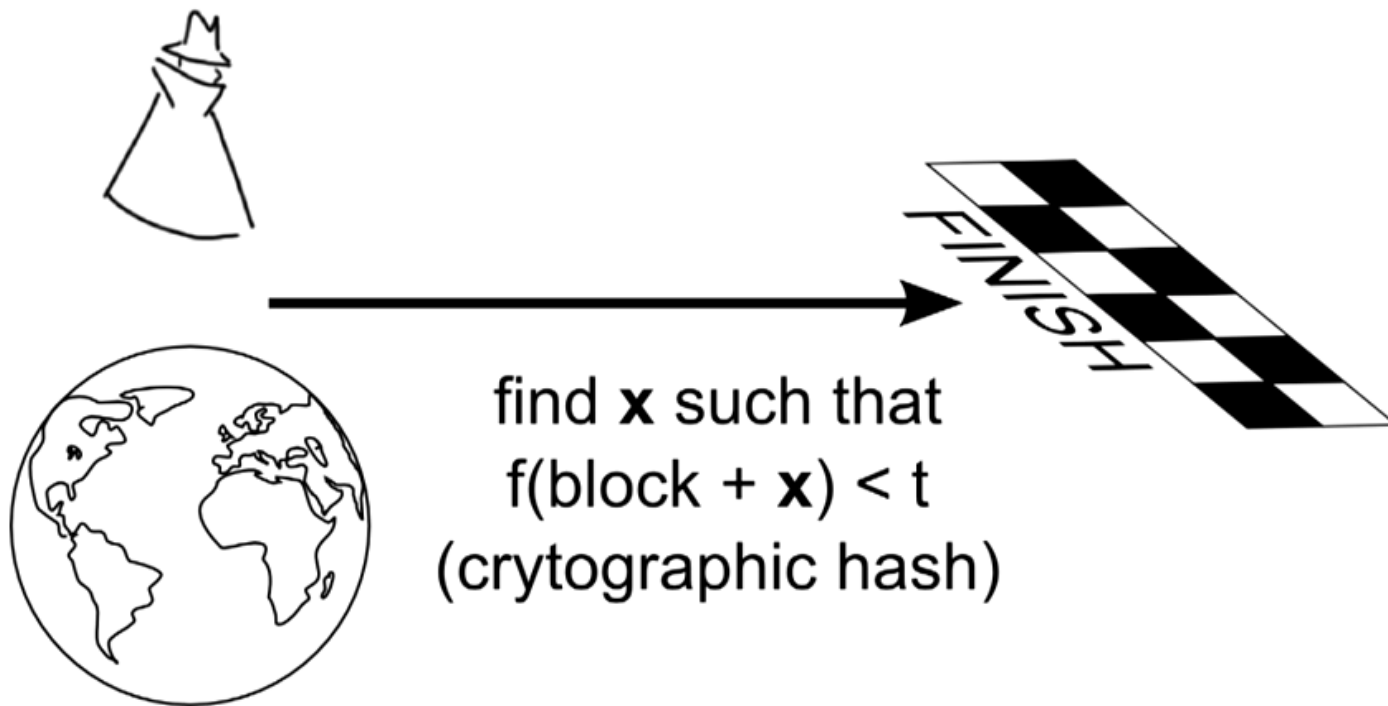


Double spend attack

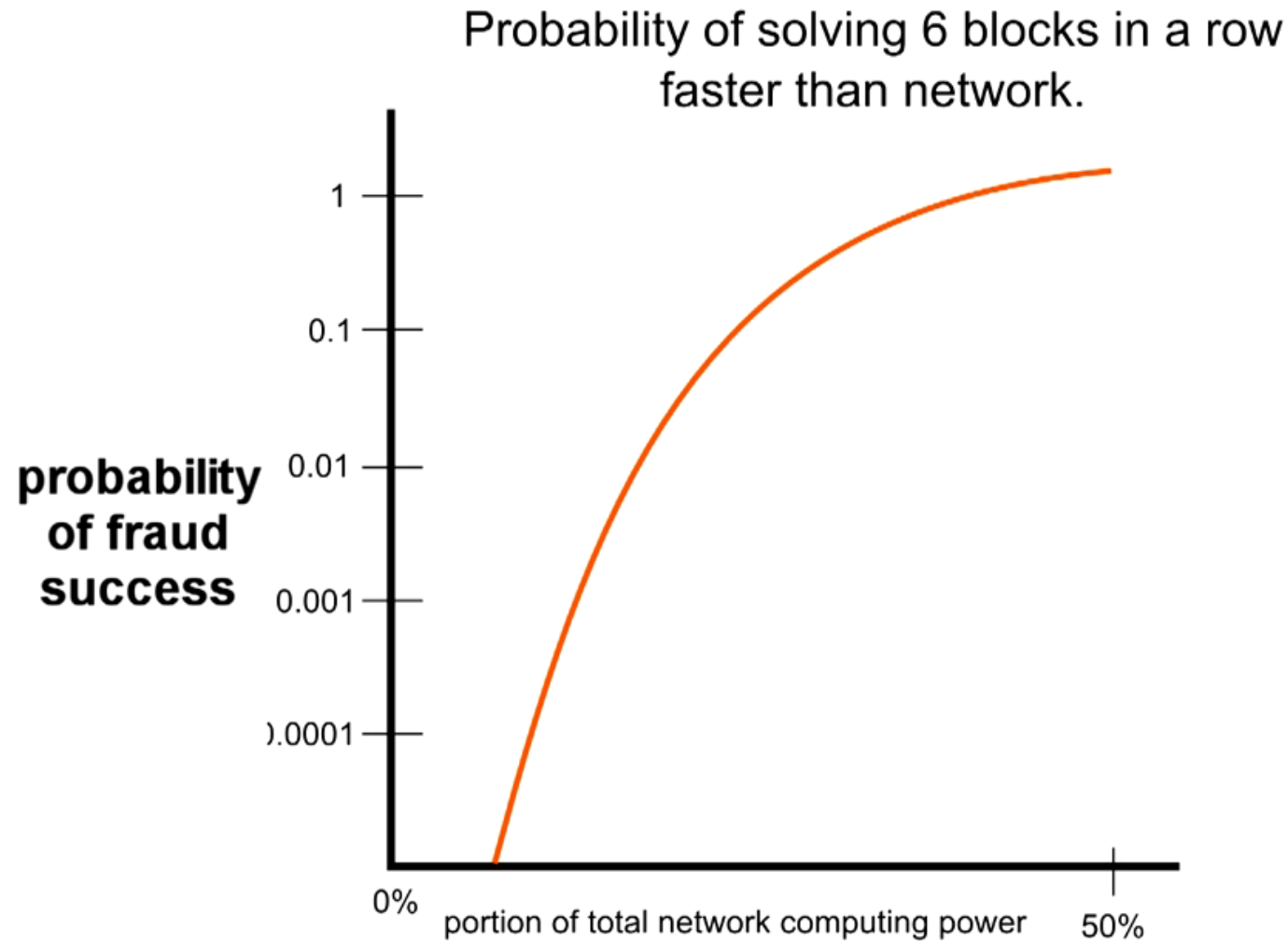


Double spend attack

Transaction Order protected by Race

