Welcome to Blockchain Development and Fintech

Martinet Lee

Martinet Lee

Senior Research Engineer / Auditor

Head of Developer Relations

Quantstamp

Cofounder Zircuit

Technical Experience

Audited more than 50+ projects, from Defi, NFT, to Layer 1s including Yearn, ETH2, Avalanche.

Technical lead of Zircuit Ecosystem
- Developed Smart Contracts that hosted 2B USD assets at the peak.
- Leading the internal Chain Abstraction and Account Abstraction research & efforts

/Why are we here?

/Goal of the course

- Provide a rudimentary technical understanding of blockchain
- Overview of Decentralized Finance
- Ability to develop smart contracts

/The course is NOT about

- Investment Advice
- How to trade crypto
- Hedge / Quant

/Tentative Schedule

DATE	Topic
02-24	Intro to cryptography and cryptocurrencies + Bitcoin 101 Introduction to Solidity (solc, hardhat/foundry)
03-03	Infrastructure of Blockchain
03-10	The Standards of Assets
03-17	Introduction to EVM
03-24	Stablecoins
03-31	Lending Protocol & Flashloan

/Tentative Schedule

DATE	Topic
04-07	Tentative Guest Speaker (Nikita Belenkov, from Anza - Solana R&D company), **Midterm Proposal Draft Submission**
04-14	(Tentatively OFF - Midterm Week!)
04-21	Security Audits & Bridge Overview,
04-28	Onsite Lab, **Midterm Proposal Finalize**
05-05	Account Abstraction
05-12	MEV

/Tentative Schedule

DATE	Topic
05-19	(TBD)
05-26	(TBD)
06-02	Final Project Presentations (TBD) **Final Project Deadline**
06-10	Final Project Presentations (TBD)

/Expectations

Prerequisite

- Data structure, Algorithm
- Proficient English

Attitude

- Active in class: ask & discuss
- Hands-on: Buidl, buidl, buidl
- Don’t about score too much, but care about the real value.

/Grading

Lab (35%)

- Every week there will be an assignment that will be due in 1 week.

Class Participation, Quiz, and hackathon participation (30%)

- We will have a discord community, activities there would also be taken into account.

Final Project (35%)

- Not necessarily in Solidity. E.g. Audit in competition. Can consider doing some bounty, or expanding on hackathon project. **Earn money while doing project at the same time!**

- Flexible on the content, discuss with me as early as possible.

/Policy

AI tools are allowed, but has to be disclosed.

- AI is a new tool. Of course you are allowed to use it. However its usage has to be disclosed.
- **You have to understand thoroughly of whatever material you submitted.**

Disclosure:
the logo of this course is produced by **MidJourney** ;)

No Plagiarism

- No copying reports / texts from others. No copying assignment solutions. Looking at the code and typing yourself is obviously also plagiarism.

- There is a **non-negotiable "FAIL"** if plagiarism is being detected. **I will not let you drop the course.**

/Warnings

- **Load will be HEAVY.** The course is aiming to give you as much training as possible to be equipped for the industry. We're not just playing house.
- **Schedule and Grading is subject to change.** This flexibility is reserved to allow the course to adapt to your ability. Feedbacks are welcome. There are also topics that I'd really like to fit in but is not in the current plan (e.g. smart contract security & audits).

/Who should drop

- Does not have background in data structure and algorithm
- 1st - 3rd year bachelor student
  - There can be exceptions, but you need to convince me with your past experience.
- Only cares about what to buy or sell
  - this sort of questions will have negative impact on course participation as it is wasting everyone’s time
- Does not consider plagiarism as a shameful behaviour
- Cannot follow up with lectures and discussion in English
- Needs course to be stable and fixed

/Finally, Logistics for additional sign-ups

I would love to have you here if you :

- Have Security background (provide CV)
- Have Cryptography background (provide CV)
- Already knows about blockchain / Solidity (provide GitHub & quick chat)
- Can have insightful discussion / questions during the lecture
- Can persuade me otherwise. (come talk to me)

Sign-ups have to:

- Complete the assignments even if the additional sign-up situation is unclear

/There are still a TON that are not covered

There are only 12 lectures so we cannot cover:

- Defi
  - Leverage
  - Derivatives
  - …(etc)
- NFTs
  - Marketplaces
  - NFTFi (Fractionalization, liquid market)
- Cross-chain Communication and value transfer (bridges)
- Secure Smart Contract Development
- Security Auditing
- MEV
- Privacy
- Different types of Consensus
- UI/UX
- … (etc)

<Ready?>

Time cannot be wasted.

