THE BLOCKCHAIN

Hello!

We are:

Jakob Roberts

Cole McGinn

Carl Masri

We are here to speak to you about the blockchain technology, and how it is used.

Never trust a computer you can't throw out a window.

-Steve Wozniak

ASK QUESTIONS AT ANY TIME!

What is a Blockchain?

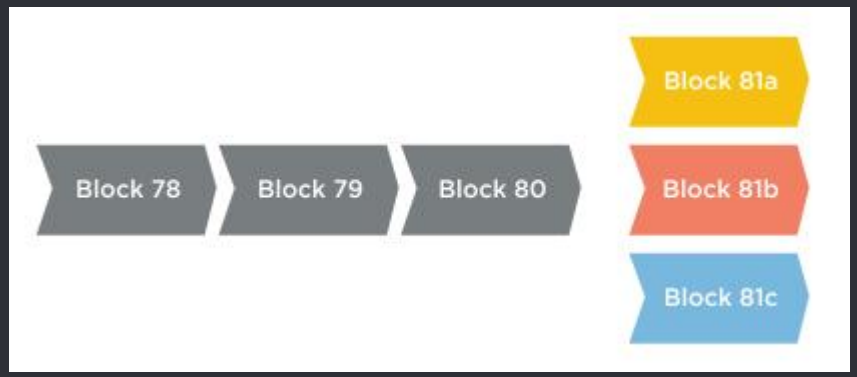
- The basics:
  - Ledger of facts
  - Facts grouped into blocks
  - Blocks joined into a chain
  - New blocks added by “miners”
  - Secured using computationally expensive math equation

Let's take an example:

BITCOIN

How does the Blockchain actually work?

- Every node gets the entire ledger
- Updates via “proof-of-work” consensus
- Node that solves the problem gets to propose the next block
- Simultaneous proposals? Go with the longest chain



Recollecting

Ledger

Bitcoin has a ledger of transactions of currency.

Immutable

When a transaction is made, it is set in stone.

Decentralization

There is no central bank for the money as all currency is kept track of on the ledger and all money is calculated from prior transactions.

Recollecting

Ledger

Bitcoin has a ledger of transactions of currency.

This also means you have everyone else's transaction records.

Immutable

When a transaction is made, it is set in stone.

Along with decentralization, there is no one to sue or go to if there is a problem!

Decentralization

There is no central bank for the money as all currency is kept track of on the ledger and all money is calculated from prior transactions.

No trust is needed!

Let's simplify things....

Alice will send 5 Bitcoins to Bob.

After the broadcast, all ledgers are updated to match.

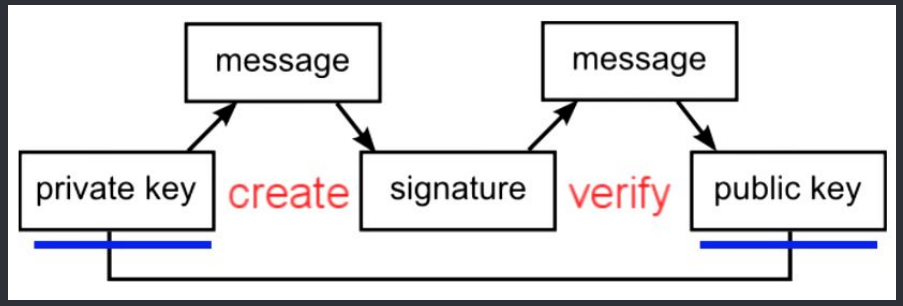
How do we know this is authentic?

Alice will need what is called a Digital Signature.

The Digital Signature

It is an alphanumeric identifier that represents a transaction

Unique signature per transaction.



Any signature changes invalidates the message/transaction sent!

Does the Ledger actually exist?

