

Quick review

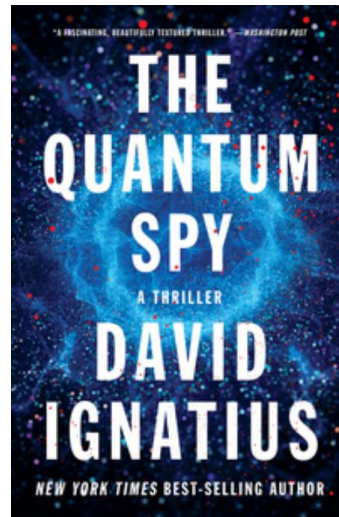
- Crypto as a currency - acceptance is lacking
- Relies on two types of cryptography - public key for the account's "identity" and hashing for the trust we have in the ledger

The techniques used for PK cryptography will be broken

Shor's algorithm will have to ...

Who/what will break them?

- A brilliant mathematician on a traditional computer
- AI on a traditional computer
- Peter Shor
- Are we ready?



Run on a quantum computer

Hashing is a different creature than PK

- Give it a try at [FileFormatInfo](#)
- Your bank doesn't really know your password, instead it hashes it to hash code. Worried that a hacker will get access to your account by trying something that accidentally hashes to your code?
- A killer rogue asteroid happens about once every 30 million years. The probability of a few billion people being killed by such an asteroid in the next second being 10^{15} . This killer asteroid event is 45 orders of magnitude more probable than a SHA-256 collision.

Unlike PK cryptography, hashing will not be broken
unless you win ...



The Golden Ticket

Bitcoin miners compete in this lottery to be first to validate a block of transactions. Nonces are the hash code glue that binds the blocks together in the *blockchain*

Public Key	Bitcoin in Satoshis	Transaction ID	Parent transaction ID	Miner Fee
PK _{Bob}	2000	6036	0929	2
PK _{Alice}	1000	CA2C	A5E3	1
PK _{Bob}	3000	4D23	C137	3
...				...
My-ID-Nonce	6E3F			
Prev-ID-Nonce	2AB6			
CoinbasePubKey _{Miner}	100000			

Hashing takes an arbitrarily long string and associates it with a 256 bit number called its hash code

- You can try a variety of them at [FileFormatInfo](#)
- Example: Your bank doesn't really know your password, instead it hashes it to hash code.
- Should you worry that a hacker gets access to your account by trying something that, although not your actual password, nonetheless hashes to it?
- A killer rogue asteroid happens about once every 30 million years on average. This leads to the probability of a few billion people being killed by such an asteroid in the next second being 10_{15} . Compared to SHA-256, this killer asteroid event is 45 orders of magnitude more probable than a SHA-256 collision.

Double spending in the accepted network blockchain

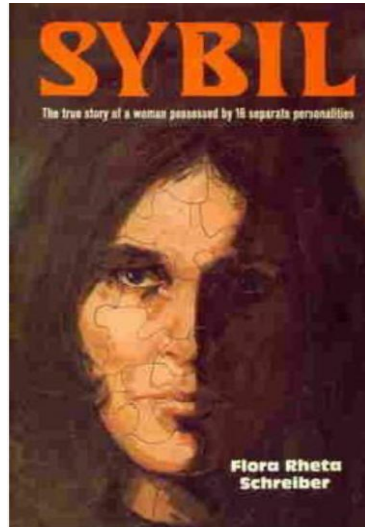
A block that holds two conflicting payments is thrown out as invalid. Hence the real danger is two different versions of the distributed blockchains are competing for acceptance (validation). For example:

- Alice has exactly 100000 Satoshis.
- She pays Bob, a car dealer, 10000 Satoshis (call it transaction T_1). T_1 goes into Block 100, and Bob hands over the car.
- In secret, Alice signs a second transaction, T_2 , that sends the same 10000 Satoshis to another public key she owns.

T_1 and T_2 can't both be valid, because they spend the same coin. The question is which one the blockchain network ends up keeping in the currently accepted chain.

Alice is the crypto reincarnation of Sybil

- A 1973 book by Flora Rheta Schreiber about the treatment of Sybil Dorsett, a woman diagnosed with a dissociative identity disorder.