“One day in the crypto world is like one year in real life.”

Introduction to Cryptography & Cryptocurrency

Martinet Lee

/What is Blockchain?

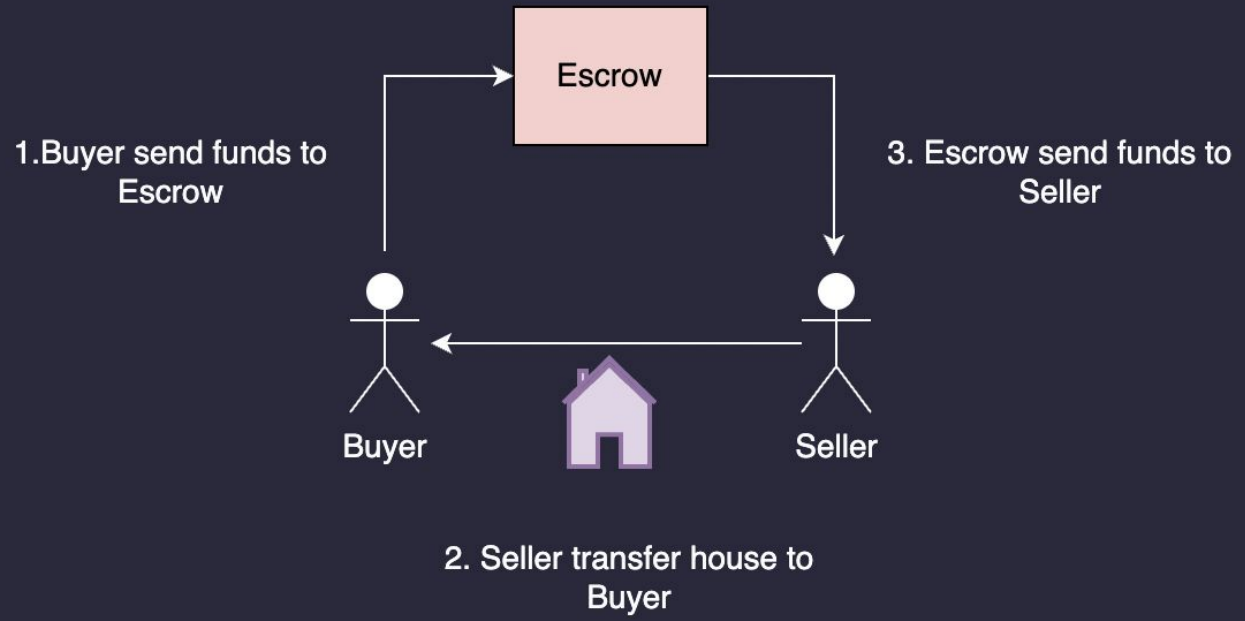
Technically:

- Public append-only data structure
- “Immutable”?
- Can run programs or scripts

Value-wise:

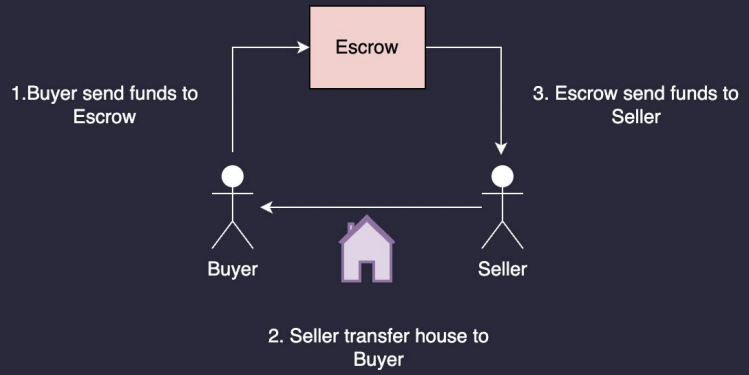
- Facilitating coordination between parties

/Example: Buying a real-estate



/Example: Buying a real-estate

- Also, how do you transfer the “house”?
- How do you transfer your “funds”?



/How large is the industry?