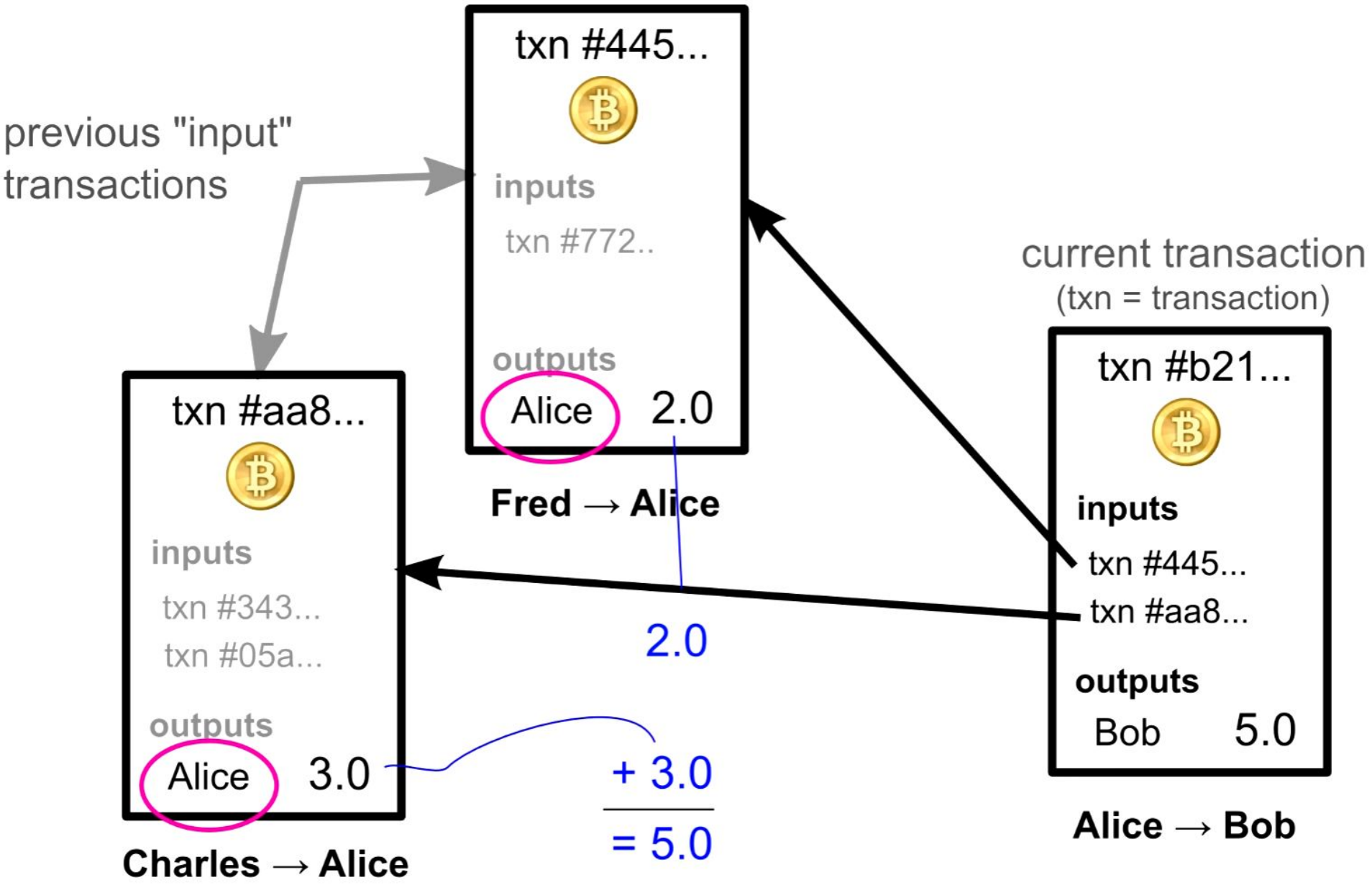
No

There is no list of current balances for all users kept inside the ledger.

….well kind of

There is however a list of all prior transactions that have not been nullified.

These transactions can then be scanned to find your balance!


previous "input" transactions
txn #445...
inputs
txn #772..
outputs
Alice 2.0
Fred → Alice
current transaction
(txn = transaction)
txn #b21...
inputs
txn #445...
txn #aa8...
outputs
Bob 5.0
Alice → Bob
txn #aa8...
inputs
txn #343...
txn #05a...
outputs
Alice 3.0
Charles → Alice
2.0
+ 3.0
= 5.0

Inputs

Previous output (index)	Amount	From address	Type	ScriptSig
eb38f77560ca...:1	8	1P9SgqzjFWgWVAuZBFwimNPV7LuuaJpgTj	Address	30450220078df7c48ed152bd40eaee4a73afefc31 044760639da2c0d6158484e1a4dab332fefc4bb8
b912994fca58...:1	0.03	18Mk65wV1E5kCVHFShvUTU6zt4yVFKM5Ft	Address	304502204e877fc5ca3783e165052e64c4788dd 04769bbfc55cbd412784e024c8624f8c4f42d7cb
58379d94fe85...:15	1	1G4hfnM2ufAPEECdawg5gtvUTBB2PxvLr2	Address	3044022075d23fd4a8004866777210f51f46c96 046dd45b37fe3ff33f1563458cfbdfb7f922d1b4a
fc9d1cd1c2ac...:1	130	1LpQVnJSMgqqibQBGZwbobdX2Ghn9YWyC7	Address	3046022100a65a188b89a4e5ae2eaa5ba387503 04ba81a1a538c5ddf7e0c76884497ab522456b9
7b6f7d4a521c...:1	0.55357267	16Kb6XppHUbjgmYQDpRyxz9jNE9Az5Xvcb	Address	3045022100eeb76e61abe62d38fd462eafd1d11f 04f4fa1d3e26f3e7058038871a31b8bf63fd127f6
544097a30e09...:0	0.03270607	1JnsDx1g6c757z8AnJUemj46YQgCTw54QN	Address	3045022100859df2ced47493e86a849cce10615 04de257fe6490bd16188be6d06ca7b34816fa4b

+

139.616

Outputs

Index	Redeemed at input	Amount	To address	Type	ScriptPubKey
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

Outputs

What happens to old transactions?

They are considered spent.

Spent transactions cannot be reused to prevent double spending.

Unspent transactions are kept in an index for quick access.

What makes bitcoin as a currency exceptionally special?

Anonymity

If you can hide your IP address such as through a service like TOR, you can make transactions completely anonymously.