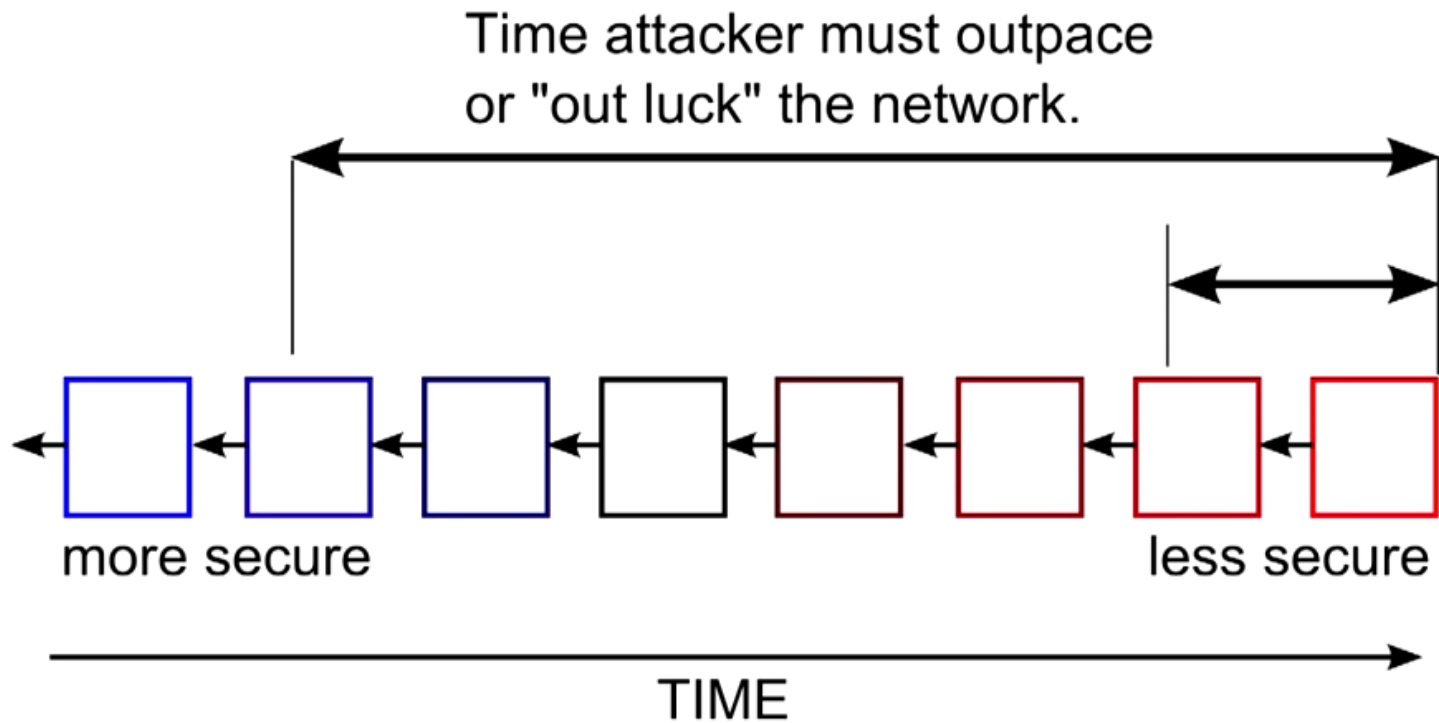


Double spend attack



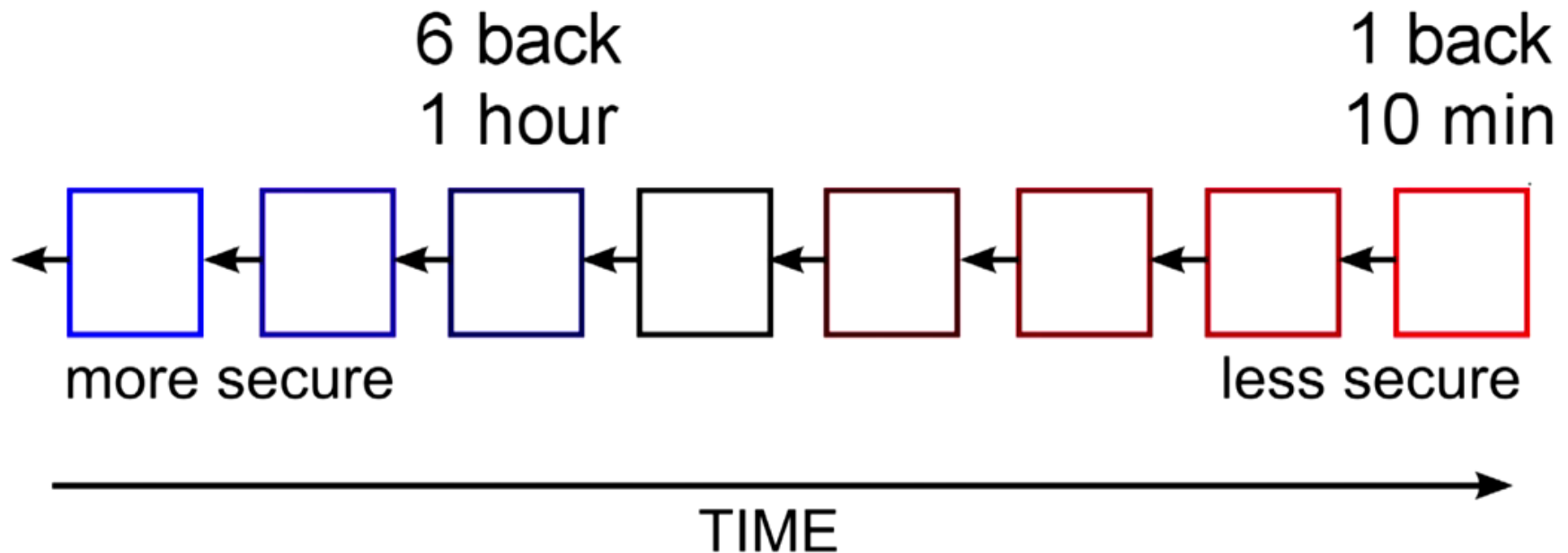
source: Analysis of hashrate-based double-spending, M. Rosenfeld