Bitcoin BTC	Buy	$63,202.09	0.1%	3.9%	7.3%	$49,927,167,514	$1,263,660,814,581	
☆	9	Broadcom AVGO	$1.566 T	$330.34	0.69%		USA	
☆	10	Tesla TSLA	$1.500 T	$399.83	2.91%		USA	
☆	11	Berkshire Hathaway BRK-B	$1.065 T	$494.09	0.82%		USA	
☆	12	Walmart WMT	$1.003 T	$125.81	2.29%		USA	

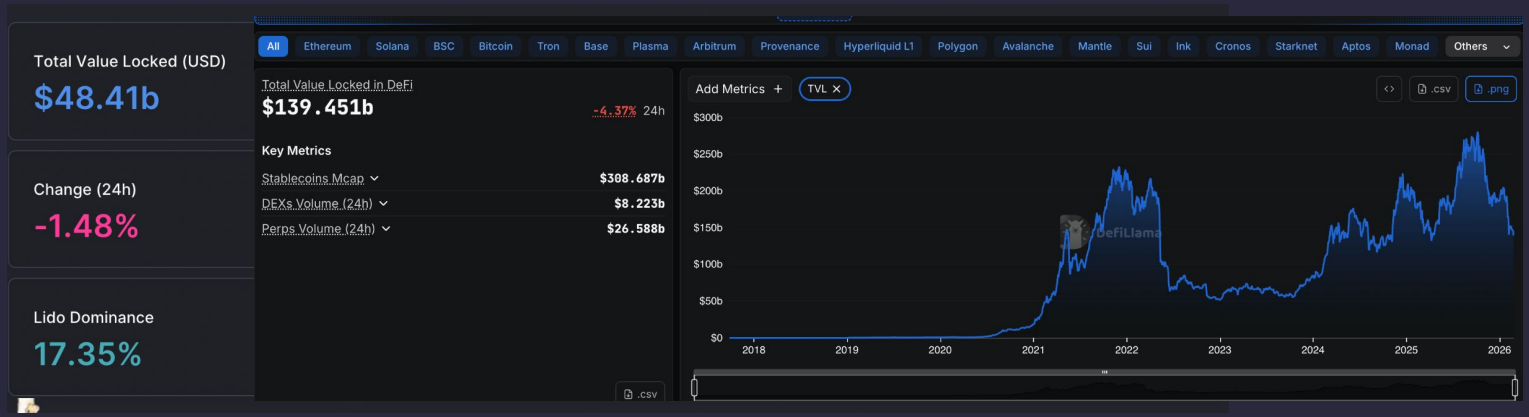
/How large is the industry?

73	Shell SHEL	$225.48 B	$79.97	▲ 0.24%	
74	Siemens SIE.DE	$222.08 B	$283.55	▼ 1.84%	
75	American Express AXP	$221.28 B	$321.24	▼ 7.20%	
76	China Mobile 0941.HK	$221.11 B	$10.10	▼ 0.57%	
77	Intel INTC	$217.93 B	$43.63	▼ 1.09%	
78	Mitsubishi UFJ Financial MUFG	$215.38 B	$19.04	▼ 1.65%	
79	Reliance Industries RELIANCE.NS	$211.62 B	$15.64	▼ 0.39%	
80	Commonwealth Bank CBA.AX	$210.98 B	$126.18	▼ 0.02%	

Ethereum ETH	Buy	$1,823.19	▼ 0.3%	▼ 2.9%	▼ 8.0%	$21,408,334,482	$220,006,460,641

Source: Companies Marketcap

/How large is the industry? (2023 v.s. 2026)