….well kind of

Keep in mind that all your future transactions are linked in the ledger, this can make for some interesting data mining on habits.

Hold up!!!

Can’t someone just take my private key and use my account?

Within the set of 2^{256} private keys, they only map to 2^{160} unique wallet addresses. So the question is how does 2^{160} compare to 2.1e14?

1 in 6.9595 decillion

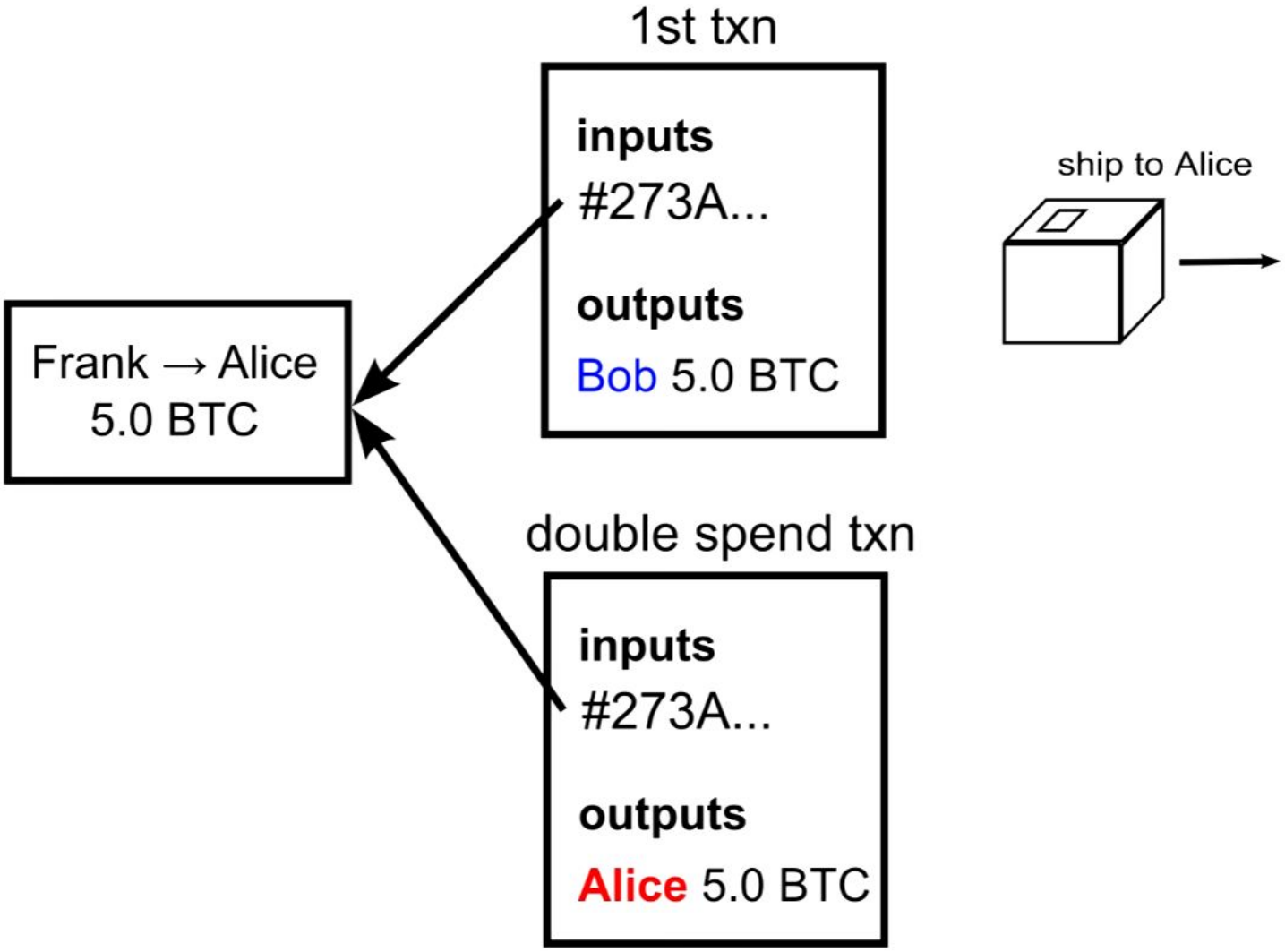
1 with 33 zeros

Number of possible bitcoin accounts

Problem: transaction order.

The order in which transactions were received may not match the order in which they were created and timestamps can’t be trusted.

Double Spending Fraud



Avoiding the double spend

If the second transaction hits first, Bob's payment would be invalidated.