How proof-of-work consensus is supposed to stop it

Any node in the network chains that see T_2 **after T_1 is validated** will reject T_2 . What mining adds is a fixed order of events that, although very computationally expensive, allows rewriting blocks in competing chains.

1. Each block is chained to the one before it by proof-of-work. This means a huge number of hash guesses have been made at the nonce.
2. Nodes treat the longest chain as the true history. But “Longest” really just means the chain with the most total work (that is, nonce guesses) behind it.
3. To get T_2 accepted, Alice has to build a competing chain that leaves out Block 100 where she paid Bob and includes T_2 instead. Then she has to make that chain longer than the honest one, which keeps growing about every 10 minutes. A race to test Alice’s computational power.

How it can be cheated – the **51%** attack

1. Alice pays Bob, and the payment lands in Block 100.
2. At the same time, she mines a private chain from Block 99 that contains T_2 instead.
3. Bob waits for some validations of blocks following Block 100 and then hands over the car. “Some” usually means about 6.
4. If Alice’s private chain ever gets longer than the public one, she broadcasts it. The network switches to it, Block 100 is dropped, and T_1 is cancelled. Alice keeps both the car and the coin.

Waiting for more validations protects Bob, but only if Alice has less than half the mining power. Above 50% and Alice wins eventually no matter how long Bob waits.



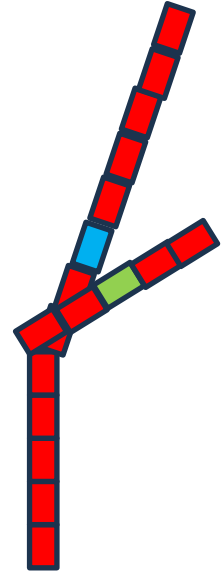
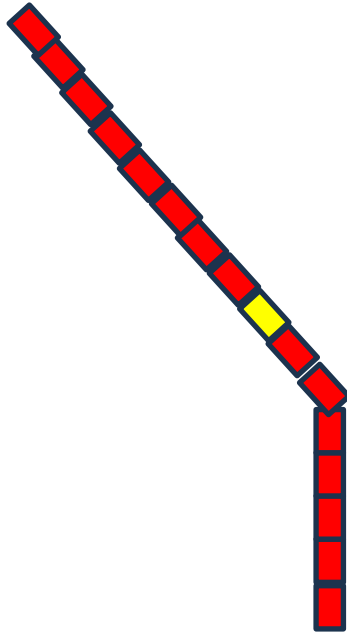
Chain Bob sees as secure



Chain Alice mines and submits to the network



A different loser chain



Such attacks can work. In the [Bitcoin Gold \(May 2018\) episode](#), attackers double-spent about 388,000 BTGcoins, worth about \$18M at the time

There are competing consensus techniques, like Ethereum's *proof of stake*

- Bitcoin's proof of work requires about 10 minutes to mine a new block.
- Ethereum miners stake an amount of Ethereum coins they are willing to lose if they are caught doing any “funny business”. A random number generator selects the miner based on the size of their stake.
- About 12 seconds to process a block.
- Easier to attack. In August 2020, a series of 51% attacks over two weeks, including 5.6 million and 1.68 million from centralized exchanges

Stable Coin currencies are directly pegged to the US dollar

- Their proponents say they're like having a checking account with anonymous, multiple identities
- But if their creators cannot actually back up the coins with real dollars, they fail. The biggest failure was TerraUSD in May 2022. At its peak in spring 2022, Terra and its sister token Luna were worth more than 50 billion combined. When they crashed in May 2022, investors lost over 40 billion.
- A personal view, but a checking that respects no international boundaries and allows multiple anonymous identities. I've never tried to launder any money, but ...

Finally the "*Not my wallet, not my keys*" caution -- when you let others store your coins

- Mt. Gox was a Tokyo bitcoin exchange that handled most of the world's Bitcoin trading in the early 2010s. The name stood for "Magic: The Gathering Online eXchange".
- 2011 an early warning: Hackers used a compromised auditor's computer to drop the exchange's bitcoin price to one cent. They then moved about 2,000 BTC out of customer accounts.
- 2014: Mt. Gox stopped all bitcoin withdrawals. It blamed "transaction malleability," a quirk in Bitcoin's software. Trading stopped and the website went offline. Mt. Gox filed for bankruptcy in Tokyo. It said 850,000 BTC were gone.