Source: Defillama

Circulating Supply

41.97 B USDC

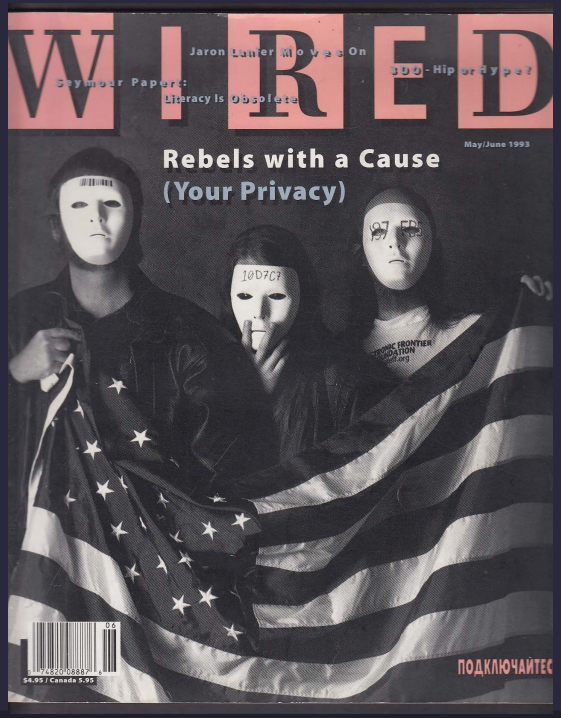
74,737,129,289

Circulating Supply

68.06 B USDT

183,624,238,441

/Back to the roots - Bitcoin. Why?



“Privacy is necessary for an open society in the electronic age.”

“When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must _always_ reveal myself. Therefore, **privacy in an open society requires anonymous transaction systems.** Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.”

A Cypherpunk’s Manifesto - Eric Hughes, 1993

/Back to the roots - Bitcoin. Why?

THE TIMES

Max 5C, min -5C

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Michael Sheen Frost, Nixon and me

Magazine

Working mums So that's how she does it

Body&Soul

Detox in style The best spas on the planet

Travel

Salman Rushdie I won't marry again

Pages 22, 23

Giant killing? Guide to the FA Cup third round

Sport

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

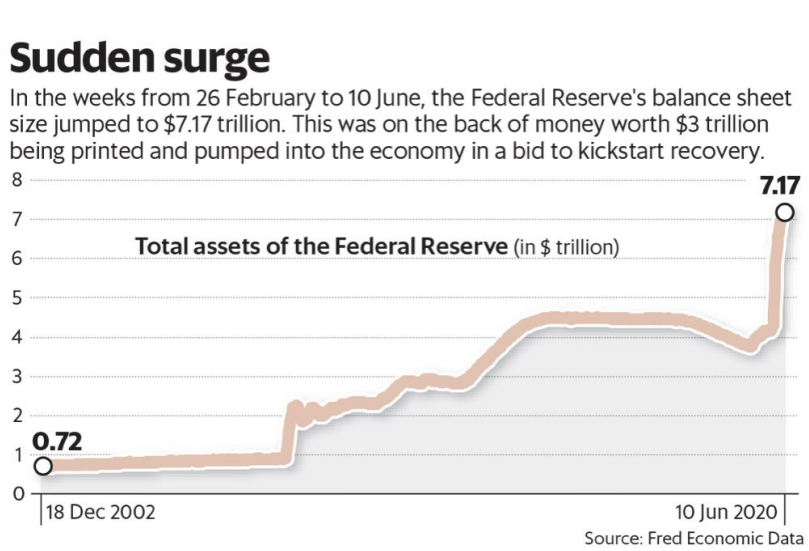
99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

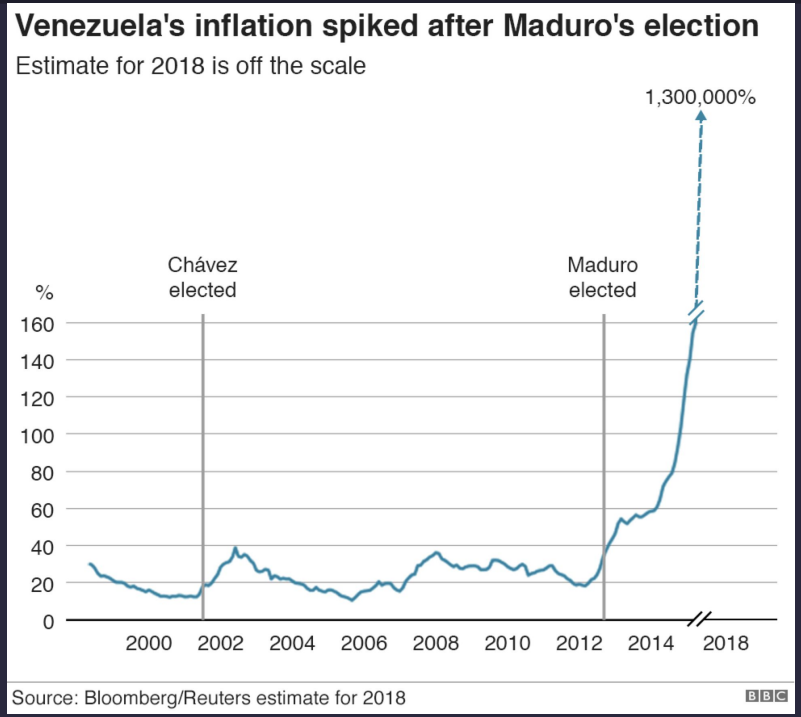
Business, page 47

What happens in a bailout?