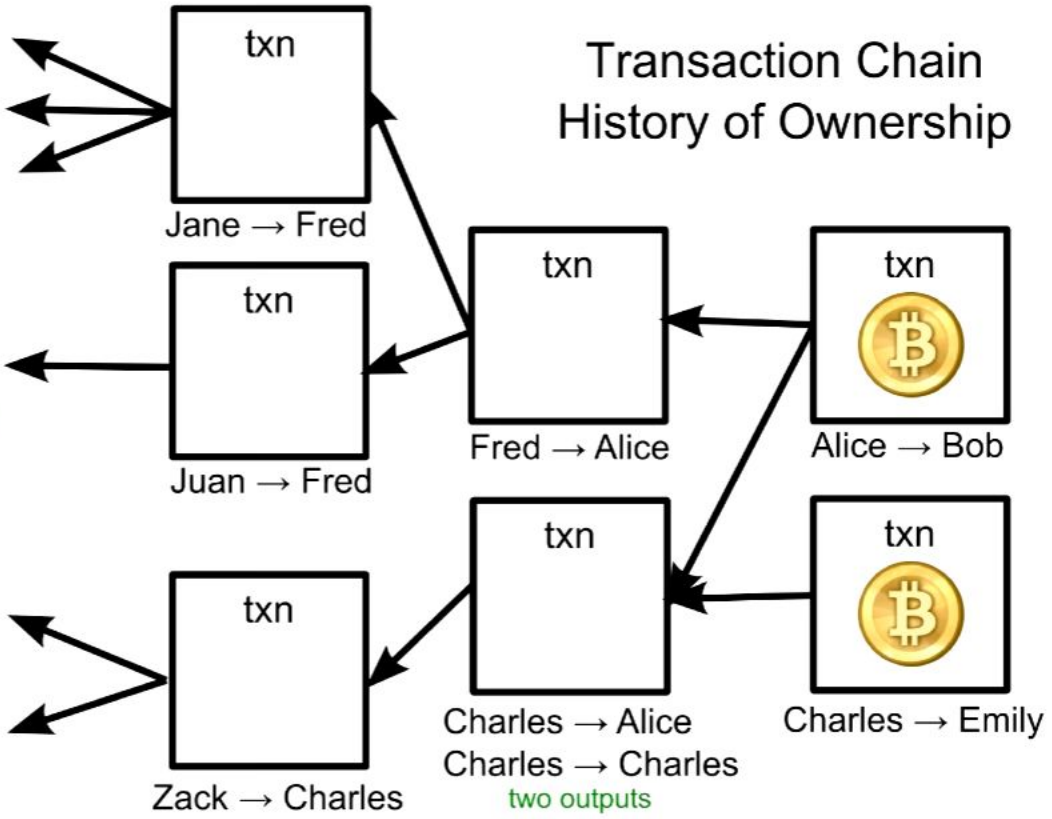
Bob would then be out of the product and his money.

How does the decentralized system agree on transaction order?

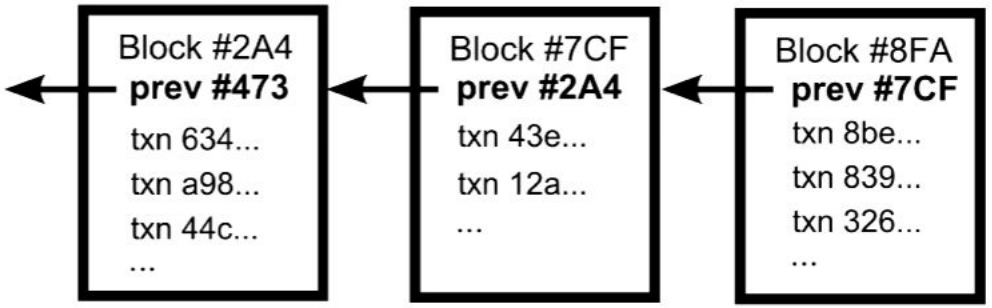
How does the decentralized system agree on transaction order?

The Blockchain!