Double spend attack



Double spend attack

How long does it take to send money?

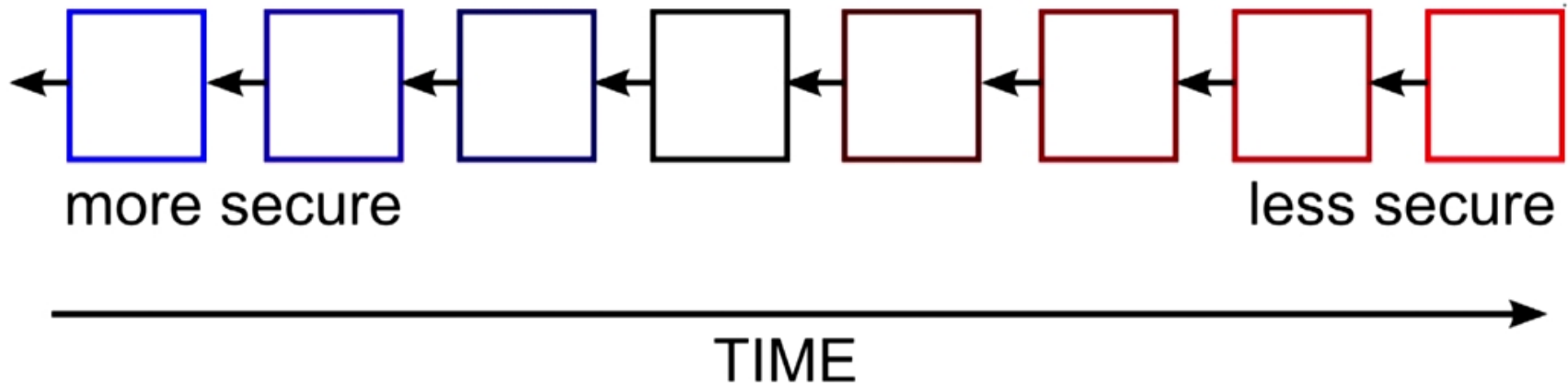


Double spend attack

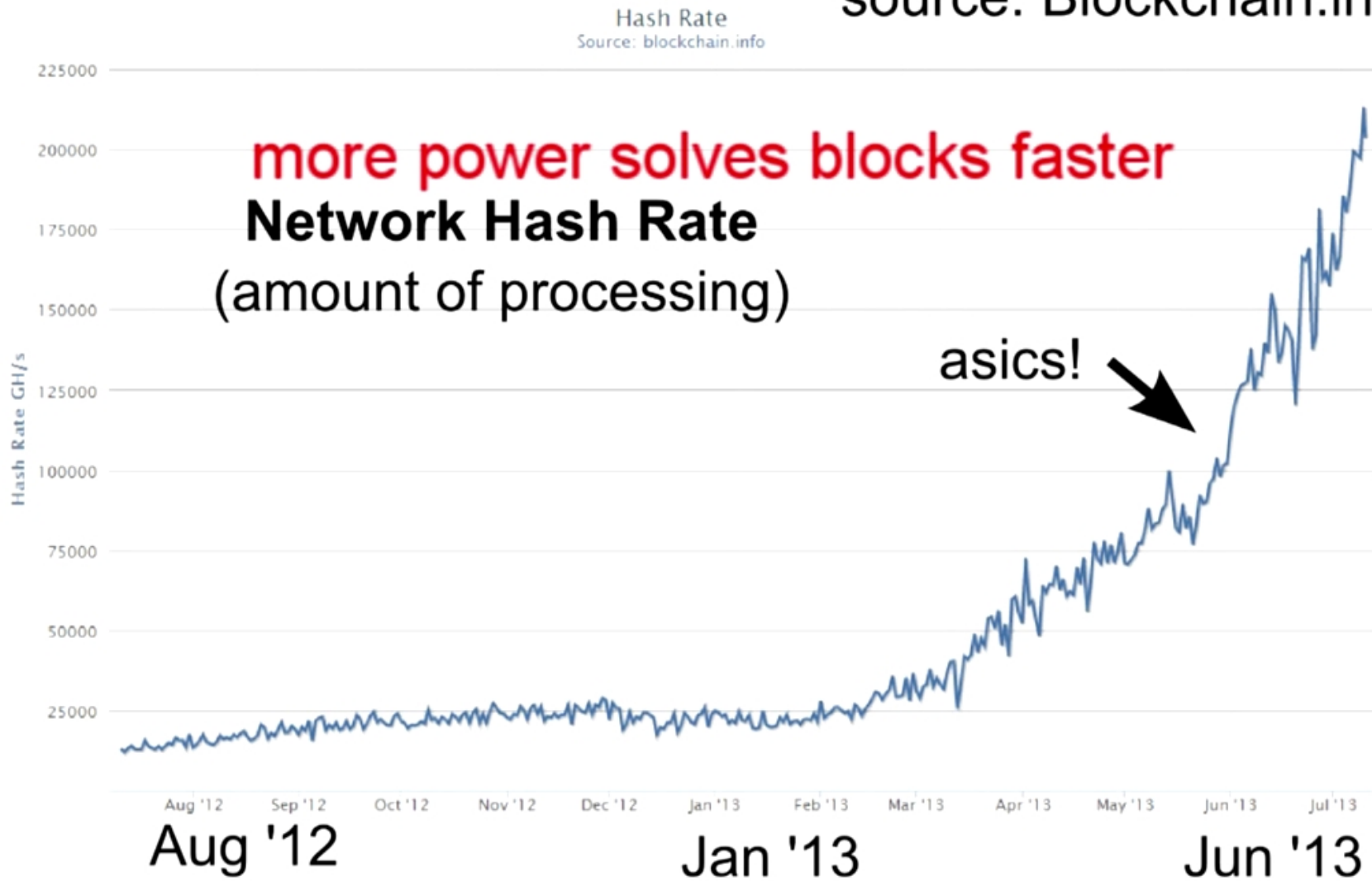
How long does it take to send money?

