Blockchain

Patch Notes

Coming up:

Recitation: Review and honeypots

Patch Notes

Coming up:

Recitation: Review and honeypots

Thursday: Guest Lecture by Andy Sayler on the legality of security, hacking, and crypto

Patch Notes

Coming up:

Recitation: Review and honeypots

Thursday: Guest Lecture by Andy Sayler on the legality of security, hacking, and crypto

Next week: Malware (guest) and social engineering (me)

Patch Notes

FCQs are available for one week, until April 16!

Patch Notes

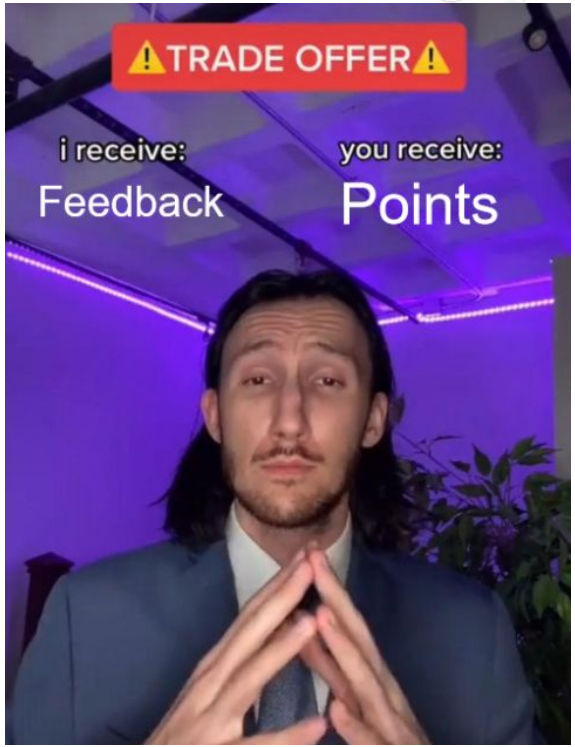
FCQs are available for one week, until April 16!

- They are very important for the future of this class

Patch Notes

FCQs are available for one week, until April 16!

- They are very important for the future of this class
- If 80% of the class submits them, I will drop the lowest quiz

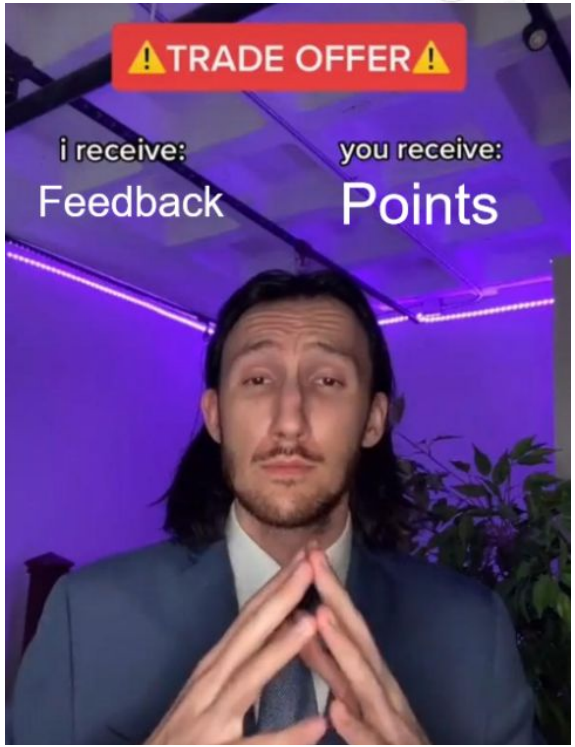


Patch Notes

FCQs are available for one week, until April 16!

- They are very important for the future of this class
- If 80% of the class submits them, I will drop the lowest quiz

Also, there is still the anonymous feedback form on Canvas!



Last submission deadline:
Thursday (4/21)

Any later work by exception only!

A short look at Blockchain security


THE GOOD

Problem: Ownership

Traditional services have **owners** and **users**

- Owners have total control over the service
- Users depend on the security of the service

Problem: Ownership

Traditional services have **owners** and **users**

- Owners have total control over the service
- Users depend on the security of the service

Problem:

Service *owners* can violate the security of service *users*

Problem: Ownership

Abuses of **confidentiality**

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters

- 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower
- Mark Zuckerberg breaks silence on Cambridge Analytica

Cambridge Analytica whistleblower: 'We spent $1m harvesting millions of Facebook profiles' – video

https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Problem: Ownership

Abuses of **integrity**

Wells Fargo Opened a Couple Million Fake Accounts

You get what you measure, even if it's not what you wanted.

One bad thing Wells Fargo did was called 'sandbagging.' *Photographer: Jessica Kourkounis/Getty Images*

https://www.bloomberg.com/opinion/articles/2016-09-09/wells-fargo-opened-a-couple-million-fake-accounts

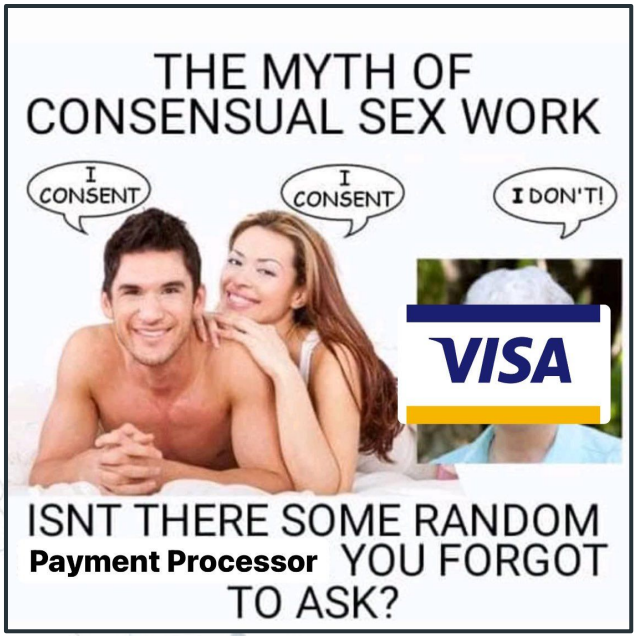
Problem: Ownership

Abuses of **availability**

https://twitter.com/inputmag/status/1428422711118901255

Problem: Ownership

Abuses of **availability**



https://twitter.com/inputmag/status/1428422711118901255

Problem: Ownership

Takeaway: The owner of a service has total control

- Always able to threaten user's security

Problem: Ownership

Note: Ownership is a ***risk***, like everything else

*(risk = probability * severity)*

Problem: Ownership

Currency: Great use case example

- Financial availability and integrity is very important!

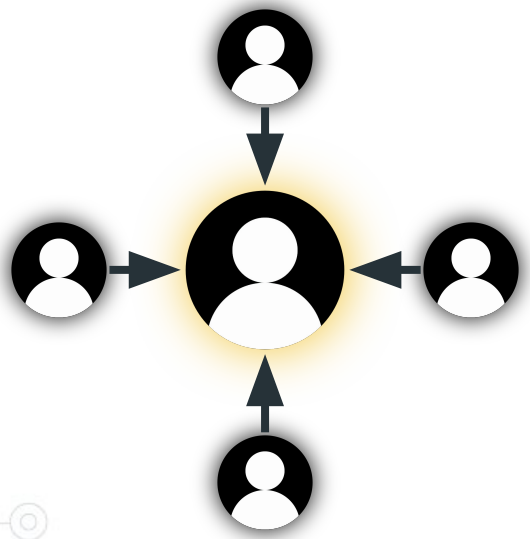
Problem: Ownership

Currency: Great use case example

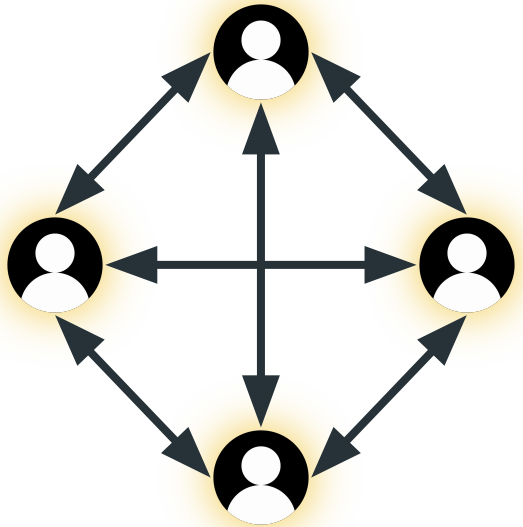
- Financial availability and integrity is very important!
- **Risk**: low **probability**, but massive **severity**

Solution: Distributed services

Centralized: Owners have total control, users have none

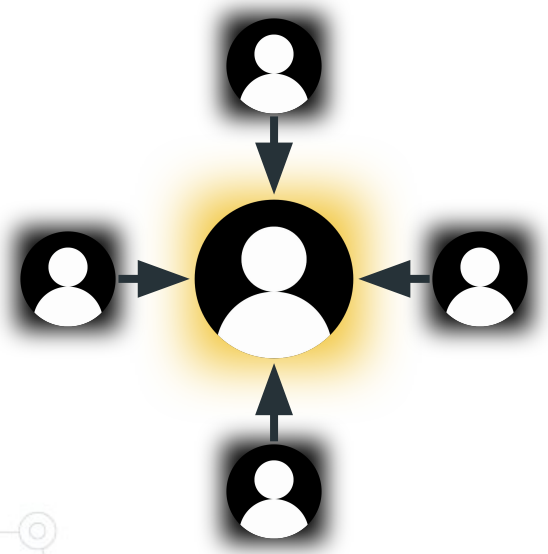


Decentralized: Owners are users, no one group has control

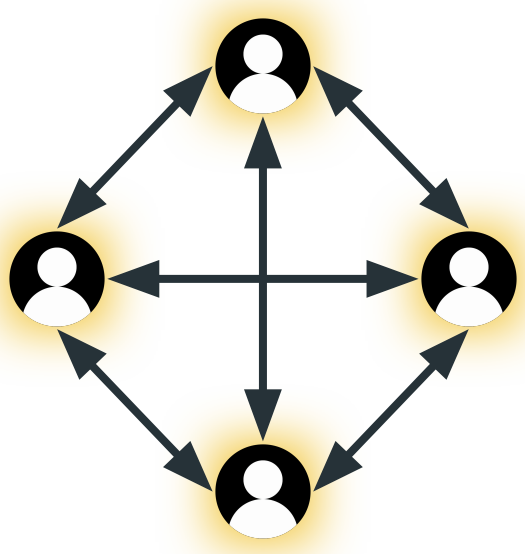


Solution: Distributed services

Centralized: Owners have total control, users have none



Decentralized: Owners are users, no one group has control



Sounds good in theory, but how does this work?

Bitcoin

How to handle currency:

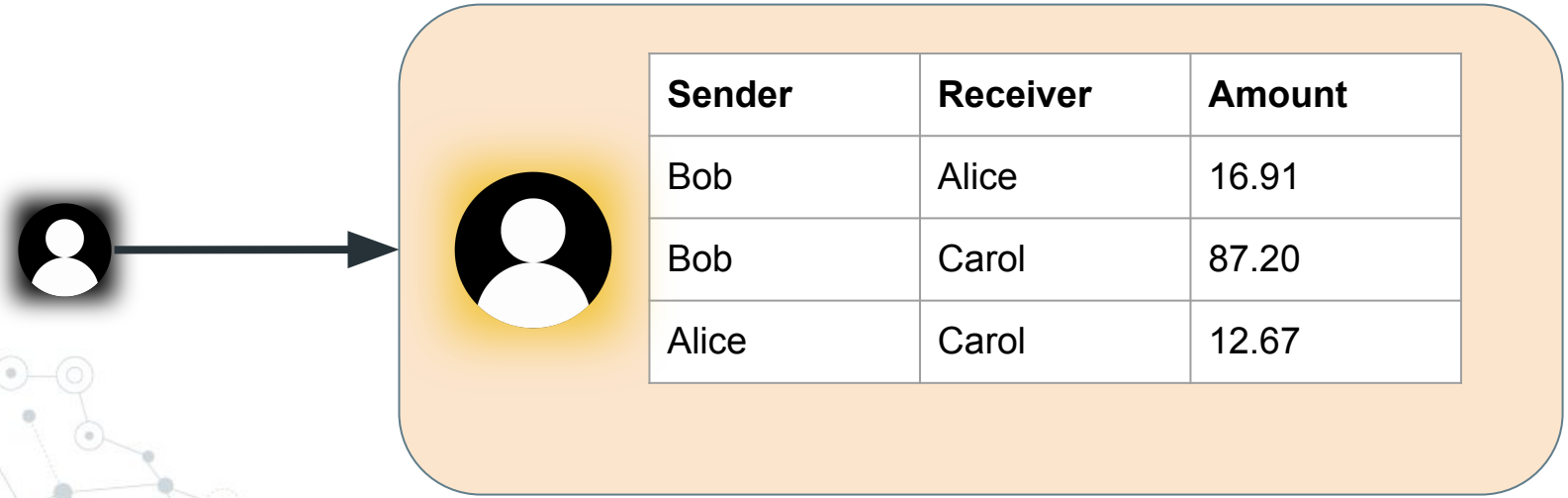
1. Store a list of transactions (a **ledger**)
2. Any time money is transferred, add a new entry

Sender	Receiver	Amount
Bob	Alice	16.91
Bob	Carol	87.20
Alice	Carol	12.67
Carol	Eve	42.00

Bitcoin

Centralized solution:

- Owner (e.g. a bank) is the **only one** with the ledger
- Users (e.g. you) can request new entries



Sender	Receiver	Amount
Bob	Alice	16.91
Bob	Carol	87.20
Alice	Carol	12.67

Bitcoin

Centralized solution:

- Owner (e.g. a bank) is the only one with the ledger
- Users (e.g. you) can request new entries

I sent $92.81 to Taco Bell

Sender	Receiver	Amount
Bob	Alice	16.91
Bob	Carol	87.20
Alice	Carol	12.67
Eve	Taco Bell	92.81