/Back to the roots - Bitcoin. Why?

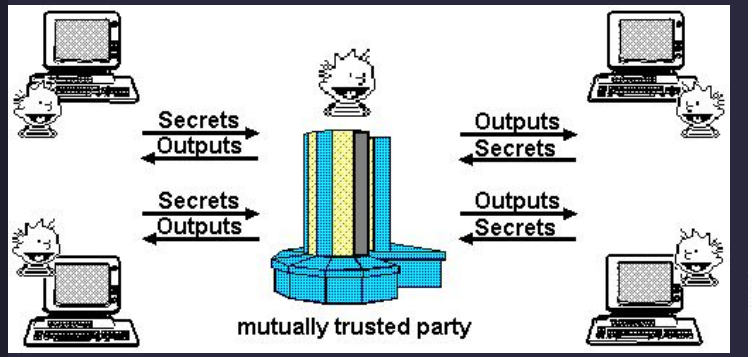


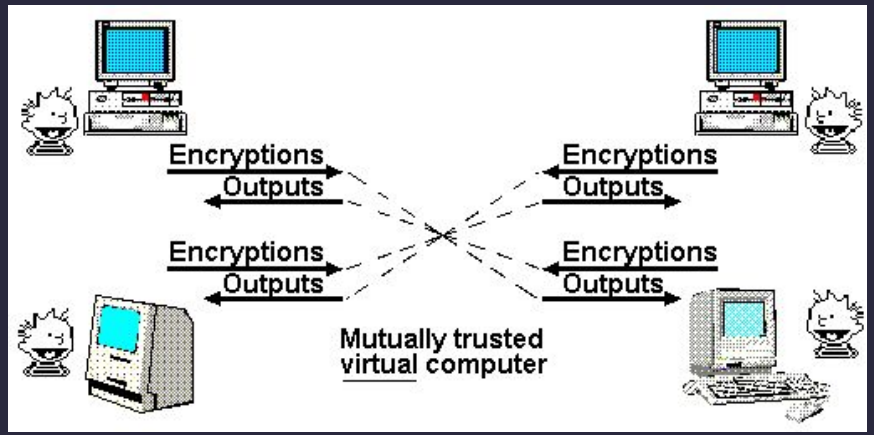
/Back to the roots - Bitcoin. Why?



Is it possible to remove the “Trusted Party”?