6 blocks back
(6 confirmations) = 1 hour

credit cards: seconds or months?



source: Blockchain.info



New Block

prev block:

#78A...

transactions:

txn 839....

txn a76...

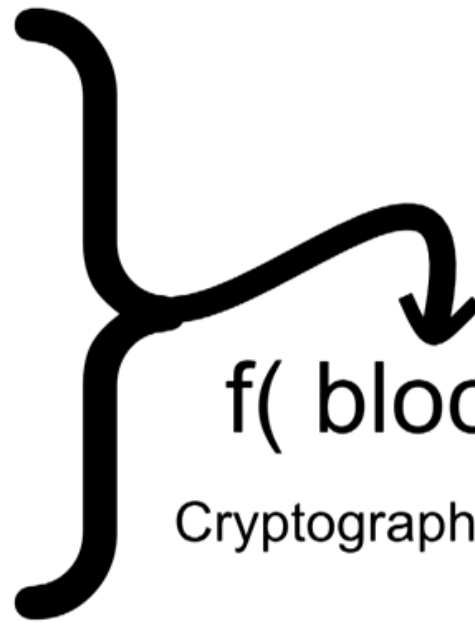
txn 91c...

txn 383...

...

random number (guess):

30282937



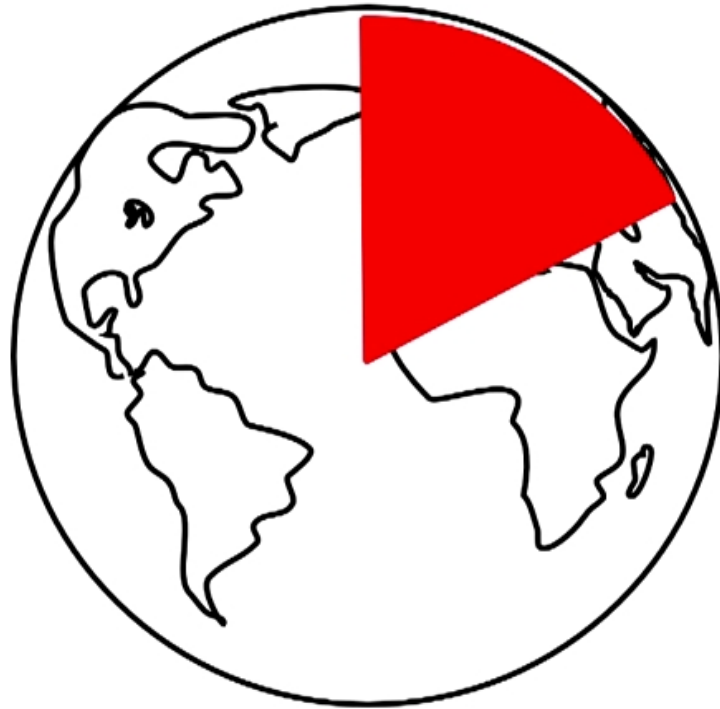
Target changed
to make solution
search harder or
easier.



$$f(\text{block}) < \text{target}$$

Cryptographic Hash (SHA256)