Transaction Chain: History of Ownership



Block Chain: Transaction Ordering



Transaction ordering with the blockchain

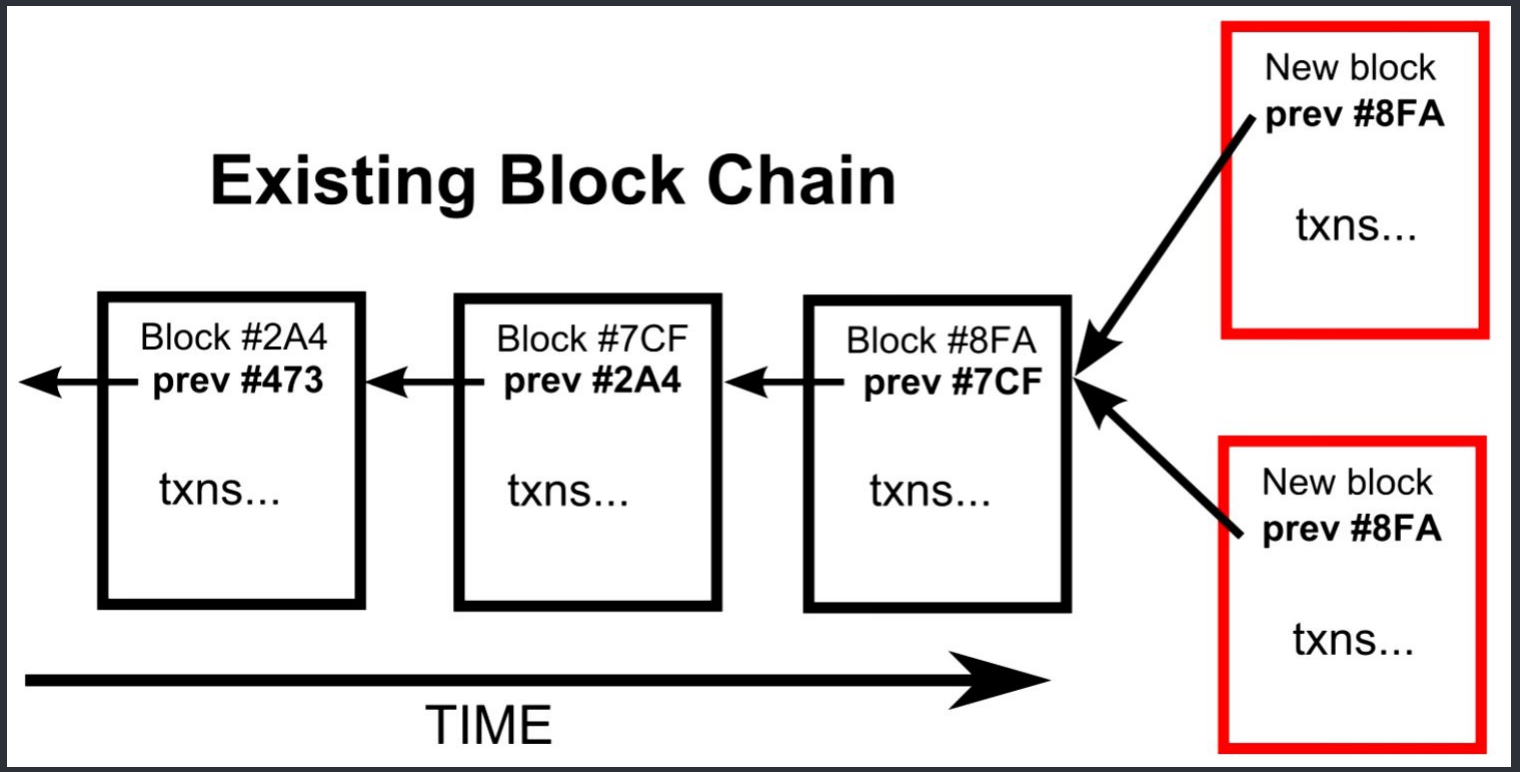
Each block references the previous block in time/the chain.

Each transaction in a block can be considered to have happened at the same time.

Transactions not in a block can be considered unconfirmed.

- Potential for multiple new blocks to be created?

- Two blocks can be created at the same time. Thankfully there is a solution....



Block Duplication

Each block that is created has its information run through a cryptographic hash (SHA256).

The output is completely unpredictable, so to discover it, guesses must be made to “unlock” the block. This takes about 10 minutes.