Bitcoin

Decentralized solution:

- **Everyone** has a copy of the ledger
- New entries are announced to everyone

Sender	Receiver	Amount
Alice	Eve	500.00

Sender	Receiver	Amount
Alice	Eve	500.00

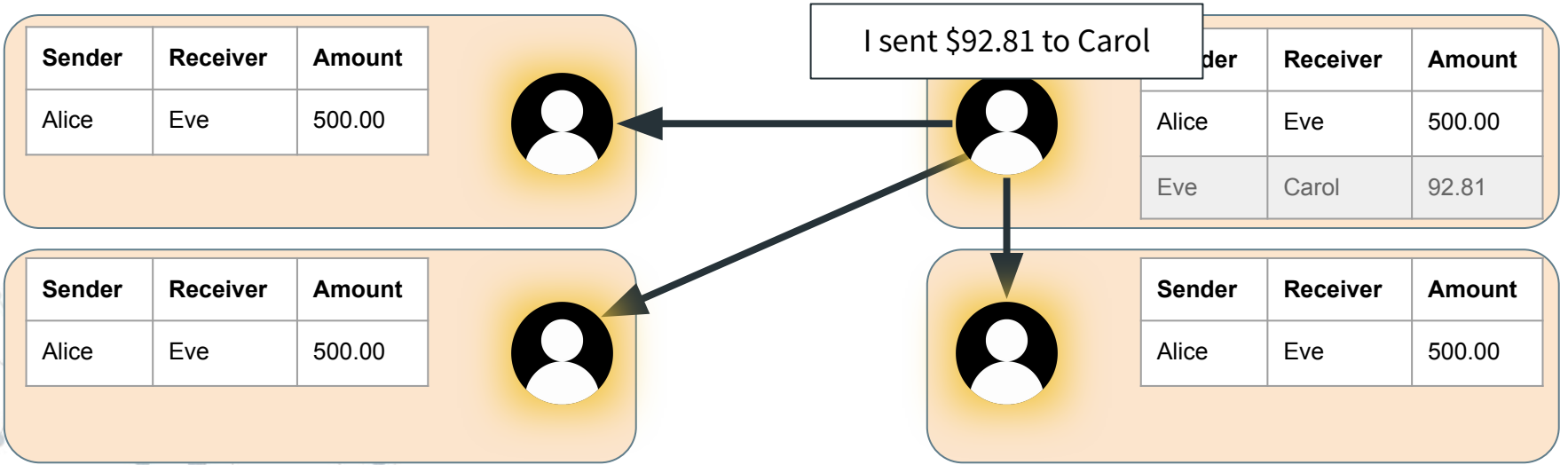
Sender	Receiver	Amount
Alice	Eve	500.00

Sender	Receiver	Amount
Alice	Eve	500.00

Bitcoin

Decentralized solution:

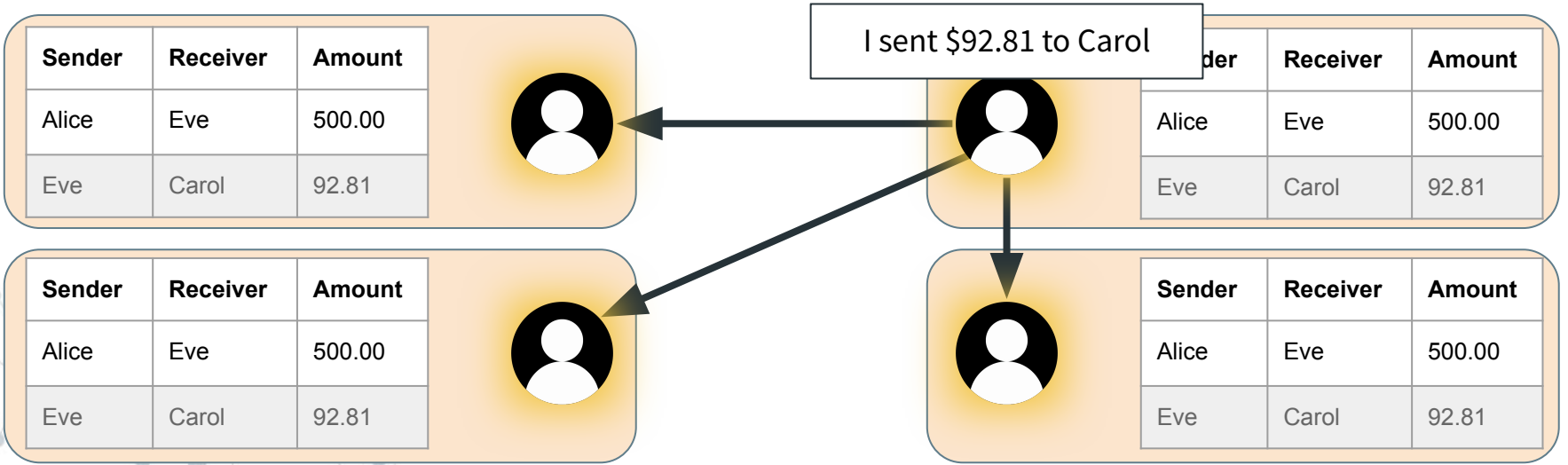
- **Everyone** has a copy of the ledger
- New entries are announced to everyone



Bitcoin

Decentralized solution:

- **Everyone** has a copy of the ledger
- New entries are announced to everyone



Bitcoin

Now there is **no owner** controlling the ledger!

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Bitcoin

Now there is **no owner** controlling the ledger!

Instead, **everyone** controls the ledger!

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Bitcoin

Now there is **no owner** controlling the ledger!

Instead, **everyone** controls the ledger!

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Sender	Receiver	Amount
Alice	Eve	500.00
Eve	Carol	92.81

Bitcoin

Potential attacks:

1. Creating fake entries (spoofing)
2. Removing real entries (repudiation)

Sender	Receiver	Amount
Bob	Alice	500.00
Alice	**Eve**	**9999.99**
Eve	Bob	11.00
Alice	Bob	20.00
Eve	Carol	116.50

Sender	Receiver	Amount
Bob	Alice	500.00
~~**Eve**~~	~~**Bob**~~	~~**11.00**~~
Alice	Bob	20.00
~~**Eve**~~	~~**Carol**~~	~~**116.50**~~

Bitcoin

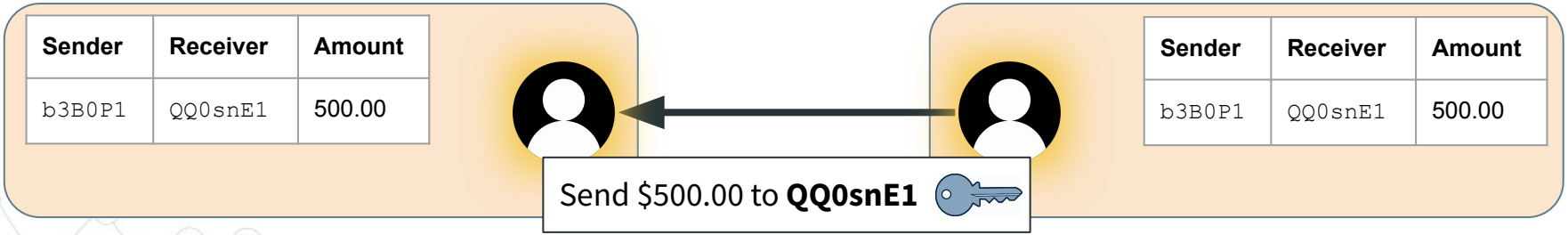
Fake entry prevention:

- Each user generates a public / private key pair

Bitcoin

Mirrors traditional username / passwords:

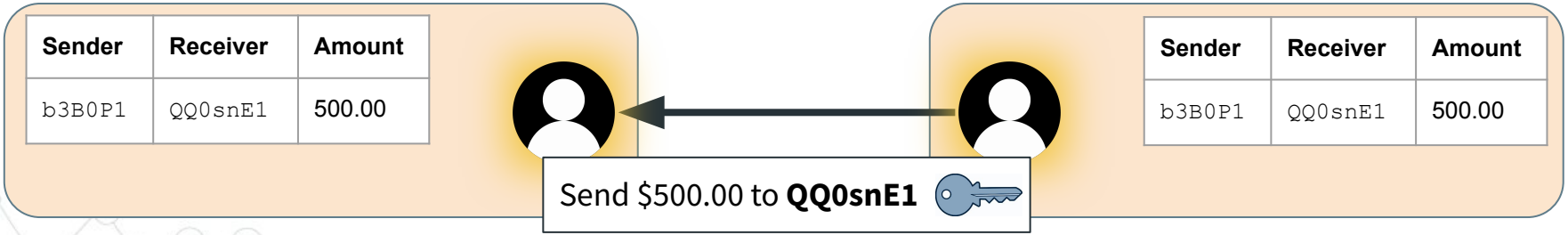
Public keys (usernames) are public



Bitcoin

Mirrors traditional username / passwords:

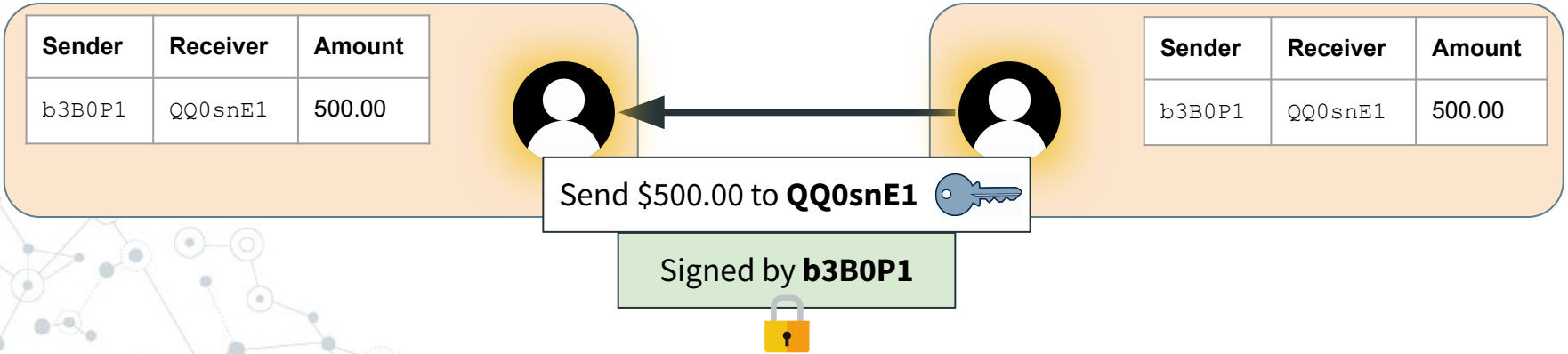
- **Public keys** (usernames) are public
  - Side bonus: pseudo-anonymity!



Bitcoin

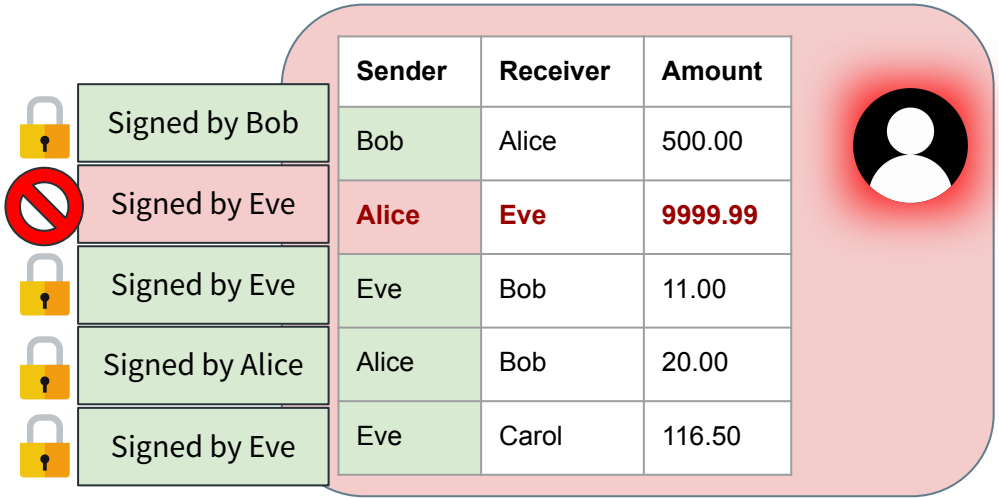
Mirrors traditional username / passwords:

- **Public keys** (usernames) are public
  - Side bonus: pseudo-anonymity!
- **Private keys** (passwords) are needed to send money



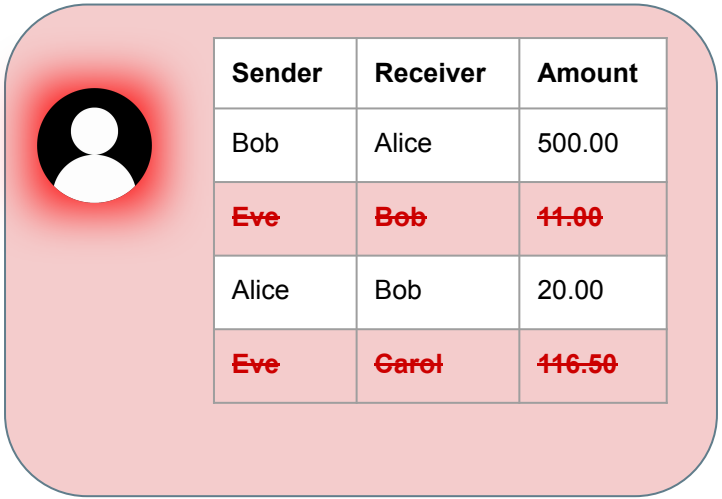
Bitcoin

Cannot fake transactions without the private key!