Mining Pools



Mining pools

- “BTC Guild” has solved 6 blocks in a row by itself

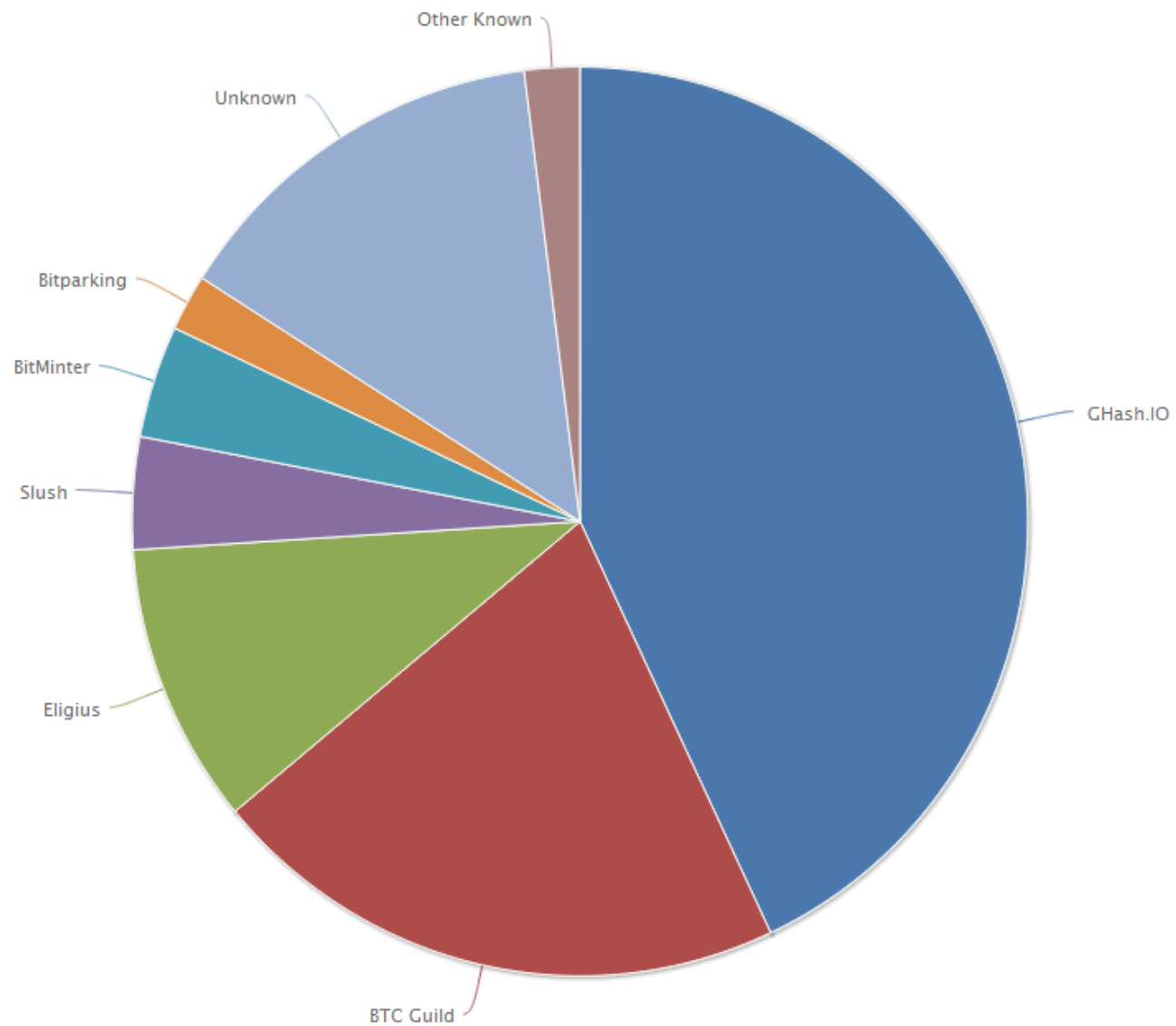
Mining pools

- “BTC Guild” has solved 6 blocks in a row by itself
- Asked members to leave to secure the network

Mining pools

- “BTC Guild” has solved 6 blocks in a row by itself
- Asked members to leave to secure the network
- Ghash.io, “yesterday's problem”

Mining pools















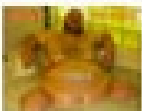



Mining pools

Home Most recently mined blocks in the bitcoin block chain

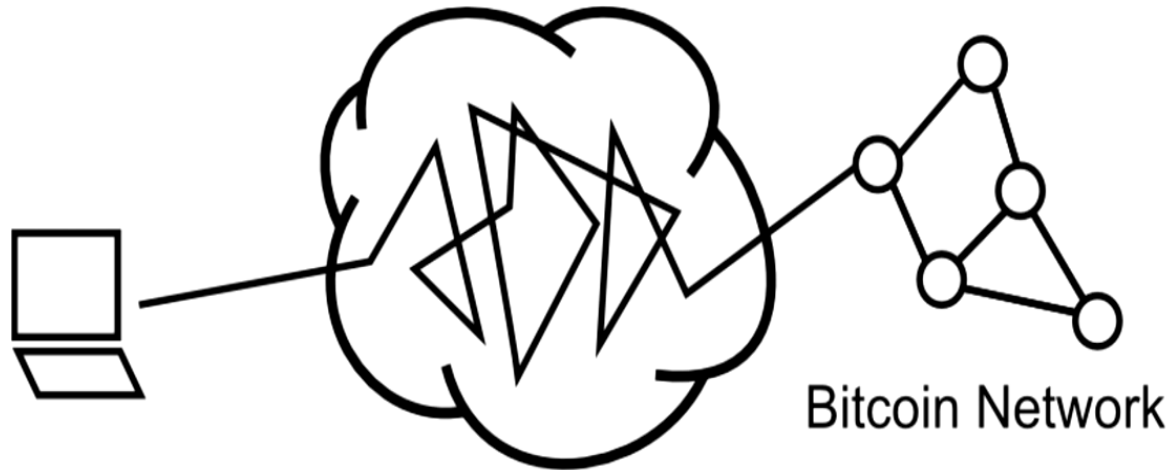
Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
279471	4 minutes	183	1,011.61797486 BTC	GHash.IO	75
279470	9 minutes	146	644.64531494 BTC	GHash.IO	51
279469	13 minutes	127	467.81522678 BTC	GHash.IO	43
279468	16 minutes	238	1,829.21490817 BTC	GHash.IO	114
279467	20 minutes	90	1,481.81074603 BTC	89.168.54.95	31
279466	25 minutes	160	9,314.35639766 BTC	GHash.IO	104
279465	28 minutes	618	7,121.30 BTC	GHash.IO	243.41

[More...](#)