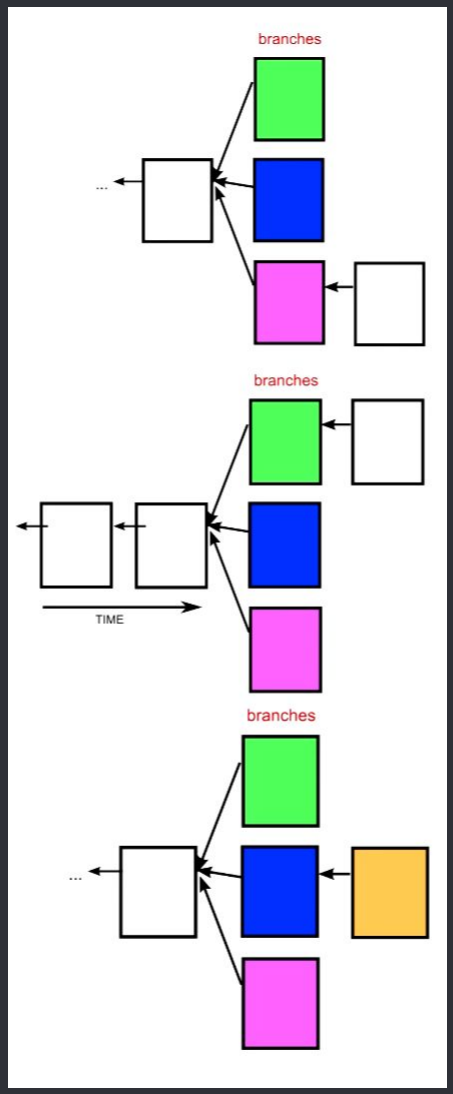
New Block

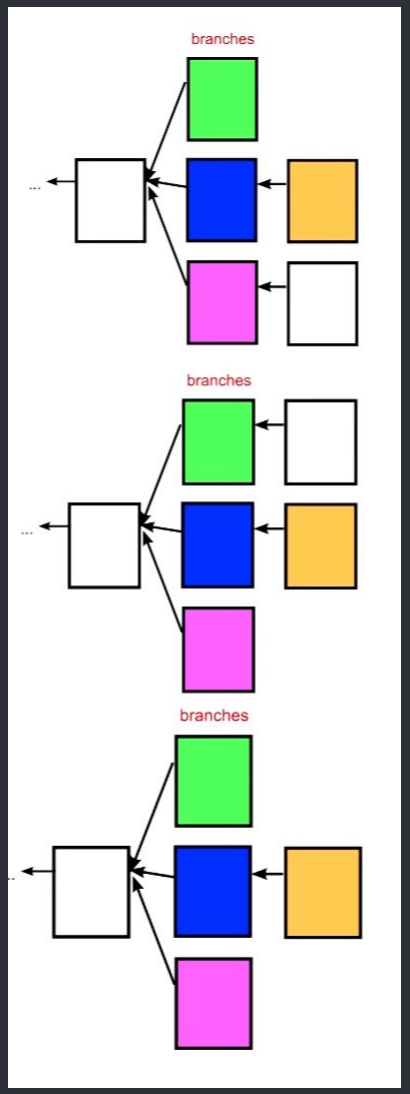
When a block is accepted into the chain, it is added into the chain.

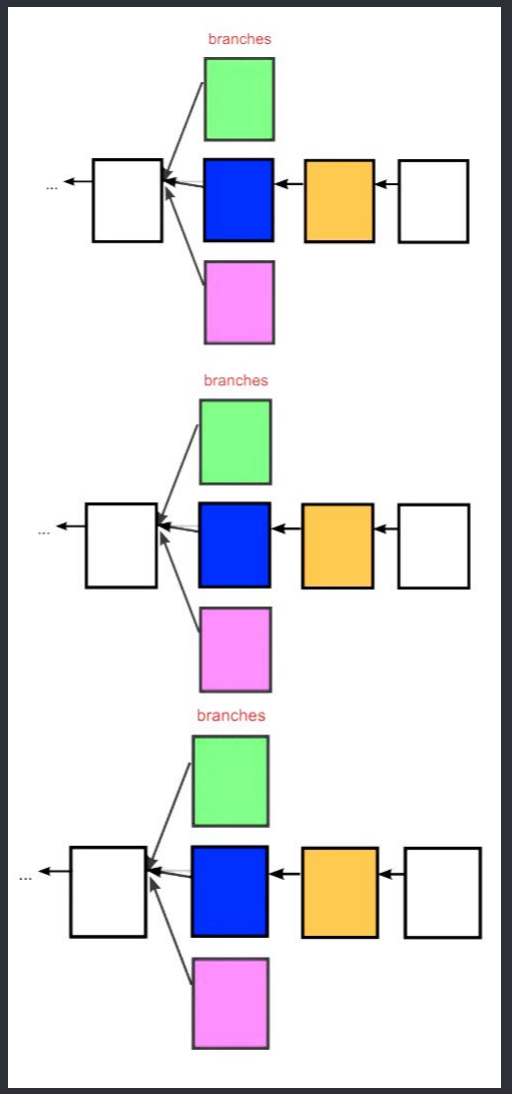
But...

What if two are solved at the same time?!