Bitcoin

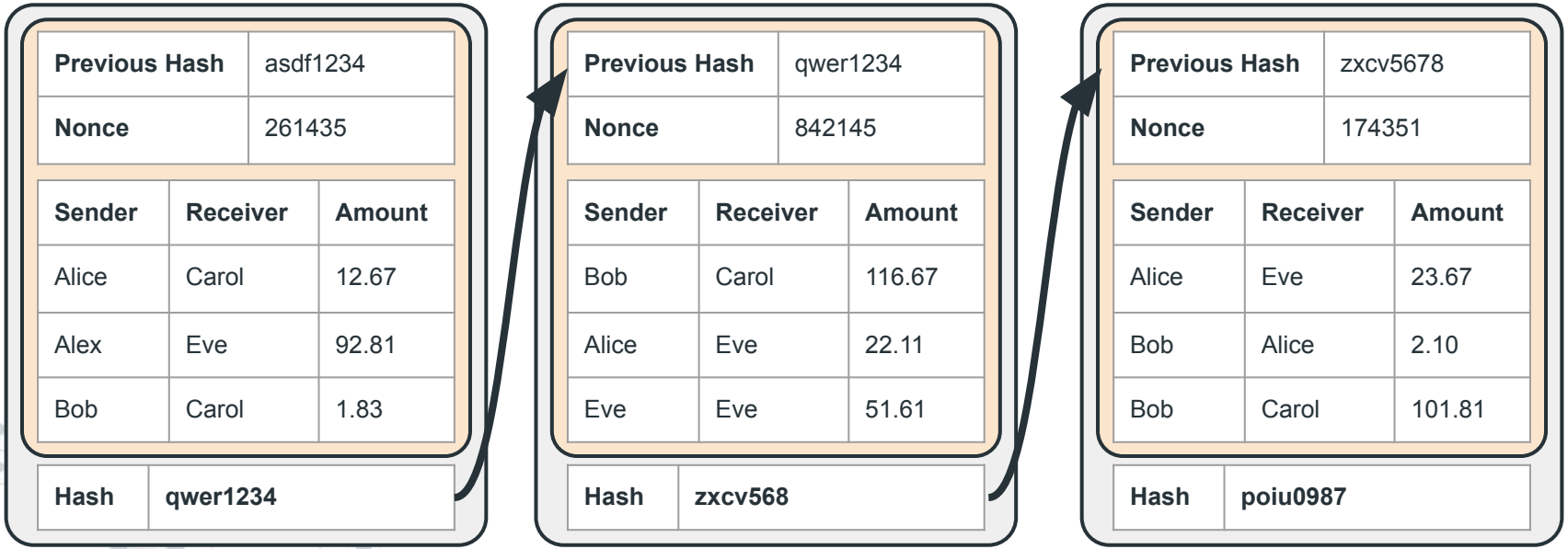
But attackers can still delete transactions!



Sender	Receiver	Amount
Bob	Alice	500.00
~~Eve~~	~~Bob~~	~~11.00~~
Alice	Bob	20.00
~~Eve~~	~~Carol~~	~~116.50~~

Bitcoin

Enter the **blockchain**!



Previous Hash	asdf1234
Nonce	261435

Sender	Receiver	Amount
Alice	Carol	12.67
Alex	Eve	92.81
Bob	Carol	1.83

Hash	qwer1234

Previous Hash	qwer1234
Nonce	842145

Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	zxcv568

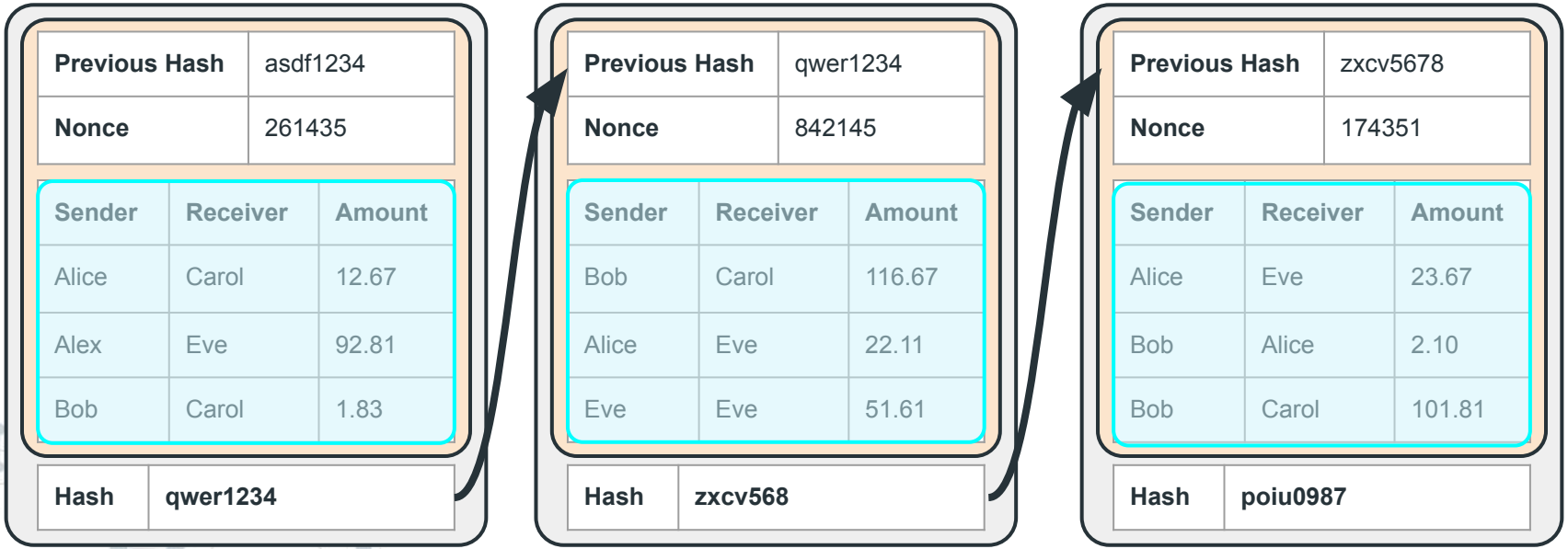
Previous Hash	zxcv5678
Nonce	174351

Sender	Receiver	Amount
Alice	Eve	23.67
Bob	Alice	2.10
Bob	Carol	101.81

Hash	poiu0987

Bitcoin

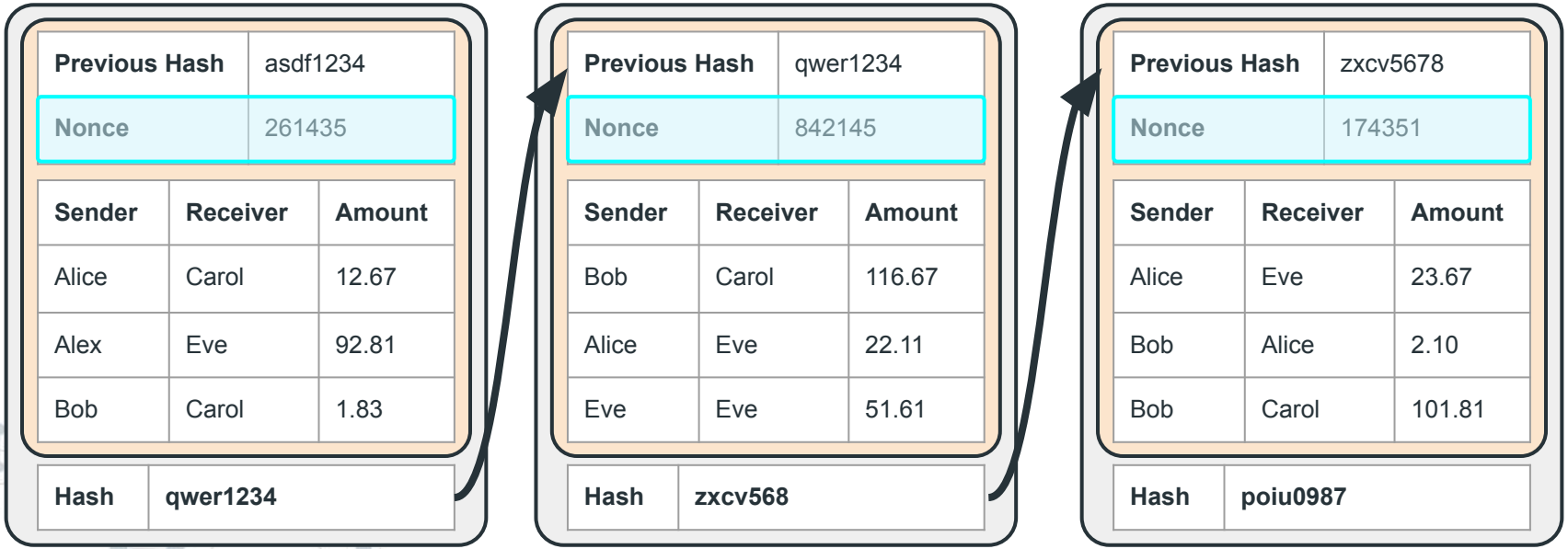
Transactions are added in blocks



Bitcoin

Blocks also store a random number called a **nonce**

This will be useful in a moment!