/The God Protocol - Nick Szabo 1997

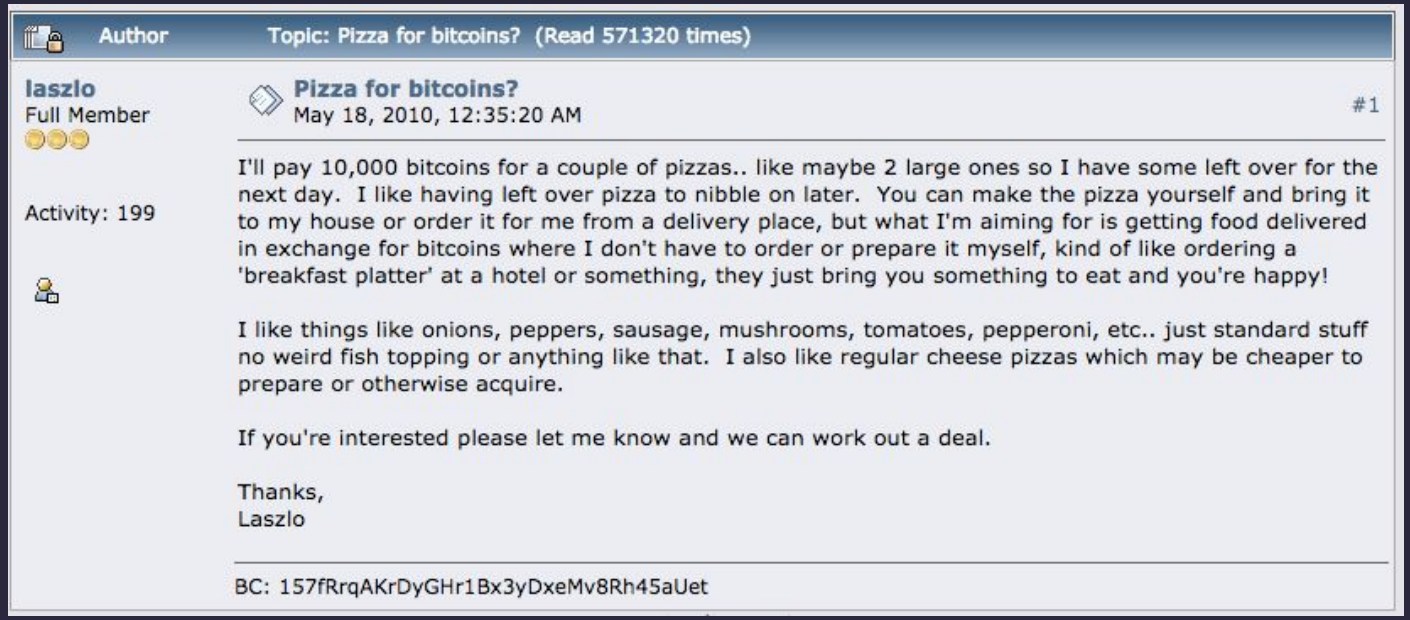




/Bitcoin, How? The technical history

- “DigiCash”, David Chaum, 1989
- “CyberCash”, Lynch, 1994
- “Hashcash”, Adam Back, 1997
- “Bit Gold”, Nick Szabo, 1998
- “b-money”, Wei Dai, 1998
- "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto, 2008

/The first real transaction of Bitcoin



Author | Topic: Pizza for bitcoins? (Read 571320 times)

laszlo
Full Member

Activity: 199

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM #1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

Source: bitcointalk.org

/Bitcoin has died...

Bitcoin Obituaries

Bitcoin has died 471 times

Source: 99bitcoins.com/bitcoin-obituaries
Image source: cryptoart.com

/What is Blockchain? (recap)

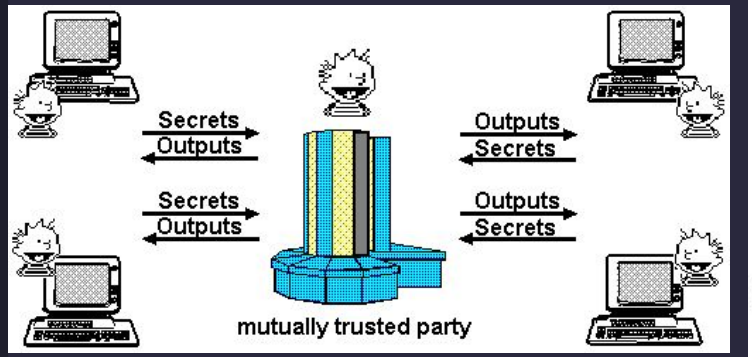
Technically:

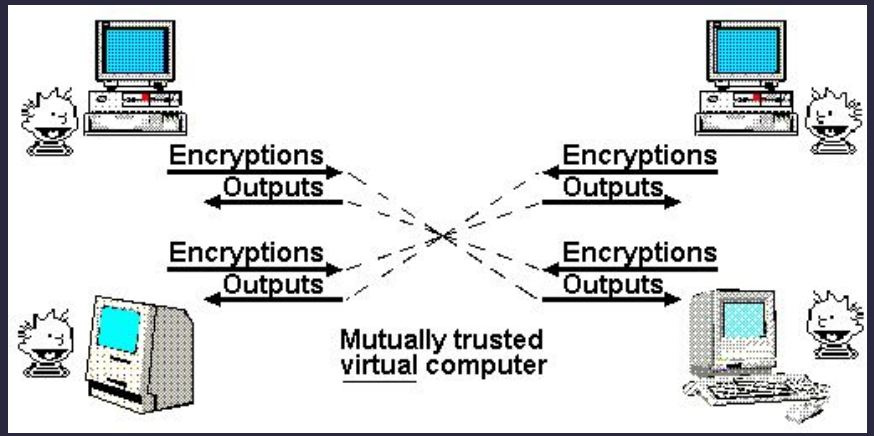
- Public append-only data structure
- “Immutable”?
- Can run programs or scripts

Value-wise:

- Facilitating coordination between parties

/What is Blockchain? Another perspective





- Mutually Trusted “Virtual” Machine

/How does a shared virtual machine work?