Blockchain Branches



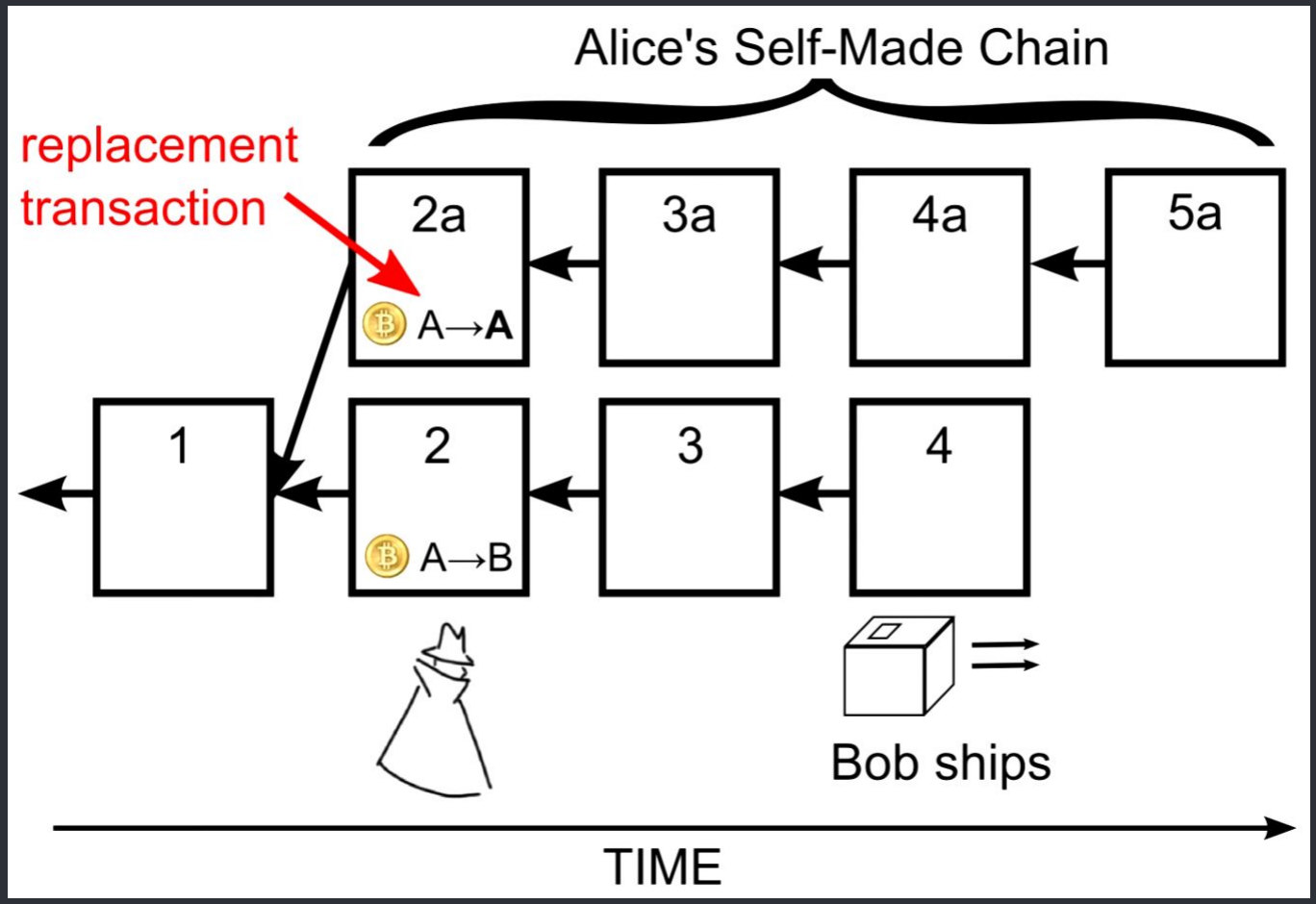




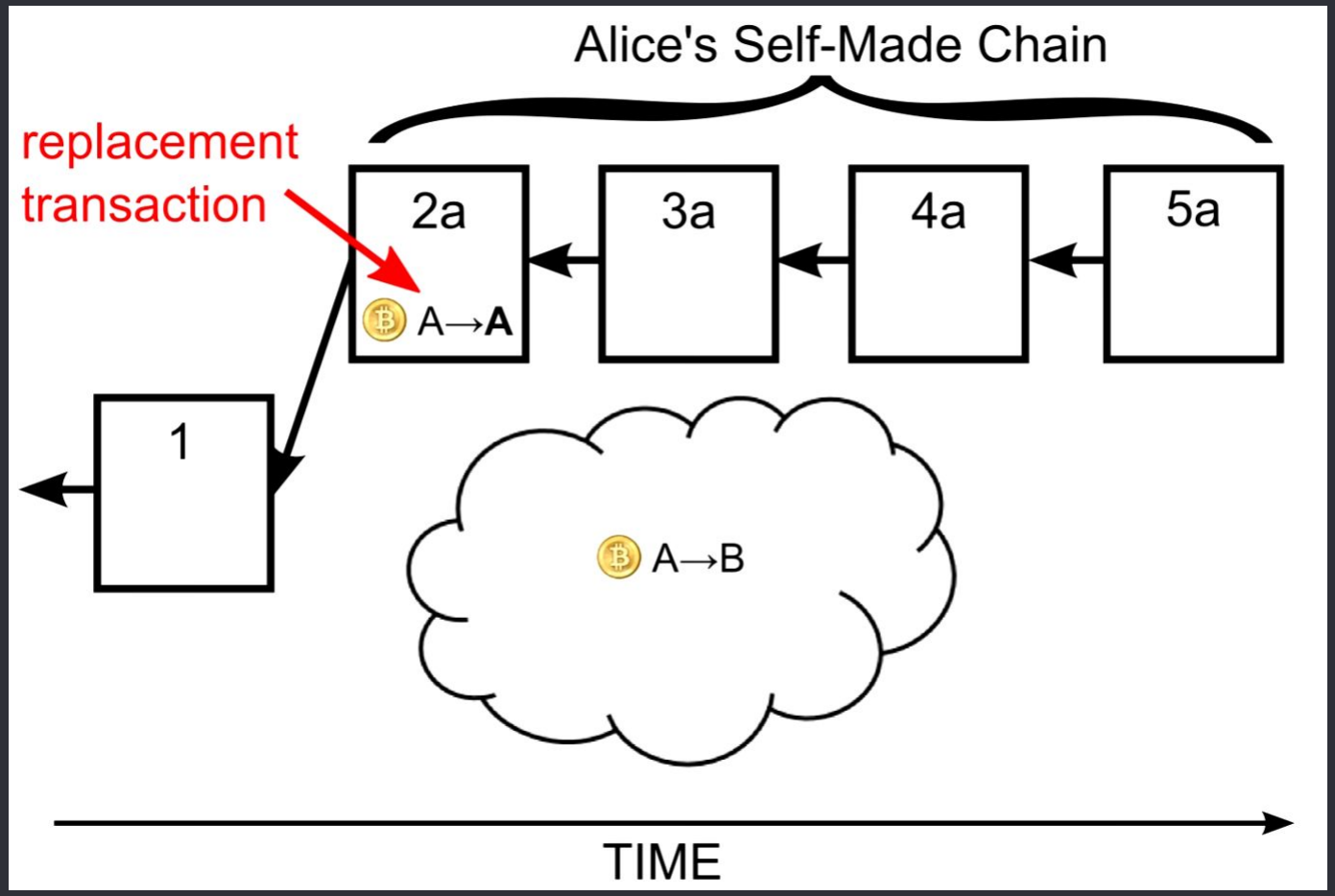
What happens to the transactions in the branches?