Previous Hash	asdf1234
Nonce	261435

Sender	Receiver	Amount
Alice	Carol	12.67
Alex	Eve	92.81
Bob	Carol	1.83

Hash	qwer1234

Previous Hash	qwer1234
Nonce	842145

Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	zxcv568

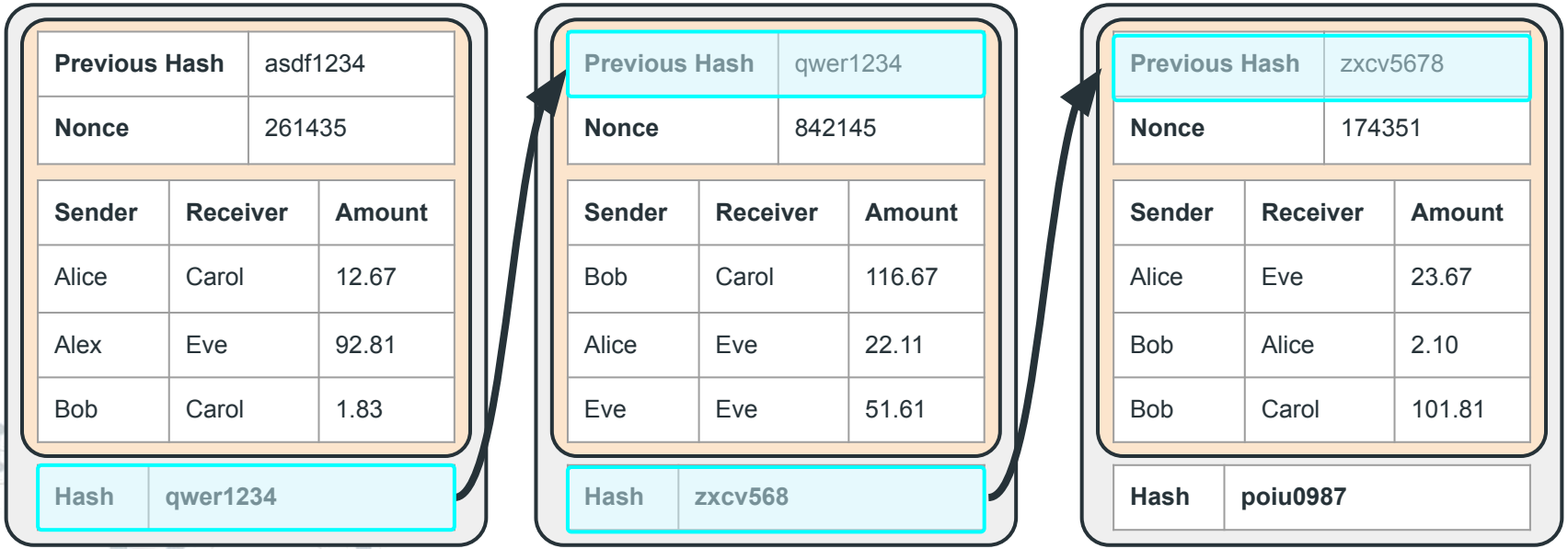
Previous Hash	zxcv5678
Nonce	174351

Sender	Receiver	Amount
Alice	Eve	23.67
Bob	Alice	2.10
Bob	Carol	101.81

Hash	poiu0987

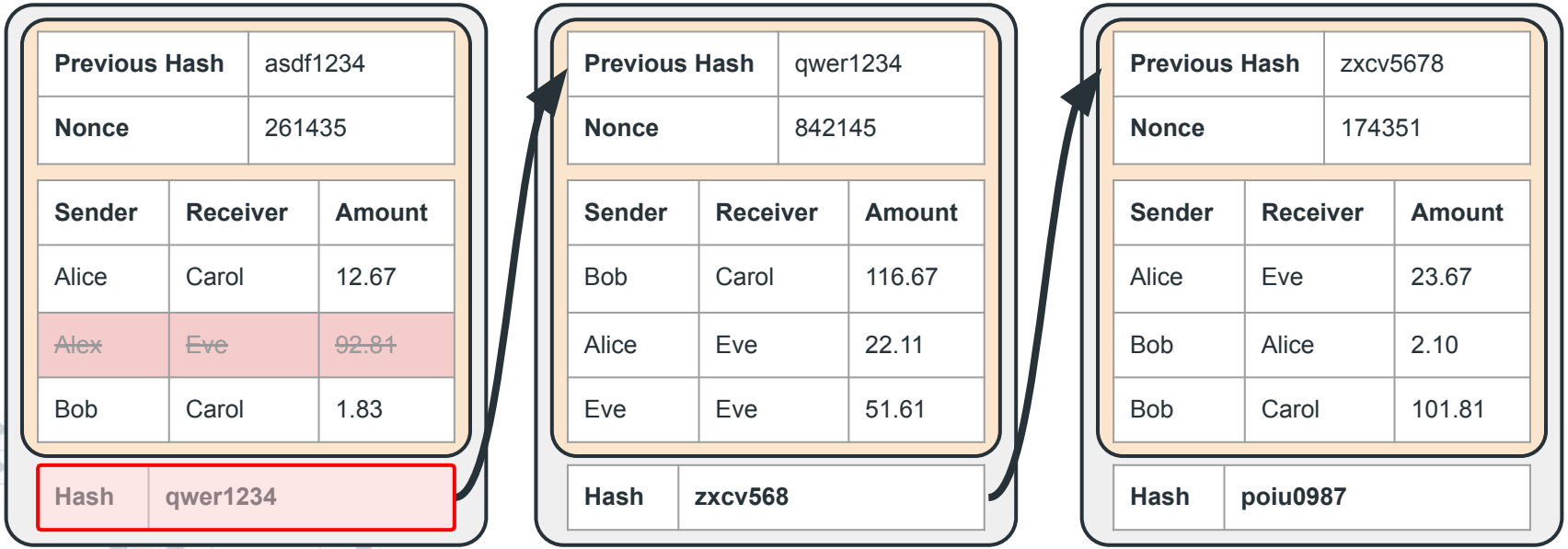
Bitcoin

Each block contains the **hash** of the previous one



Bitcoin

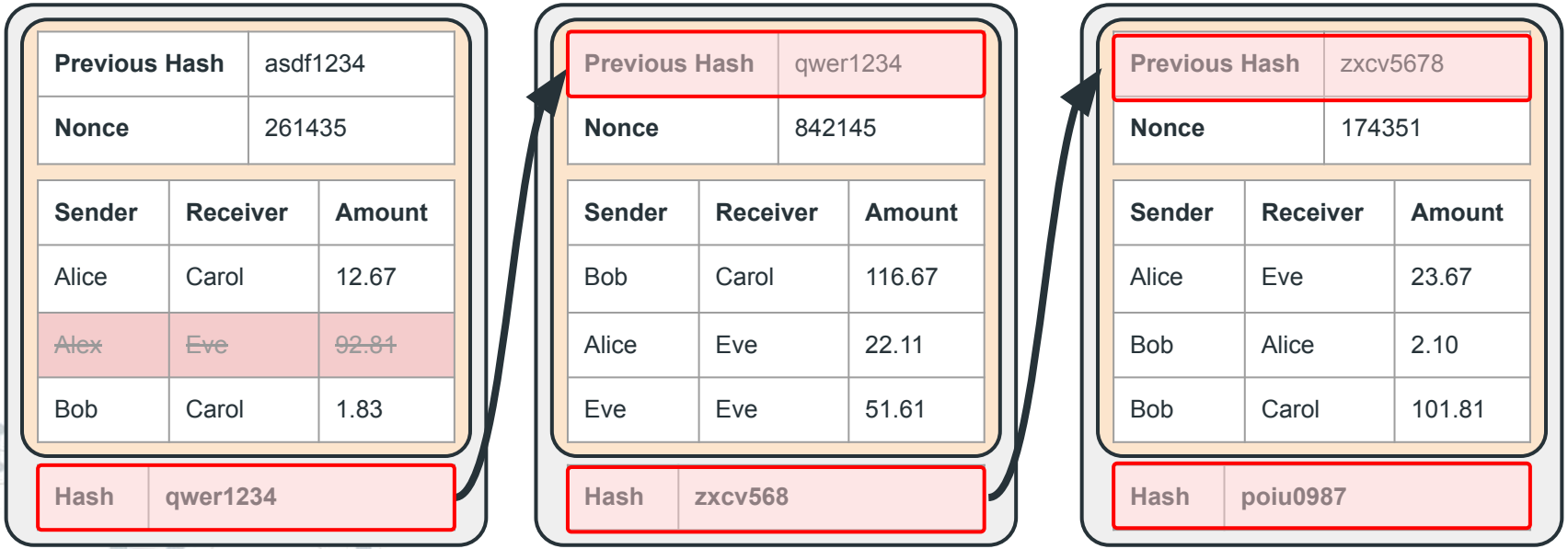
Any change to the transactions will change the hash…



Bitcoin

Any change to the transactions will change the hash…

…and the next block's hash, and the next, and so on!



Previous Hash	asdf1234
Nonce	261435

Sender	Receiver	Amount
Alice	Carol	12.67
~~Alex~~	~~Eve~~	~~92.81~~
Bob	Carol	1.83

Hash	qwer1234

Previous Hash	qwer1234
Nonce	842145

Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	zxcv568

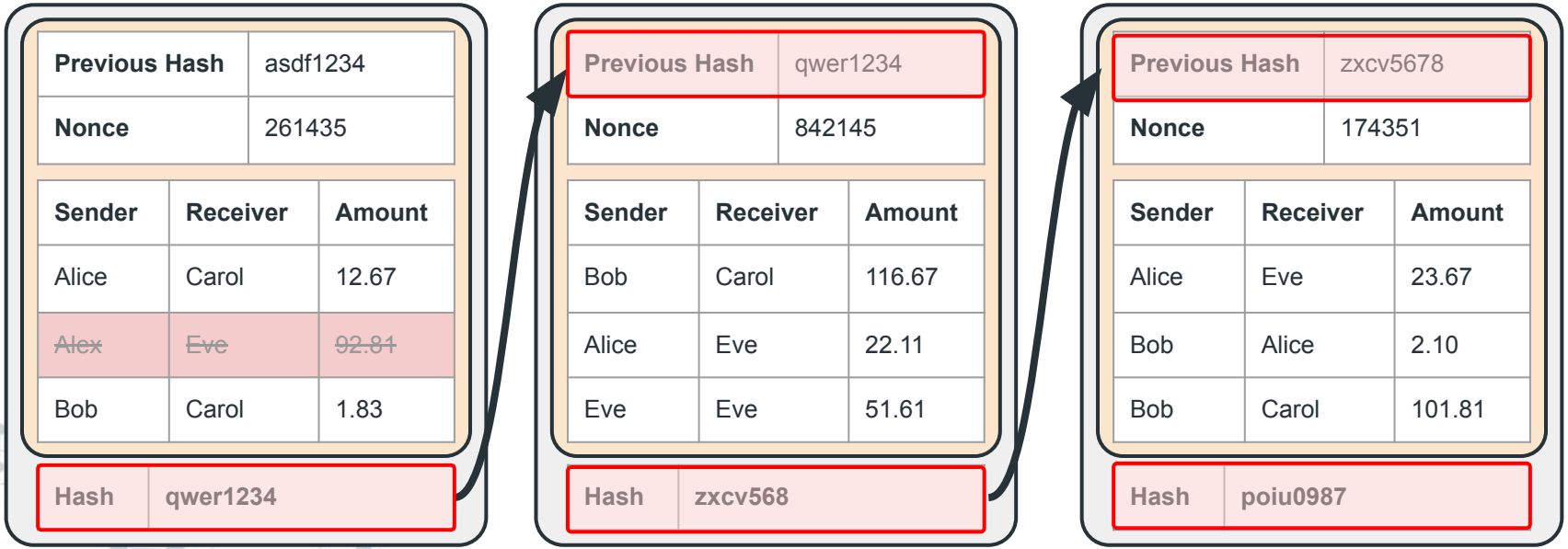
Previous Hash	zxcv5678
Nonce	174351

Sender	Receiver	Amount
Alice	Eve	23.67
Bob	Alice	2.10
Bob	Carol	101.81

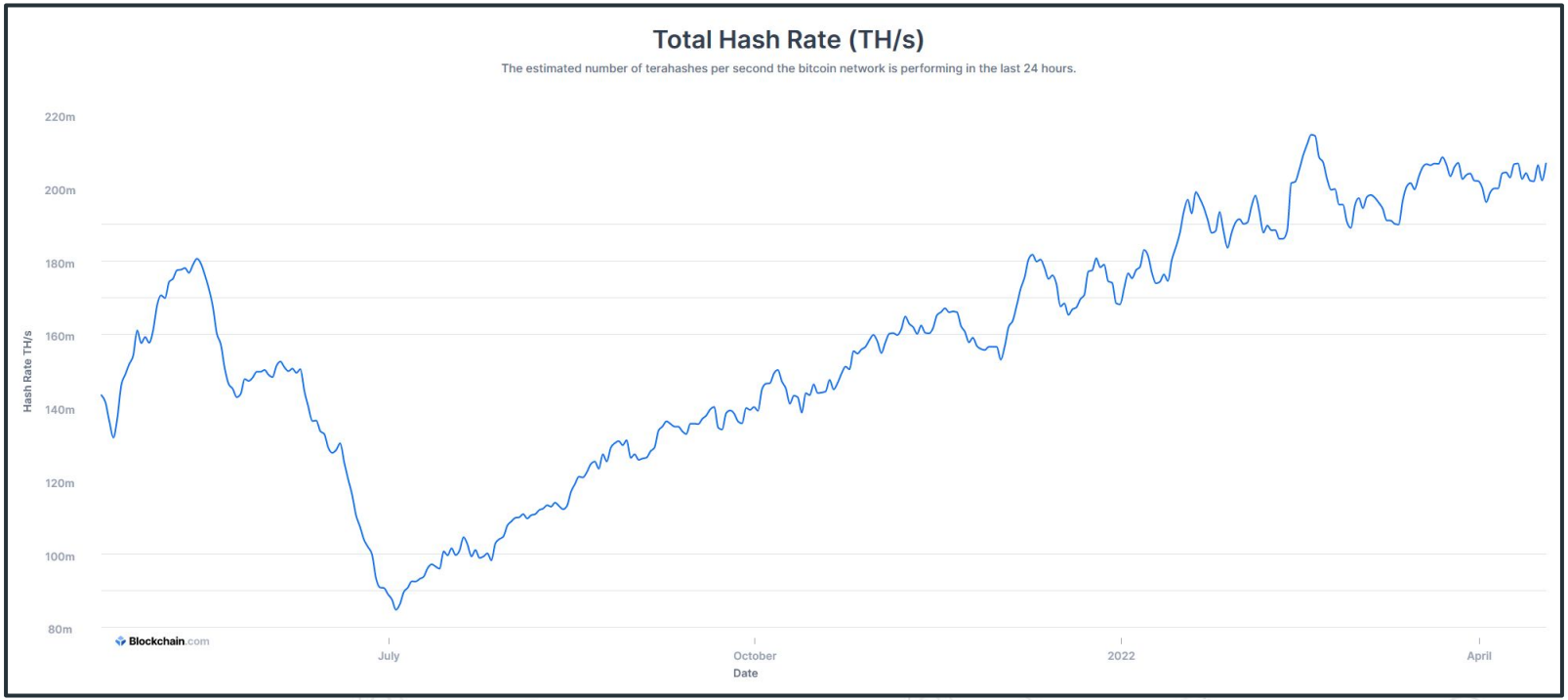
Hash	poiu0987

Bitcoin

Result: Any small change requires updating tens or hundreds of hashes!



Bitcoin



https://www.blockchain.com/charts/hash-rate

Bitcoin

Problem: Hashing is too fast, anyone can generate a fake blockchain instantly

Previous Hash	zxcv5678
Nonce	261435

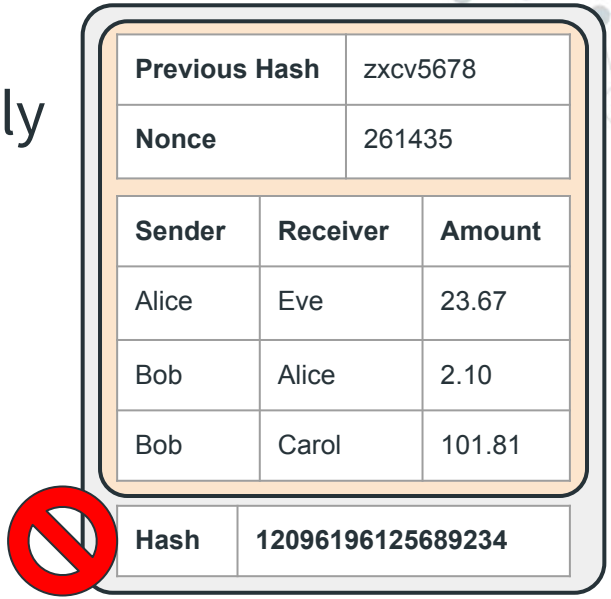
Sender	**Receiver**	**Amount**
Alice	Eve	23.67
Bob	Alice	2.10
Bob	Carol	101.81

Hash	**12096196125689234**

Bitcoin

Problem: Hashing is too fast, anyone can generate a fake blockchain instantly

Solution: Slow it down: only allow hashes that start with 8 zeros!*



*This number changes over time: currently up to 22 zeros

Bitcoin

Remember that random number (**nonce**)?