Mining pools

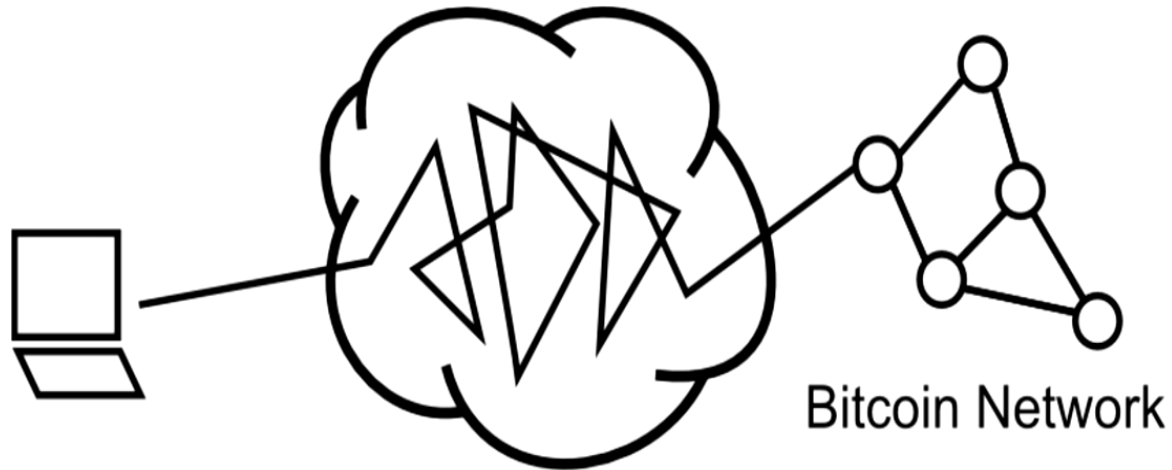
- ↑ 1088
↓
-  **WARNING: GHASH.IO IS NEARING 51% – LEAVE THE POOL** (cryptocoinsnews.com)
(1110|264) submitted 10 hours ago by awd2r4 
328 comments share save hide report [I+c]
- ↑ 356
↓
-  **Congratulations r/Bitcoin! You have created a decentralised discussion! (P.S. Ghash.io is EVIL)** (self.Bitcoin)
[Aa] (485|128) submitted 6 hours ago* (last edited 3 minutes ago) by gabblox 
61 comments (1 new) share save hide report [I=c]
- ↑ 465
↓
-  **LEAVE GHASH.IO** (self.Bitcoin)
[Aa] (599|195) submitted 8 hours ago by Chillyperiod 
60 comments share save hide report [I=c]
- ↑ 567
↓
-  **Bitcoin Miners, Step Away From GHash.IO !** (cryptoarticles.com)
(738|208) submitted 9 hours ago by jdebunt 
61 comments share save hide report [I+c]
- ↑ 221
↓
-  **FOR THE LOVE OF GOD CHANGE THE F***ING POOL IF YOU'RE ON GHASH.IO** (25.media.tumblr.com)
[Aa] (393|176) submitted 5 hours ago by Drollian 
19 comments share save hide report [I+c]
- ↑ 1009
↓
-  **GHash.IO At 42% Of Mined Blocks Over Past 24 Hours.** (blockchain.info)
(1307|303) submitted 13 hours ago by skillard4 
443 comments share save hide report [I+c]
- ↑ 404
↓
-  **WARNING: GHASH.IO IS NEARING 51% – LEAVE THE POOL (with image)** (imgur.com)
[Aa] (662|290) submitted 8 hours ago by robmon 
14 comments share save hide report [I+c]
- ↑ 130
↓
-  **The network health of Bitcoin is awful. The 2 largest pools comprise 60% of the network. All you need to do to take over the network is coerce 2 people. Please switch to P2Pools.** (blockchain.info)
(178|60) submitted 3 hours ago by lysobit 
62 comments share save hide report [I+c]

Anonymity



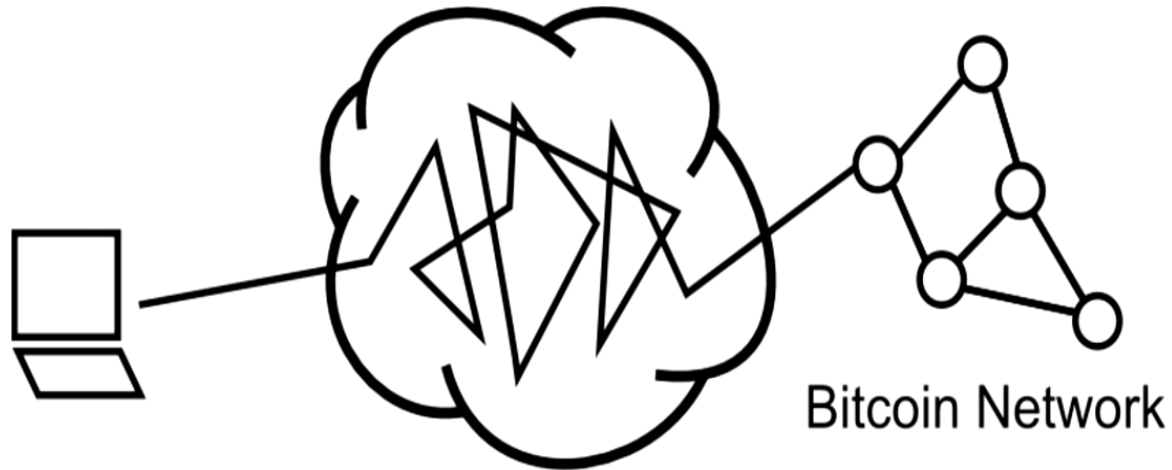
- Hide behind Tor or I2P

Anonymity



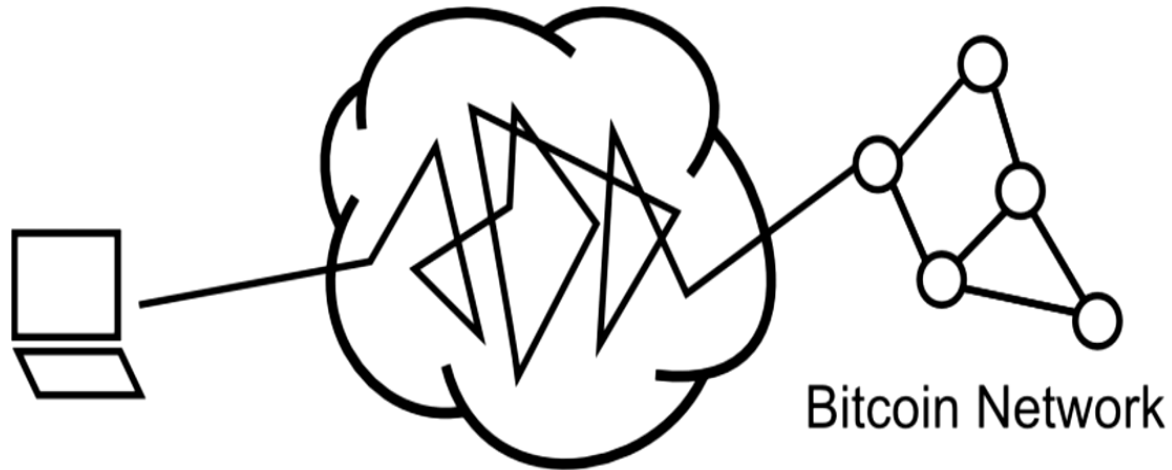
- Hide behind Tor or I2P
- Only reveal public address