They get re-added to the pool of unspent/unconfirmed transactions.

Reiterating



Reiterating



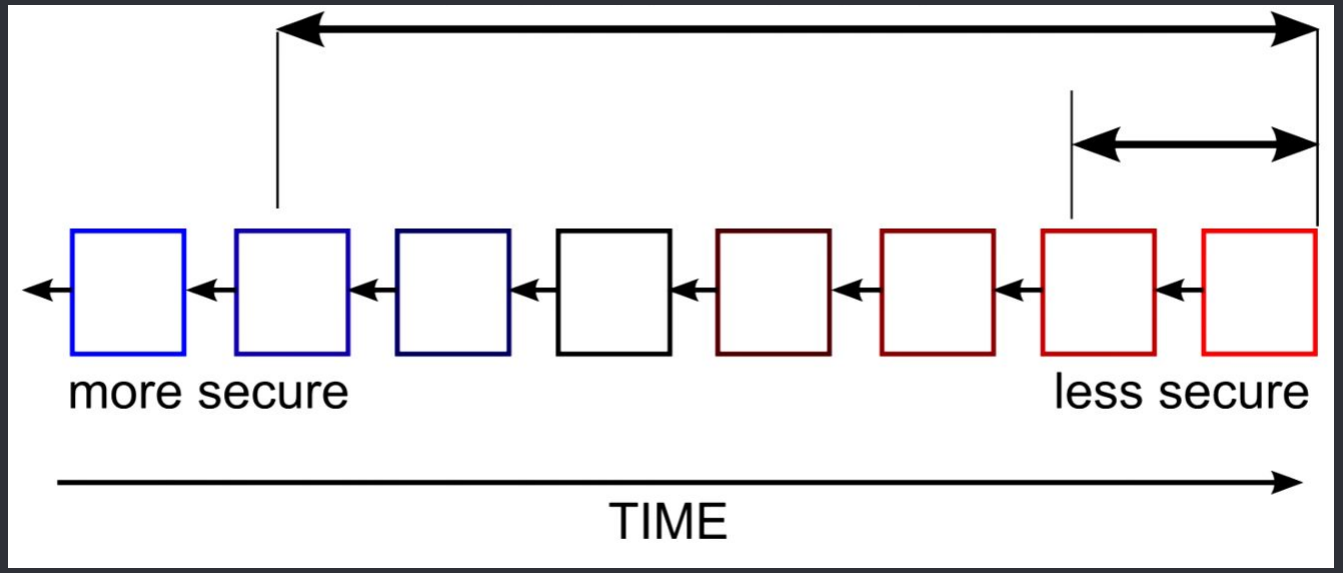
Remember that cryptographic hash?

The hash using SHA256 that was created is the title of the block. In the following block, it is pointing to that hash. If the hash in the matching guess matches that of the previous block, the block is “unlocked”.

Blocks can’t be swapped out in the middle, because then the hash values would all be different for the following blocks.

Security through time on a transaction

As a block propagates further back in the chain, it is more secure as it is proven to be correct by the decentralized network.



Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
424806	8 minutes	114	848.23 BTC	BTCC Pool	107.77
424805	8 minutes	1308	16,268.12 BTC	F2Pool	999.92
424804	18 minutes	200	601.07 BTC	ViaBTC	987.94
424803	18 minutes	1552	12,562.31 BTC	F2Pool	919.32
424802	27 minutes	2051	24,112.05 BTC	F2Pool	999.84
424801	30 minutes	2323	25,818.74 BTC	BTCC Pool	998.2

24,112.05 BTC

Is that a lot of money?

$18,340,755.00 CAN

That's a lot of money!

Height	Age	Transactions	Total Sent	Relayed By
424806	8 minutes	114	848.23 BTC	BTCC Pool
424805	8 minutes	1308	16,268.12 BTC	F2Pool
424804	18 minutes	200	601.07 BTC	ViaBTC
424803	18 minutes	1552	12,562.31 BTC	F2Pool
424802	27 minutes	2051	24,112.05 BTC	F2Pool
424801	30 minutes	2323	25,818.74 BTC	BTCC Pool

Hold on a second!

Two blocks in the chain are competing!

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
424807	5 minutes	1144	13,757.75 BTC	BW.COM	478.74
424806	13 minutes	114	848.23 BTC	BTCC Pool	107.77
424805	13 minutes	1308	16,268.12 BTC	F2Pool	999.92

Other Applications of the Blockchain

Ethereum

Distributed computing platform providing a decentralized virtual machine.

Storj.io

Distributed, encrypted file storage solution.

Slock.it

Payment solution to rent out products or services. Uses Ethereum system.

The Future

The blockchain technology and all associated platforms are still in their infancy. The biggest challenge to date is scaling solutions. None of these currencies or transactional platforms face a fraction of the demand as credit card services like Visa and Mastercard do.

Thanks!

ANY QUESTIONS?