We can adjust that to change the hash

Previous Hash	asdf1234
Nonce	261435

Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	15980709324621

Previous Hash	asdf1234
Nonce	842145

Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	00087329146849391

Previous Hash	asdf1234
Nonce	174351

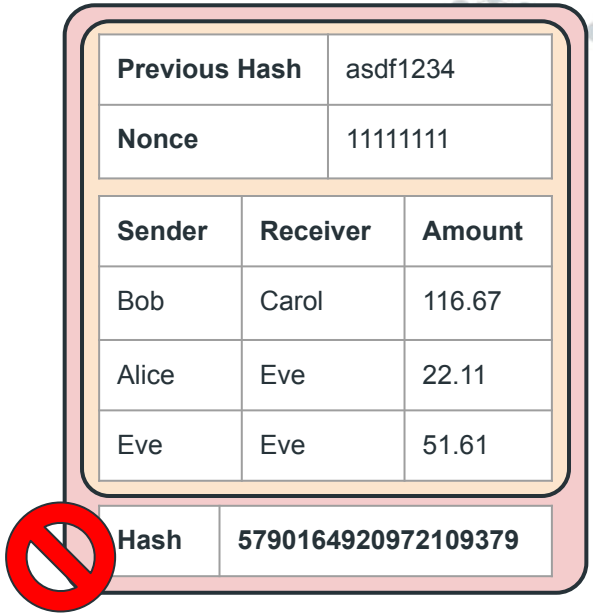
Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	00000000128681236

Bitcoin

To create a new block:

1. Pick a nonce
2. Hash
3. Repeat until the hash is valid



Previous Hash	asdf1234
Nonce	11111111

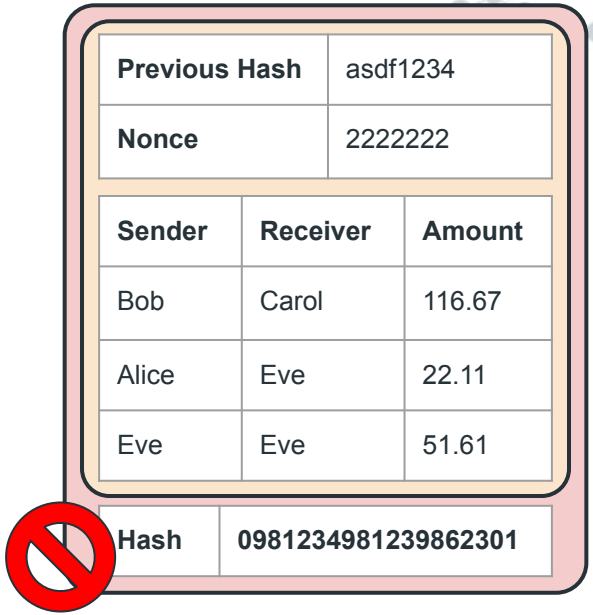
Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	5790164920972109379

Bitcoin

To create a new block:

1. Pick a nonce
2. Hash
3. Repeat until the hash is valid



Previous Hash	asdf1234
Nonce	2222222

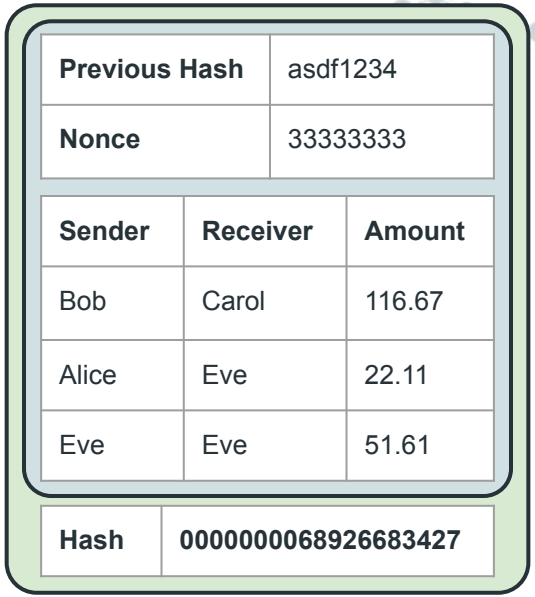
Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	0981234981239862301

Bitcoin

To create a new block:

1. Pick a nonce
2. Hash
3. Repeat until the hash is valid



Previous Hash	asdf1234
Nonce	33333333

Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

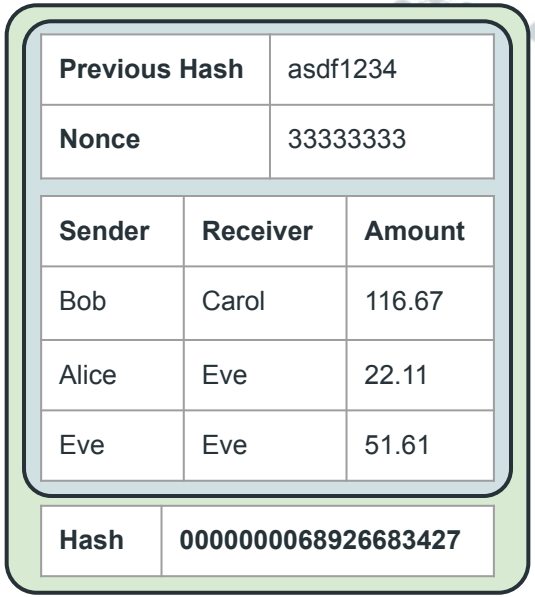
Hash	0000000068926683427

Bitcoin

To create a new block:

1. Pick a nonce
2. Hash
3. Repeat until the hash is valid

*This is called **mining** a block*



Previous Hash	asdf1234
Nonce	33333333

Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	0000000068926683427

Bitcoin

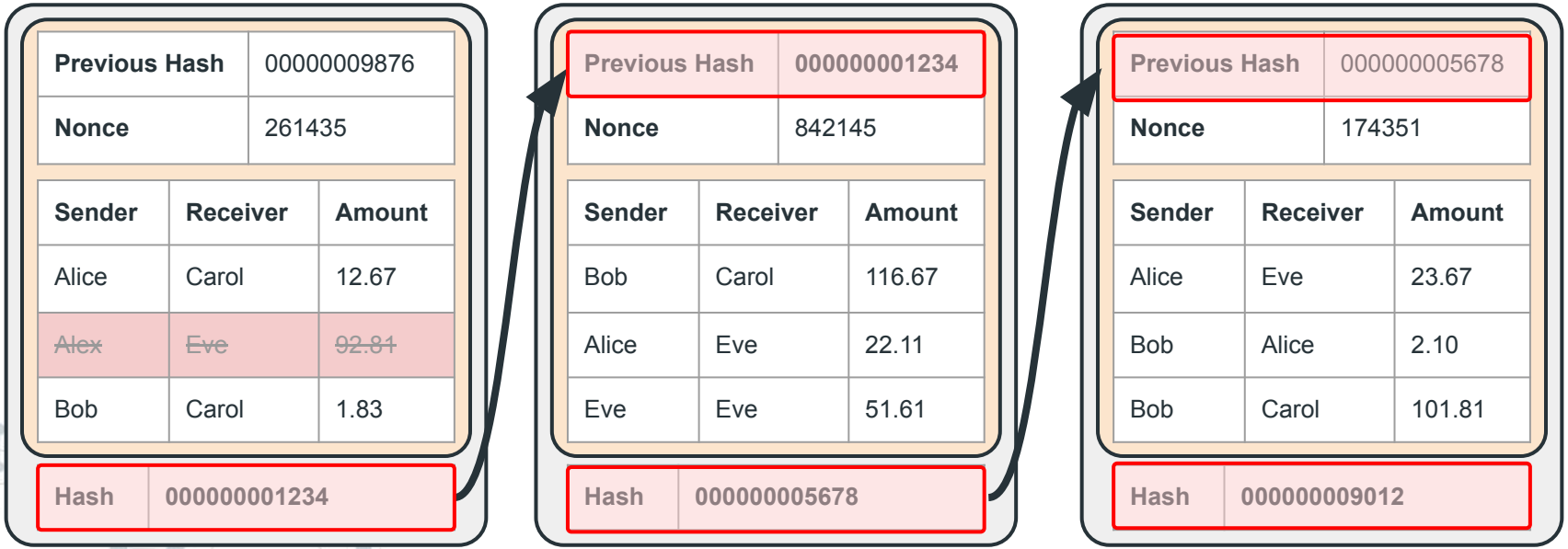
Cost: More energy than Finland for 10 minutes per block!

Previous Hash	zxcv5678	
Nonce	174351	
Sender	**Receiver**	**Amount**
Alice	Eve	23.67
Bob	Alice	2.10
Bob	Carol	101.81
Hash	**0000000038234704386**	

Bitcoin

Remember:

Any change requires re-hashing all future blocks!



Previous Hash	00000009876
Nonce	261435

Sender	Receiver	Amount
Alice	Carol	12.67
~~Alex~~	~~Eve~~	~~92.81~~
Bob	Carol	1.83

Hash	000000001234

Previous Hash	000000001234
Nonce	842145

Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	000000005678

Previous Hash	000000005678
Nonce	174351

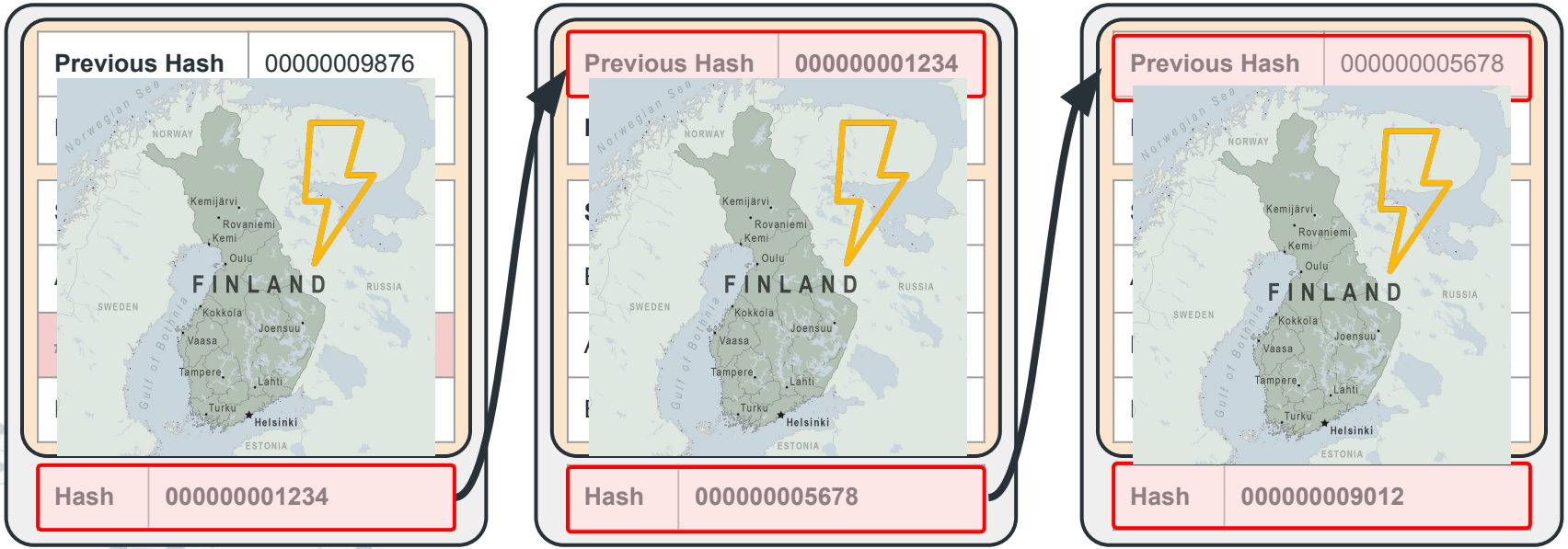
Sender	Receiver	Amount
Alice	Eve	23.67
Bob	Alice	2.10
Bob	Carol	101.81

Hash	000000009012

Bitcoin

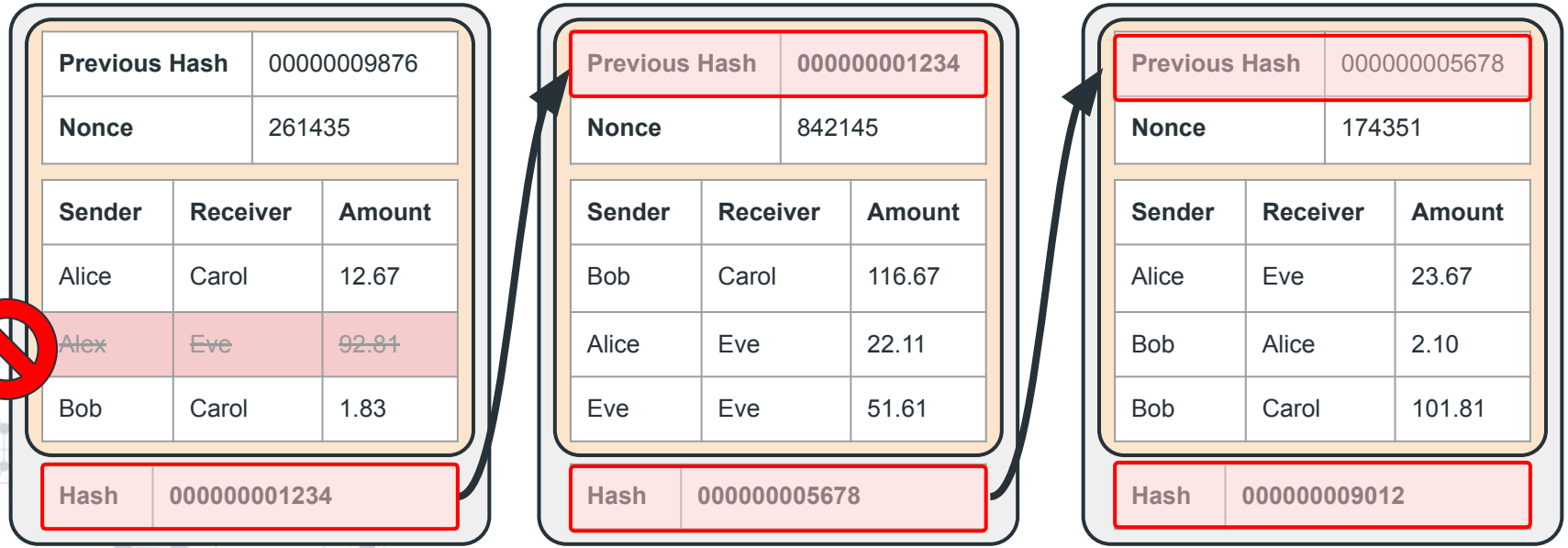
Remember:

Any change requires re-hashing all future blocks!



Bitcoin

Result: An attacker cannot modify the blockchain without an **insane** amount of energy!