Anonymity



- Hide behind Tor or I2P
- Only reveal public address
- Generate new for each income

Anonymity



- Hide behind Tor or I2P
- Only reveal public address
- Generate new for each income
- Still get linked

Anonymity

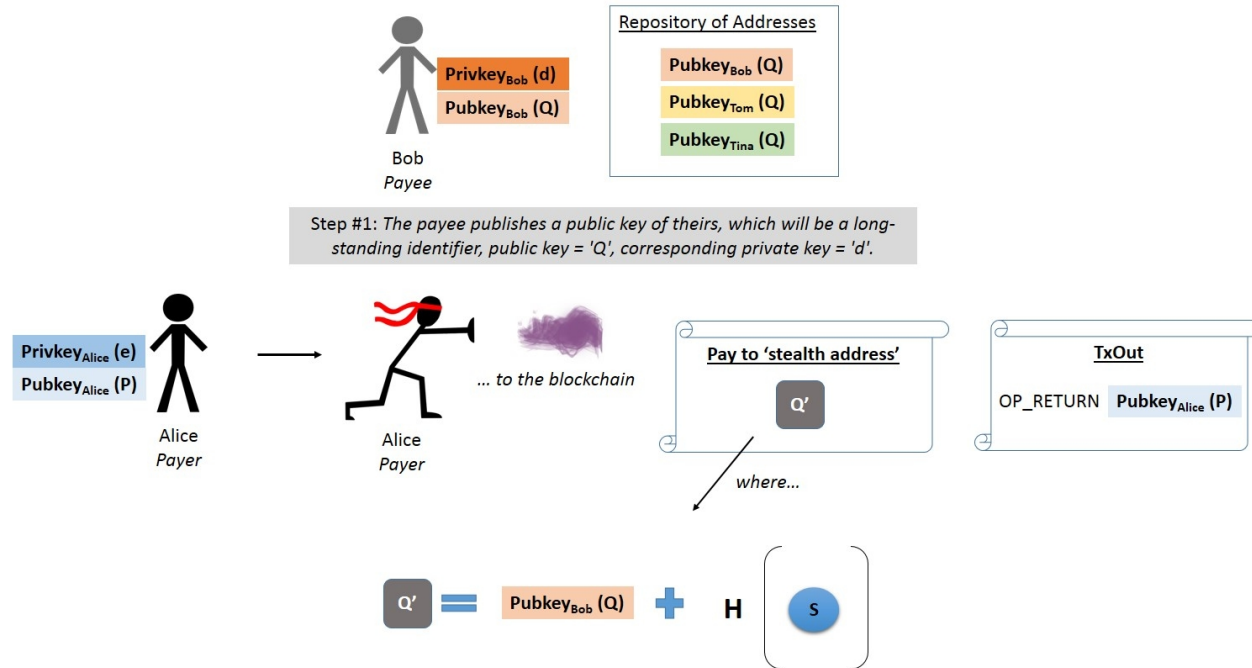
Inputs²

Previous output (index) ²	Amount ²	From address ²	Type ²	ScriptSig ²
eb38f77560ca...1	8	1P9SgqzjFWgWVAuZBFwimNPV7Luna/pgTj	Address	30450220078df7c48ed152bd40eae4a73afefc31044760639da2c0d6158484e1a4dab332fefe4bb8 ◀ <input type="text"/> ▶
b912994fca58...1	0.03	18Mk65wV1E5kCVHFSlvUTU6zt4yVFKM5Ft	Address	304502204e877fc5ca3783e165052e64c4788dd04769bbfc55cbd412784e024c8624f8c4f42d7cb ◀ <input type="text"/> ▶
58379d94fe85...15	1	1G4hfmM2ufAPEECdawg5gvUTBB2PvLr2	Address	3044022075d23fd4a8004866777210f51f46c96046dd45b37fe3ff3f1563458cfbd7f922d1b4a ◀ <input type="text"/> ▶
fc9d1cd1c2ac...1	130	1LpQVnJSMggqibQBGZwbobdX2Ghn9YWYc7	Address	3046022100a65a188b89a4e5ae2eaa5ba38750304ba81a1a538c5dd7e0c76884497ab522456b9 ◀ <input type="text"/> ▶
7b6f7d4a521c...1	0.5535726	16Kb6XppHLbjgmYQDpRyxz9jNE9Az5Xvcb	Address	3045022100eeb76e61abe62d38fd462eafdd1d1104f4fa1d3e26f3e7058038871a31b8bf63fd127f6 ◀ <input type="text"/> ▶
544097a30e09...0	0.0327060	1JnsDxlg6c757z8AnJUemj46YQgCTw54QN	Address	3045022100859df2ced47493e86a849cce1061504de257fe6490bd16188be6d06ca7b34816fa4b ◀ <input type="text"/> ▶

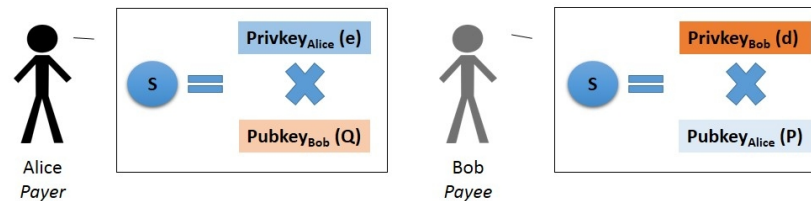
Outputs²

Index ²	Redeemed at input ²	Amount ²	To address ²	Type ²	ScriptPubKey ²
0	5baaca27d158...	0.01071174	1F7BgzQbyWTWzEMUKNzzLdjbjaQT9K96m	Address	OP_DUP OP_HASH160 9abd2e0c0a63dea36b75c3128fe15d82f274e394 OP_EQUALVERIFY OP_CHECKSIG ◀ <input type="text"/> ▶
1	1bb973b4ccc8...	139.605567	1NT2zFMa11NiCZydt4kqgXRZPF3iS6ZPGZ	Address	OP_DUP OP_HASH160 eb471d7a903e538cb94c1f2faf20eaadad8479af OP_EQUALVERIFY OP_CHECKSIG