Previous Hash	00000009876
Nonce	261435

Sender	Receiver	Amount
Alice	Carol	12.67
~~Alex~~	~~Eve~~	~~92.81~~
Bob	Carol	1.83

Hash	000000001234

Previous Hash	000000001234
Nonce	842145

Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	000000005678

Previous Hash	000000005678
Nonce	174351

Sender	Receiver	Amount
Alice	Eve	23.67
Bob	Alice	2.10
Bob	Carol	101.81

Hash	000000009012

Bitcoin

Potential attacks:

1. Creating fake entries (spoofing)
2. Removing real entries (repudiation)

Sender	Receiver	Amount
Bob	Alice	500.00
Alice	**Eve**	**9999.99**
Eve	Bob	11.00
Alice	Bob	20.00
Eve	Carol	116.50

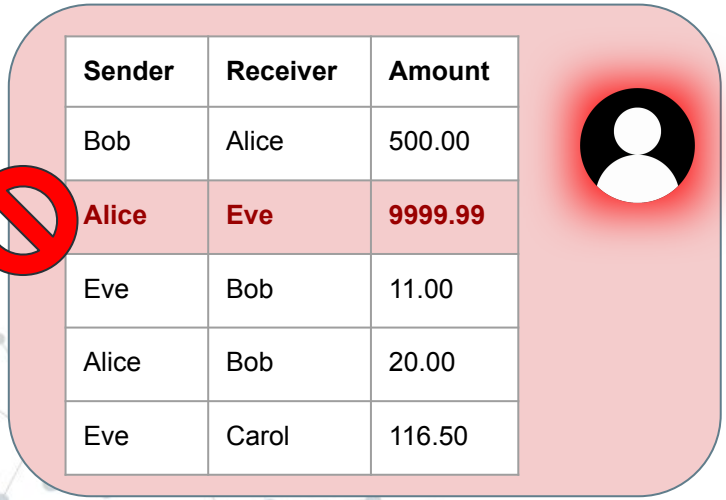
Sender	Receiver	Amount
Bob	Alice	500.00
~~**Eve**~~	~~**Bob**~~	~~**11.00**~~
Alice	Bob	20.00
~~**Eve**~~	~~**Carol**~~	~~**116.50**~~

Bitcoin

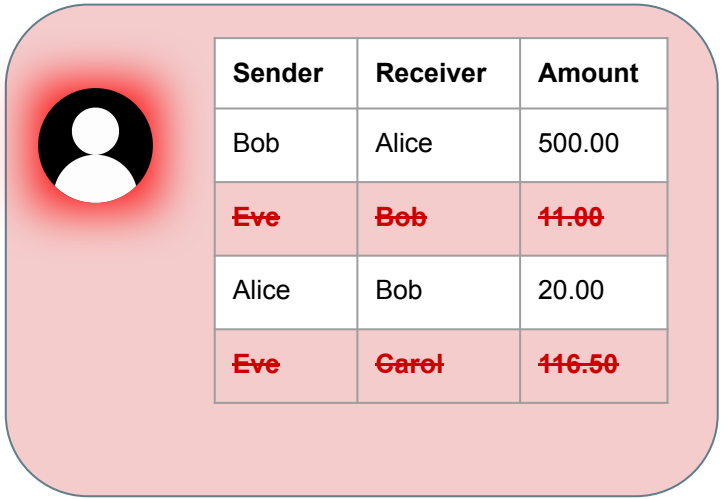
Potential attacks:

1. ~~Creating fake entries (spoofing)~~
2. Removing real entries (repudiation)

Cannot sign transactions



Sender	Receiver	Amount
Bob	Alice	500.00
Alice	**Eve**	**9999.99**
Eve	Bob	11.00
Alice	Bob	20.00
Eve	Carol	116.50



Sender	Receiver	Amount
Bob	Alice	500.00
~~**Eve**~~	~~**Bob**~~	~~**11.00**~~
Alice	Bob	20.00
~~**Eve**~~	~~**Carol**~~	~~**116.50**~~

Bitcoin

Potential attacks:

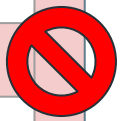
1. ~~Creating fake entries (spoofing)~~
2. ~~Removing real entries (repudiation)~~

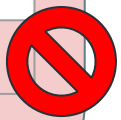
Cannot sign transactions

Cannot forge blocks fast enough

Sender	Receiver	Amount
Bob	Alice	500.00
Alice	**Eve**	**9999.99**
Eve	Bob	11.00
Alice	Bob	20.00
Eve	Carol	116.50

Sender	Receiver	Amount
Bob	Alice	500.00
~~**Eve**~~	~~**Bob**~~	~~**11.00**~~
Alice	Bob	20.00
~~**Eve**~~	~~**Carol**~~	~~**116.50**~~

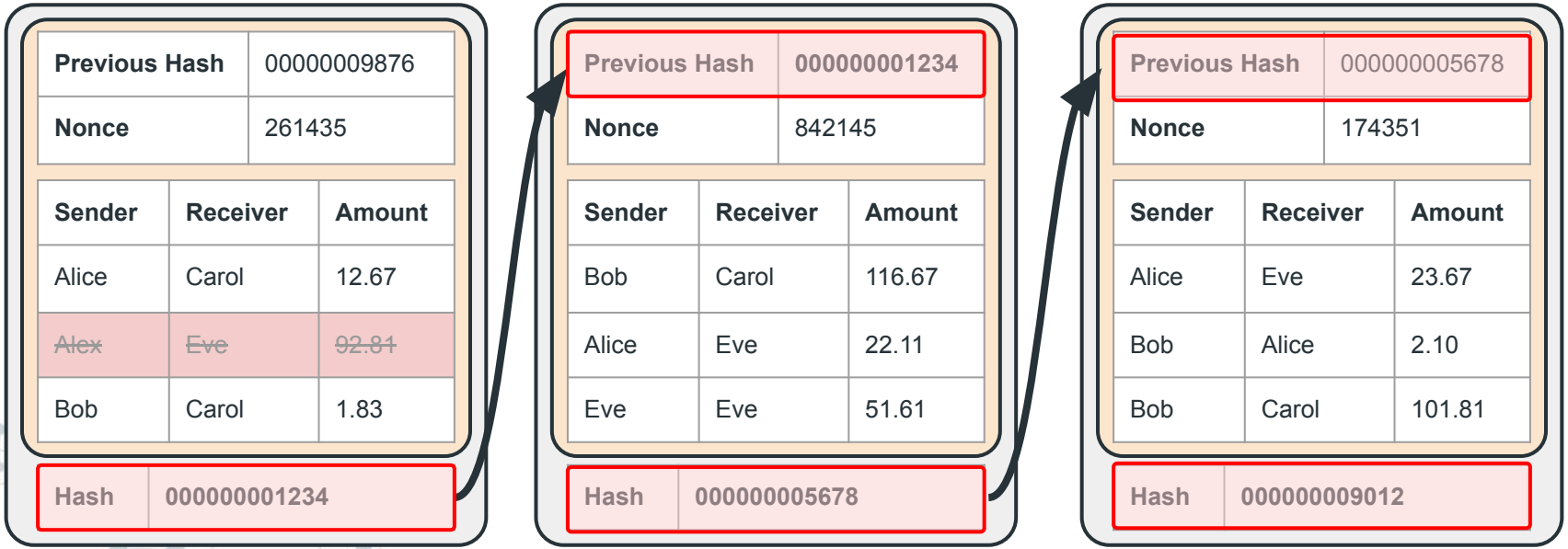





THE BAD

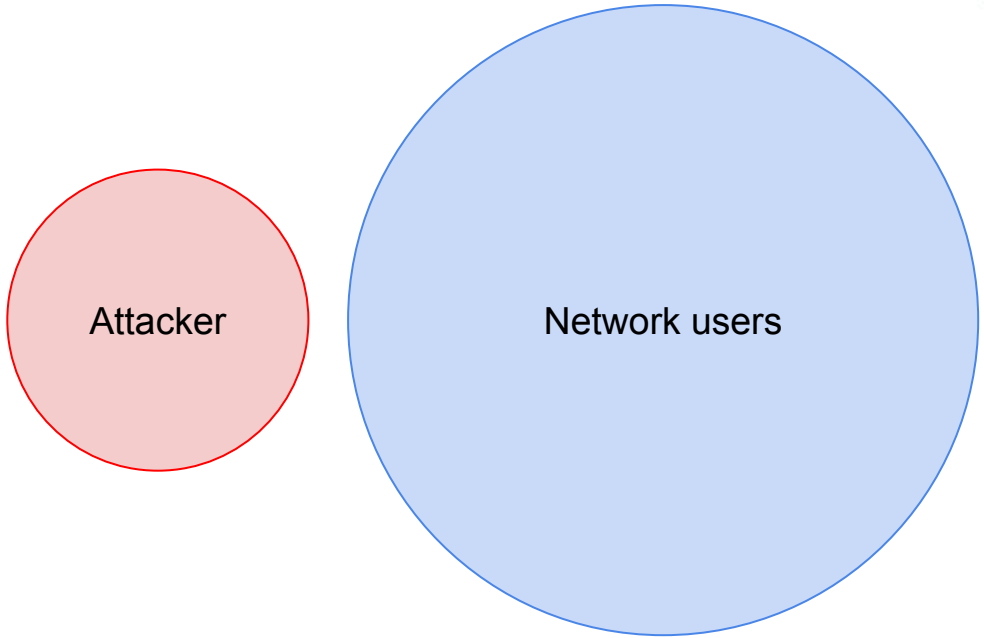
51% Attacks

This mechanism (called **proof-of-work**) relies on it being **very difficult** to edit the blockchain



51% Attacks

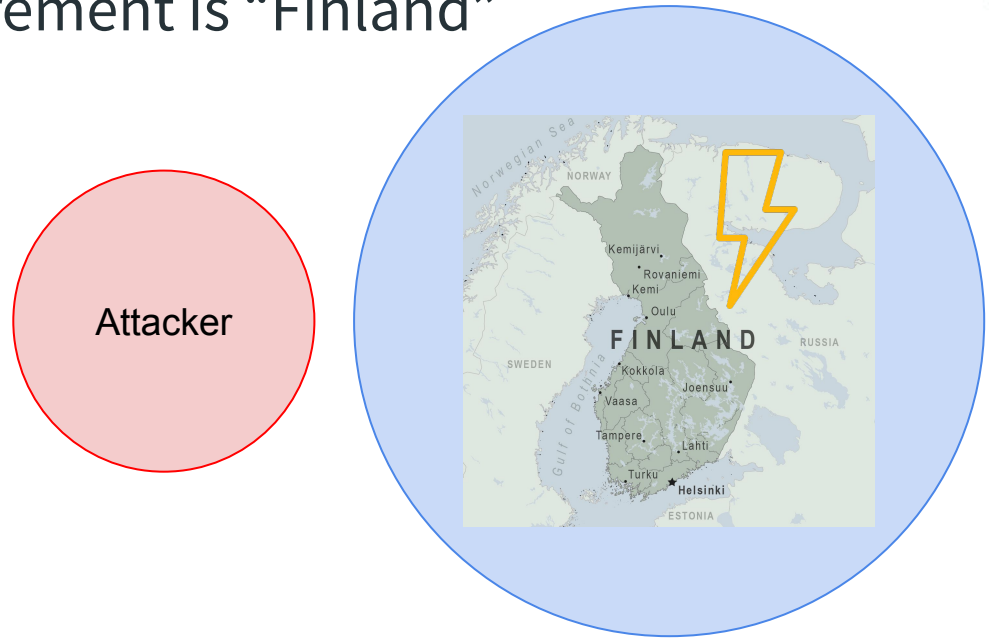
Requirement: The attacker **<<<** the rest of the network



51% Attacks

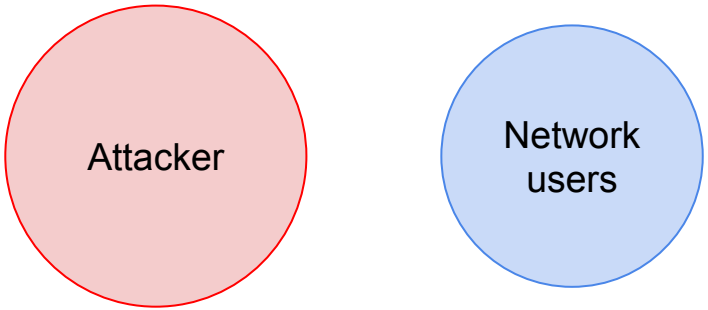
Requirement: The attacker **<<<** the rest of the network

- Easy if energy requirement is “Finland”



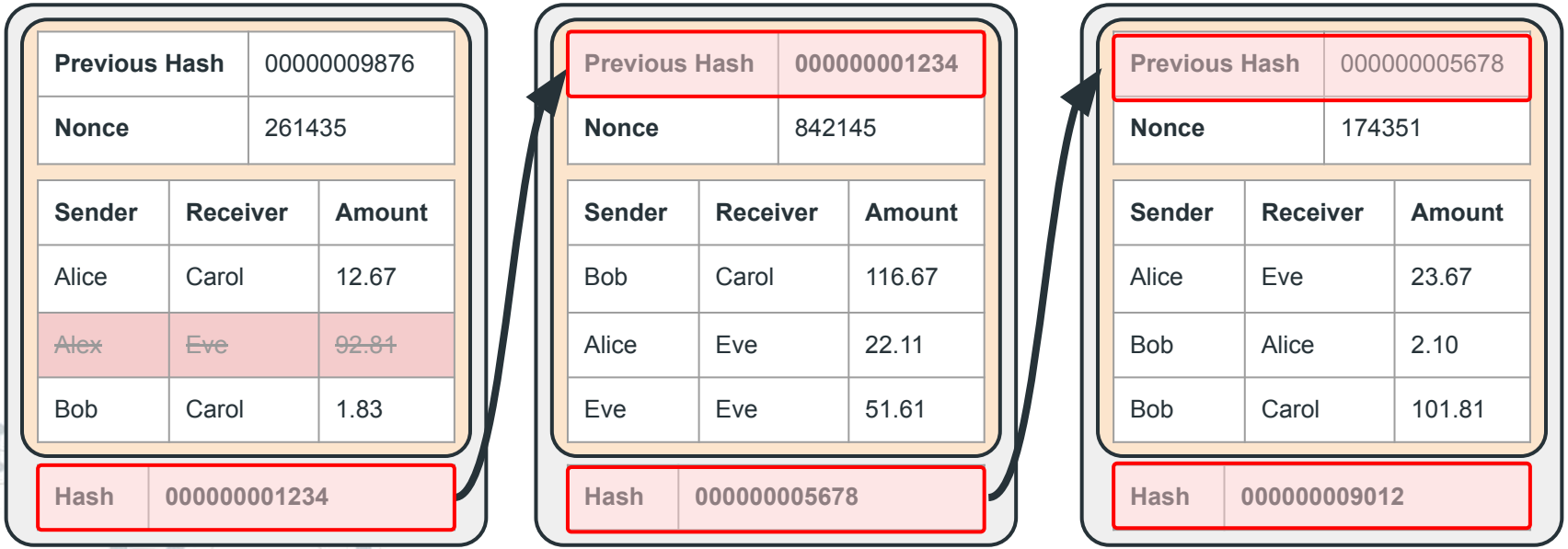
51% Attacks

But what about smaller coins?