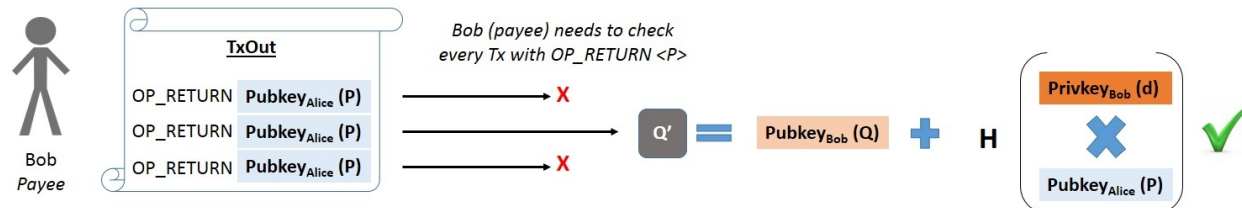
How Stealth Addresses Work



Step #2: To pay them, payer generates a keypair, private key = 'e' public key of 'P'. Publish 'P' in the transaction.

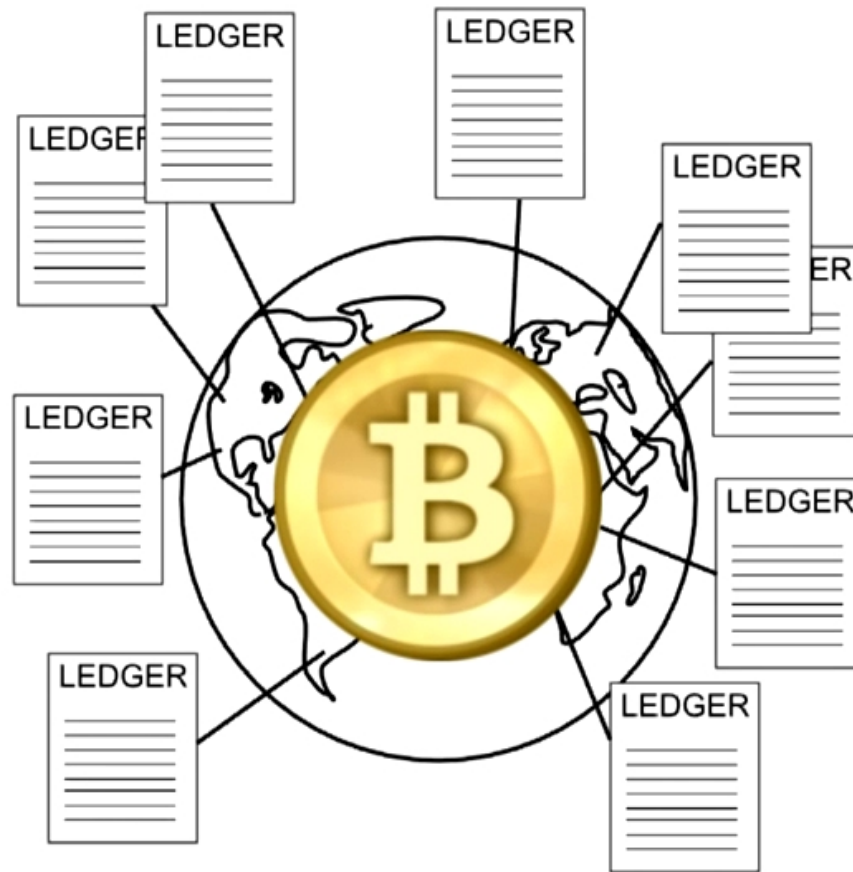


Step #3: The payer can calculate $S = eQ$, where S is a shared secret between payer/payee. The payee calculates the same S as $S = dP$. So the payee sees 'P' in a transaction, and multiplies by their private key, to get S .



Step #4: Now that we have the shared secret, either side can calculate an offset to Q which becomes the pay-to-address. A payee has to check each transaction (or every transaction of a fixed prefix) with 'P', calculate $Q' = Q + H(dP)$ and see if that transaction pays to Q' . If the address matches, then the payee can spend it with private key of $d + H(dP)$.

Summary



Summary

- Digital signatures
 - protects money
- Transaction chains
 - store history of ownership
- Block chain
 - hold transaction order

Benefits?

- Government can't print, or manipulate currency

Benefits?

- Government can't print, or manipulate currency
- “Anonymity”

Benefits?

- Government can't print, or manipulate currency
- “Anonymity”
- Lower fees than credit cards

References, and thanks to

- bitcointalk.org
- imponderablethings.com
- en.bitcoin.it
- coinchoose.com
- IRC (Freenode, #bitcoin-wizards, #bitcoin-dev)

- Bitcoin: 10 min, diff: 1,789,546,951.05320, SHA256, 14967.91 Th/sec
- PPCoin: 10 min, diff: 58,462,273.67400, SHA256, 82990.827 Gh/sec
- Litecoin: 2.5 min, diff: 3,931.59487, scrypt, 100.08 GH/sec
- Anoncoin 3 min, diff: 59.04968, scrypt, 1.39 GH/sec
- Franko: 0.5 min, diff: 1.38000, scrypt, 43.66 MH/sec

Difficulty is as of 15 Januar 2014.

Note: scrypt takes about ~10x time more than sha256

Technologies and keywords

- Base58 (Fonts, 0011, what is what)
- ECDSA (secp256k1)
- JSON (Control, RPC)
- Leveldb (key/value database, data storage)
- OpenSSL (for ECDSA, RPC SSL)
- Qt (for GUI in the original client)