51% Attacks

An attacker with enough power can recalculate these hashes



Previous Hash	00000009876
Nonce	261435

Sender	Receiver	Amount
Alice	Carol	12.67
~~Alex~~	~~Eve~~	~~92.81~~
Bob	Carol	1.83

Hash	000000001234

Previous Hash	000000001234
Nonce	842145

Sender	Receiver	Amount
Bob	Carol	116.67
Alice	Eve	22.11
Eve	Eve	51.61

Hash	000000005678

Previous Hash	000000005678
Nonce	174351

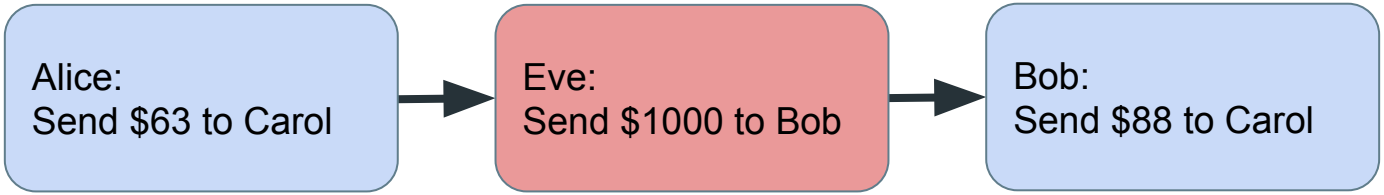
Sender	Receiver	Amount
Alice	Eve	23.67
Bob	Alice	2.10
Bob	Carol	101.81

Hash	000000009012

51% Attacks

Double-spend (or, 51% attack)

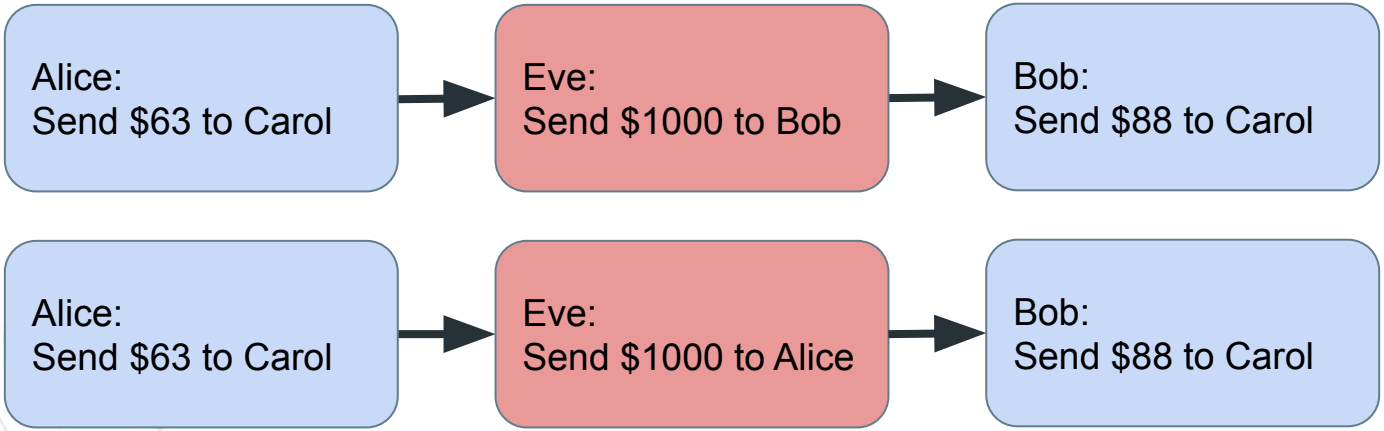
1. Spend money



51% Attacks

Double-spend (or, 51% attack)

1. Spend money
2. Rebuild a “fake” chain with a **different** spend



51% Attacks

ATTACK (COMPUTING)

Bitcoin Gold hit by 51% attacks, $72K in cryptocurrency double-spent

Smaller Proof-of-Work networks are prone to these incidents

https://thenextweb.com/news/bitcoin-gold-51-percent-attack-blockchain-reorg-cryptocurrency-binance-exchange

Ethereum Classic hackers steal over $1.1M with 51% attacks

Decentralized networks aren't always as decentralized as they seem

https://thenextweb.com/news/ehtereum-classic-51-percent-attack

Almost $500,000 in Ethereum Classic coin stolen by forking its blockchain

Rollback attack let attackers spend 88,500 previously spent coins.

https://arstechnica.com/information-technology/2019/01/almost-500000-in-ethereum-coin-stolen-by-forking-its-blockchain/

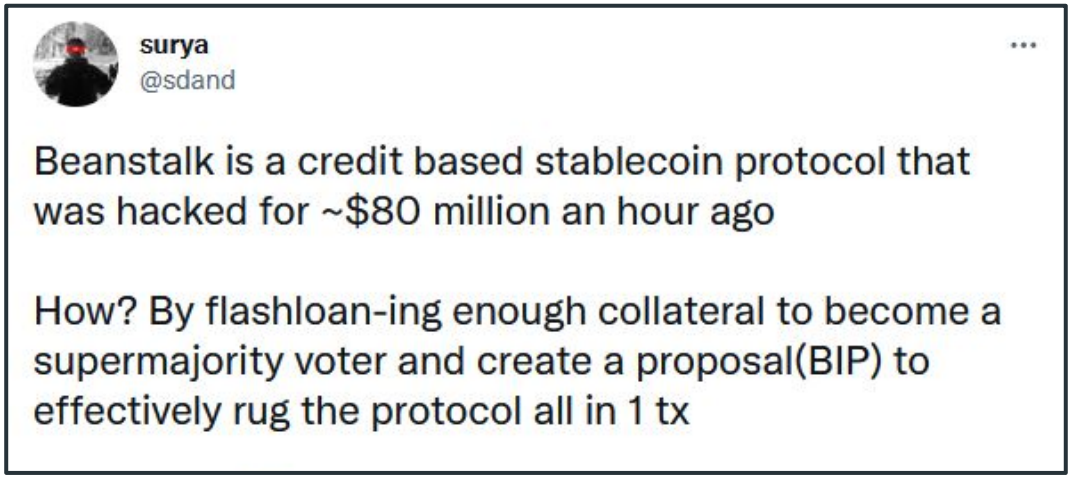
51% Attacks

I know someone is thinking: Proof-of-stake solves this!

51% Attacks

I know someone is thinking: Proof-of-stake solves this!

It's out of scope, but the short answer is "not entirely"

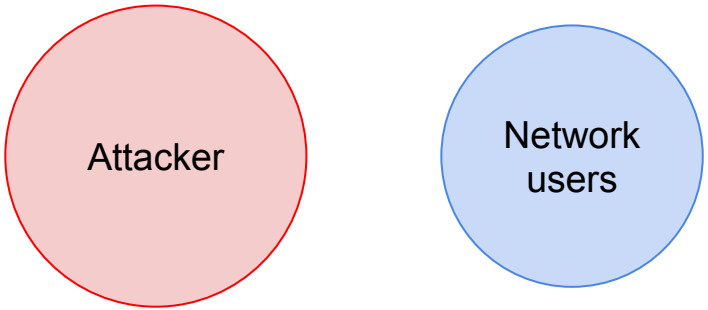


https://twitter.com/sdand/status/1515695132502380545

51% Attacks

Takeaway:

Small chains with few users are less secure



No moderation

Another risk: No moderation

- A bank **can** undo fraudulent charges
- A blockchain **cannot**

No moderation

Irreversible problems:

- Scams and phishing
- Mistakes
- Bugs

https://twitter.com/TylerGlaiel/status/1487925938834661377

No moderation

toddkramer.eth
@toddkramer1

I been hacked.
all my apes gone. this just sold please help me

2:10 AM · Dec 30, 2021 · Twitter Web App

“Around 20 percent [of bitcoin] appear to be in lost or otherwise stranded wallets”

https://www.nytimes.com/2021/01/13/business/tens-of-billions-worth-of-bitcoin-have-been-locked-by-people-who-forgot-their-key.html

No moderation

Mistakes are security risks too!

$220M in Bitcoin May Be Encrypted Forever on IronKey

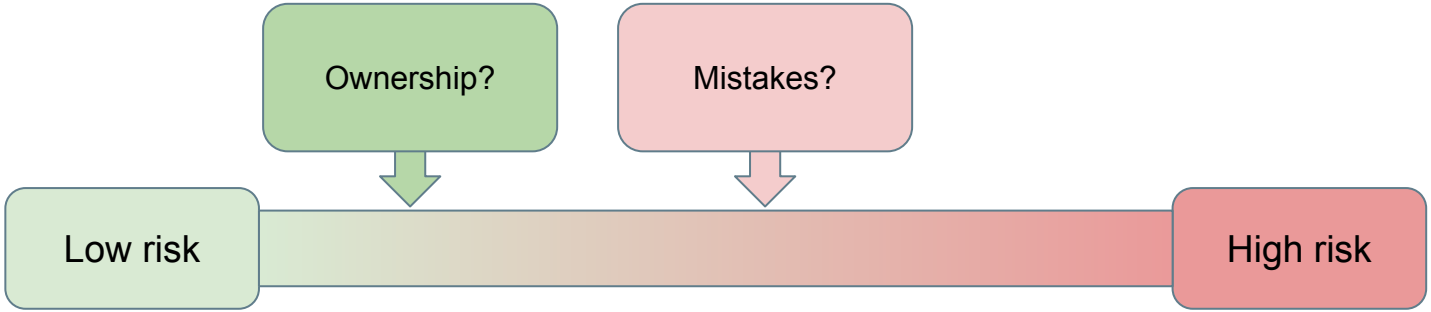
FIPS Certified Tamperproof Hardware Encryption Proves Unbreakable after 10 Years

https://ciphertrace.com/220m-in-bitcoin-encrypted-forever-on-ironkey/

No moderation

Takeaway:

Be aware of the risks. Threat model!




THE UGLY

Security Theater

Using the blockchain requires:

- Time
- Effort
- Technical knowledge

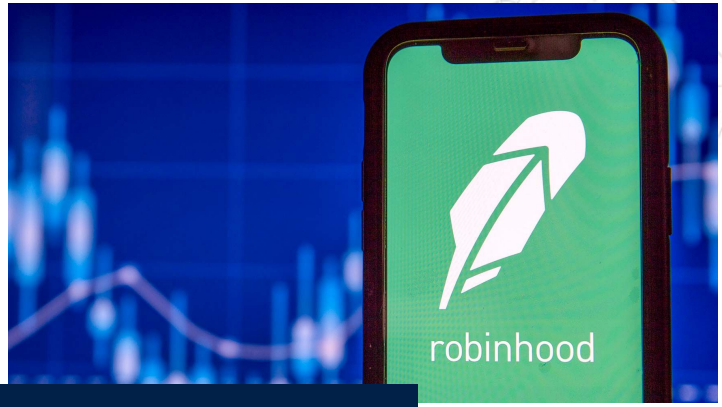
Security Theater

Using the blockchain requires:

- Time
- Effort
- Technical knowledge

…so people don’t!

Security Theater



BitMart

Security Theater

This is not decentralized!

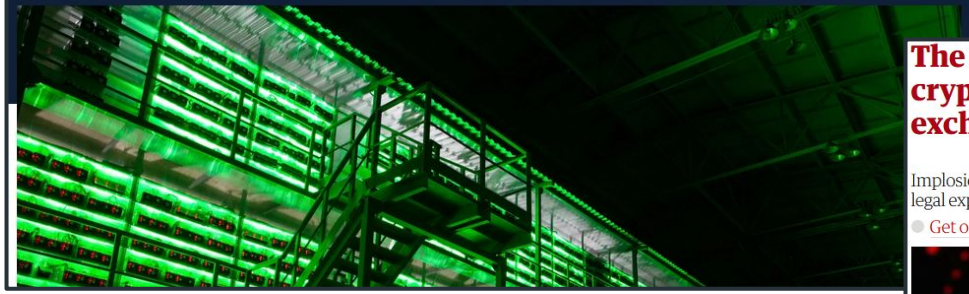
Security Theater

This is not decentralized!

Security Theater

Crypto exchanges keep getting hacked, and there's little anyone can do

One of the biggest heists happened this month, when the crypto trading platform Bitmart said hackers stole almost $200 million after they broke into a company account.



https://www.nbcnews.com/tech/security/bitcoin-crypto-exchange-hacks-little-anyone-can-do-rcna7870

Crypto.com admits over $30 million stolen by hackers

In a new blog post the company said that 4,836 ETH and 443 bitcoin were taken

By Corin Faife | @corintxt | Jan 20, 2022, 8:23am EST

SHARE

https://www.theverge.com/2022/1/20/22892958/crypto-com-exchange-hack-bitcoin-ethereum-security

The search is on for $50m in lost cryptocurrency after two Australian exchanges collapse

Implosion of online trading hubs highlights pitfalls of what one legal expert describes as 'tulipmania' investments

Get our free news app; get our morning email briefing

https://www.theguardian.com/technology/2021/dec/12/the-search-is-on-for-50m-in-lost-cryptocurrency-after-two-australian-exchanges-collapse

Security Theater

Using a crypto exchange is **not** using the blockchain

Ask yourself:

Who has my private key?

Recap

Blockchain pros:

- No “owner” with total control

Blockchain cons:

- Transactions can be faked with enough power
- Mistakes cannot be undone
- Requires technical knowledge to use properly

Recap

General advice:

- Avoid small blockchains
- Be extra careful of scams
- Do not use a crypto exchange
  - Unless you do not care about using the blockchain

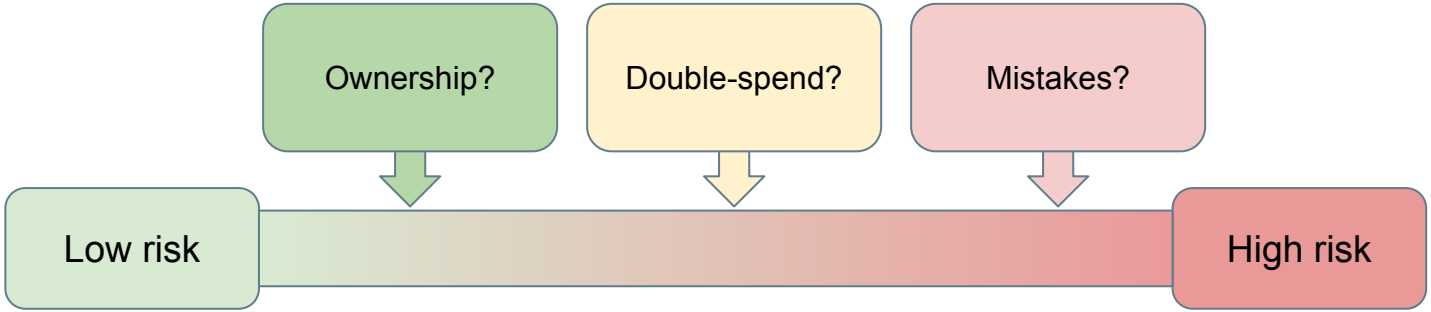
Recap

General advice:

- Avoid small blockchains
- Be extra careful of scams
- Do not use a crypto exchange

Problem: Ownership

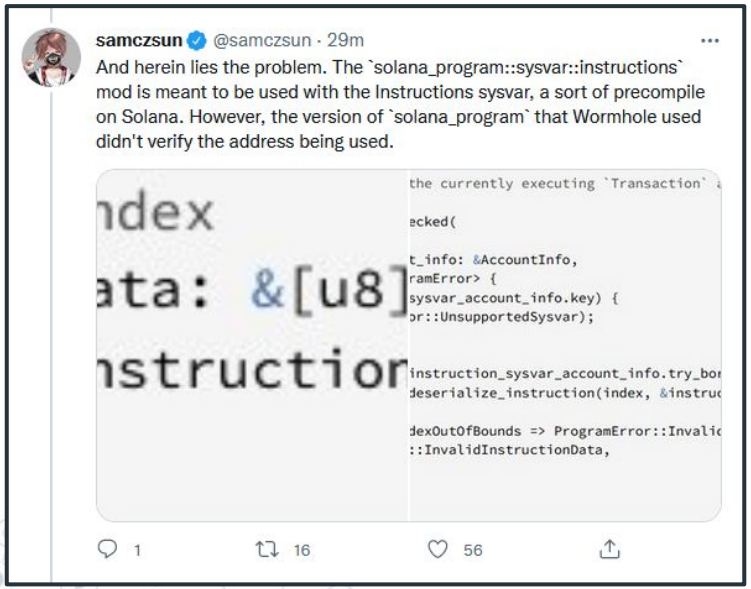
Everyone has a different threat model!



Questions?

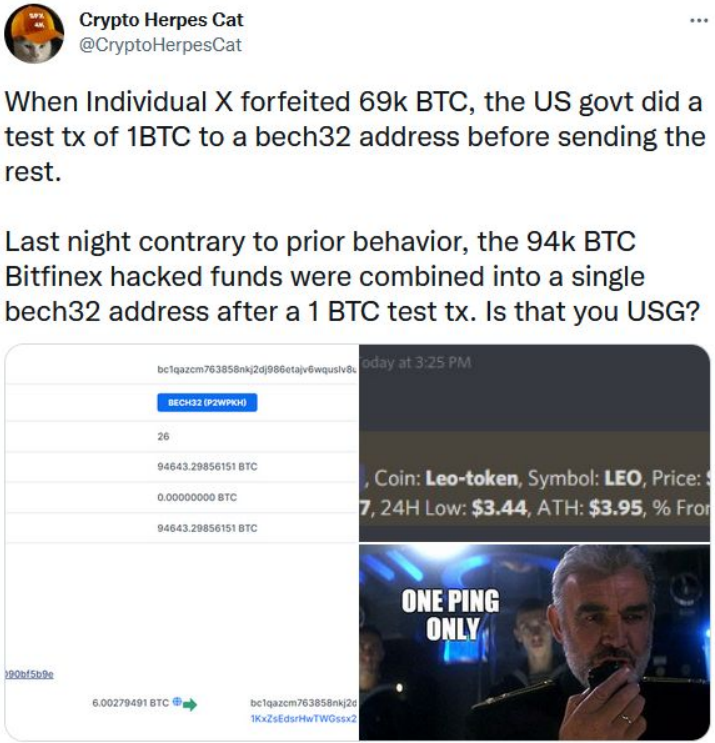
Permanence

This includes bugs in Blockchain code…



https://twitter.com/samczsun/status/1488974372756987906

https://twitter.com/sdand/status/1515695132502380545



https://twitter.com/CryptoHerpesCat/status/1488534656538533888

6. The 2017 transfers notwithstanding, the majority of the stolen funds remained in Wallet 1CGA4s from August 2016 until January 31, 2022. On January 31, 2022, law enforcement gained access to Wallet 1CGA4s by decrypting a file saved to LICHTENSTEIN's cloud storage account,[8] which had been obtained pursuant to a search warrant. The file contained a list of 2,000 virtual currency addresses, along with corresponding private keys.[9] Blockchain analysis confirmed that almost all[10] of those addresses were directly linked to the hack. Between January

Cops: 'Ethical Hacker' Was Anything But

Aaron Motta of Florida accused of robbing customer of nearly $600K in cryptocurrency

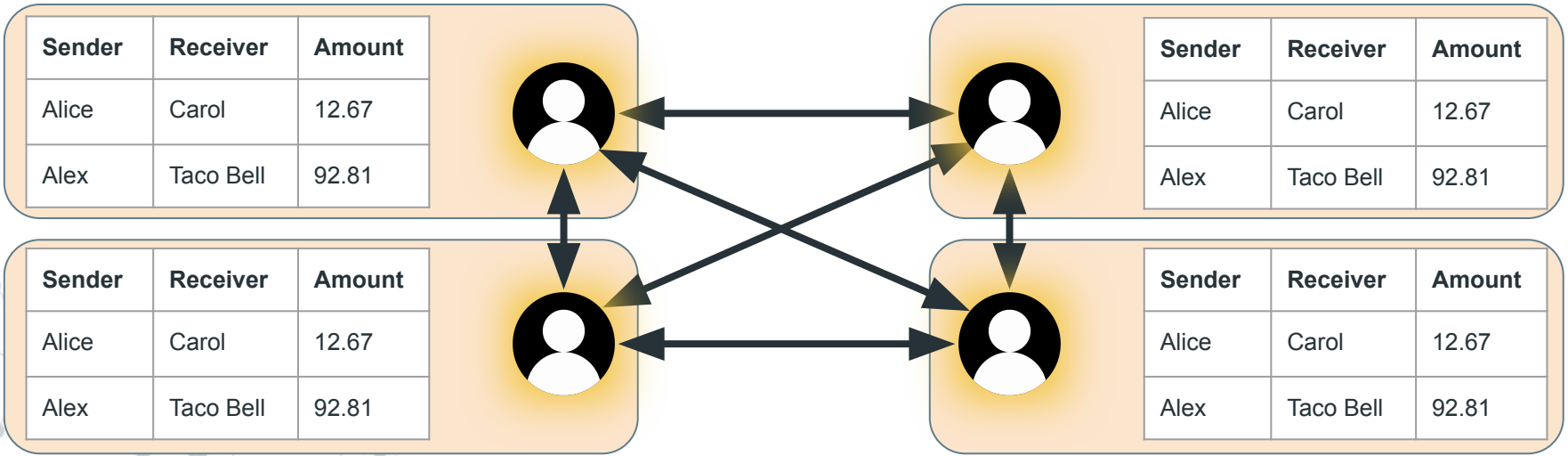
By John Johnson, Newser Staff
Posted Apr 11, 2022 2:30 AM CDT

Aaron Daniel Motta. (Pinellas County Sheriff's Office)

https://www.newser.com/story/319147/cops-ethical-hacker-was-anything-but.html

“Motta tried to cover his tracks by making multiple transactions, but authorities were able to track the $575,910 to his wallets”

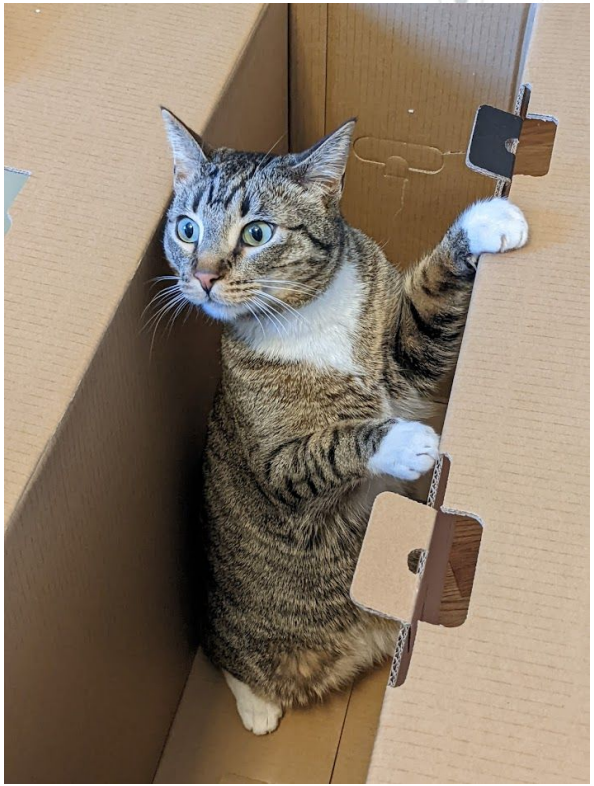
Problem #1: Cost



Problem #1: Cost

This 5.3KB photo costs:

$0.0002 on a $100 2TB hard drive



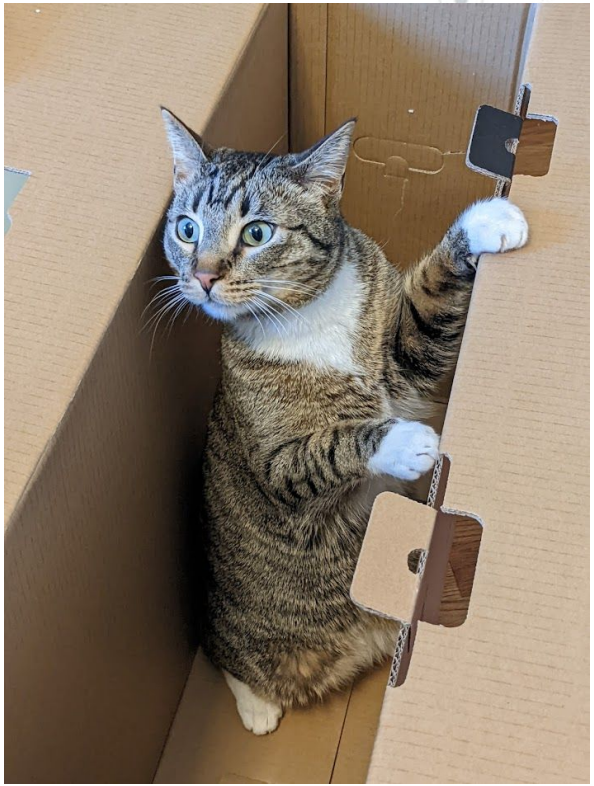
Problem #1: Cost

This 5.3KB photo costs:

$0.0002 on a $100 2TB hard drive

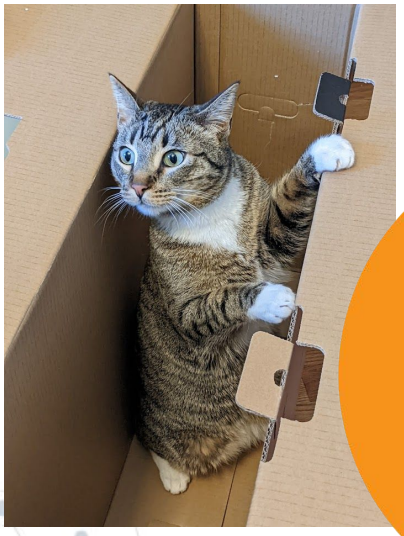
$70,000 on the Etherium blockchain

(as of 2019: ethereum.stackexchange.com/a/74260)



Beyond Bitcoin

Blockchains can also store money, images, code, etc!




```
{
    "image": "https://gateway.pinata.cloud/ipfs/Qmb86L8mUphwJGzLPwXNTRiK1S4scBdj9cc2Sev3s8uLiB/0.png",
    "tokenId": 0,
    "name": "NFT_CREATOR 0",
    "attributes": [
        {
            "trait_type": "Face",
            "value": "White"
        },
        {
            "trait_type": "Eyes",
            "value": "regular"
        },
        {
            "trait_type": "Ears",
            "value": "ears1"
        },
        {
            "trait_type": "Hair",
            "value": "hair7"
        },
        {
            "trait_type": "Nose",
            "value": "n2"
        },
        {
            "trait_type": "Mouth",
            "value": "m4"
        }
```