A computer / machine: A state machine + transition logic. You control your input to the state machine.

A virtual machine: You could emulate a machine in a physical machine. Typically you control the input.

For a “shared” virtual machine:

- The virtual machine still runs in your physical machine.
- You do NOT control the input. You receives the input and the virtual machine executes it.

/Challenges

- How do we perform identity verification? How do we know if an account really does have the intent to do something?
- How to agree on a simulation result across a trust-less / distributed system?
- How to construct a reliable network?
- How to make this whole thing “Permissionless”?

/Technical Foundations of Blockchain

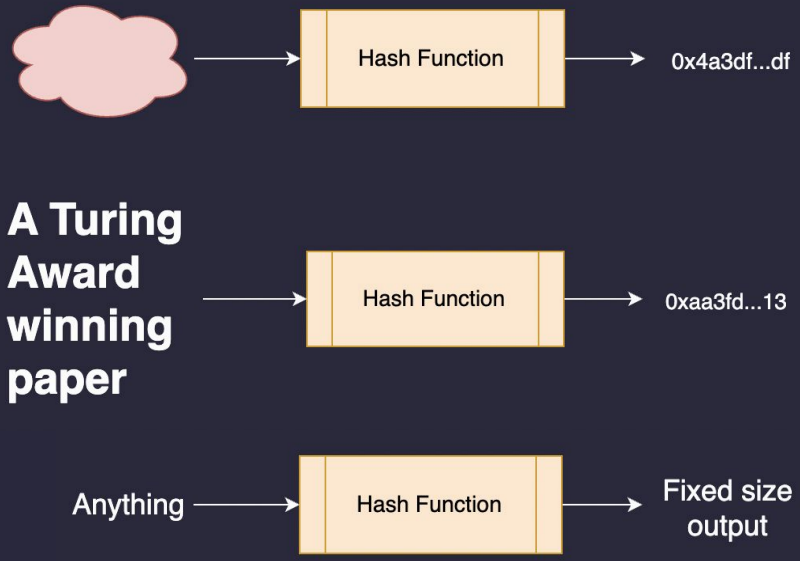
- How do we perform identity verification? How do we know if an account really does have the intent to do something? ⇒ **Cryptography**
- How to agree on a simulation result across a trustless / distributed system? and Permissionless? ⇒ **Innovative Consensus Algorithm**
- How to construct a reliable network? ⇒ **Peer to Peer Network**

/Cryptography (schemes that are useful in blockchain)

- Hash function
  - Merkle Tree
  - Proof of Work
- Public Key Cryptography
  - Digital Signature
- *(Zero-Knowledge Proofs)*
- *(Homomorphic Encryption)*
- *(Multi-Party Computation)*
- *(Threshold Signature)*

<Cryptography>

/Hash function



Given input of any size, a hash function outputs a fixed length of bits.

Important properties:

- Given a hash, should not be easy to find a message that produces the hash.
- Given a message, should not be easy to find another message that produces the same hash.
- Should be hard to find any message pair that produces the same hash.

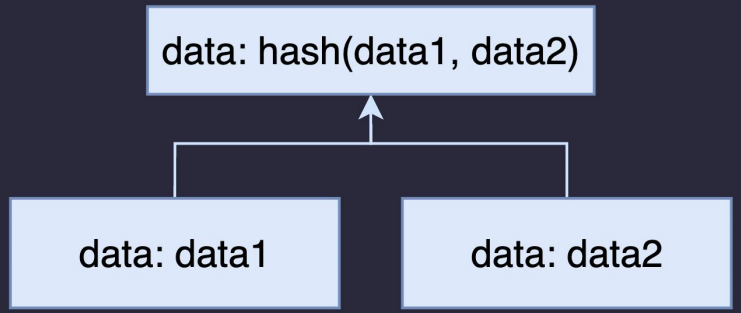
/Applications of Hash function

- Digest
  - File download check
  - Used when signing large chunks of data
  - Merkle Tree (a super useful data structure!)
- Commit Reveal Scheme

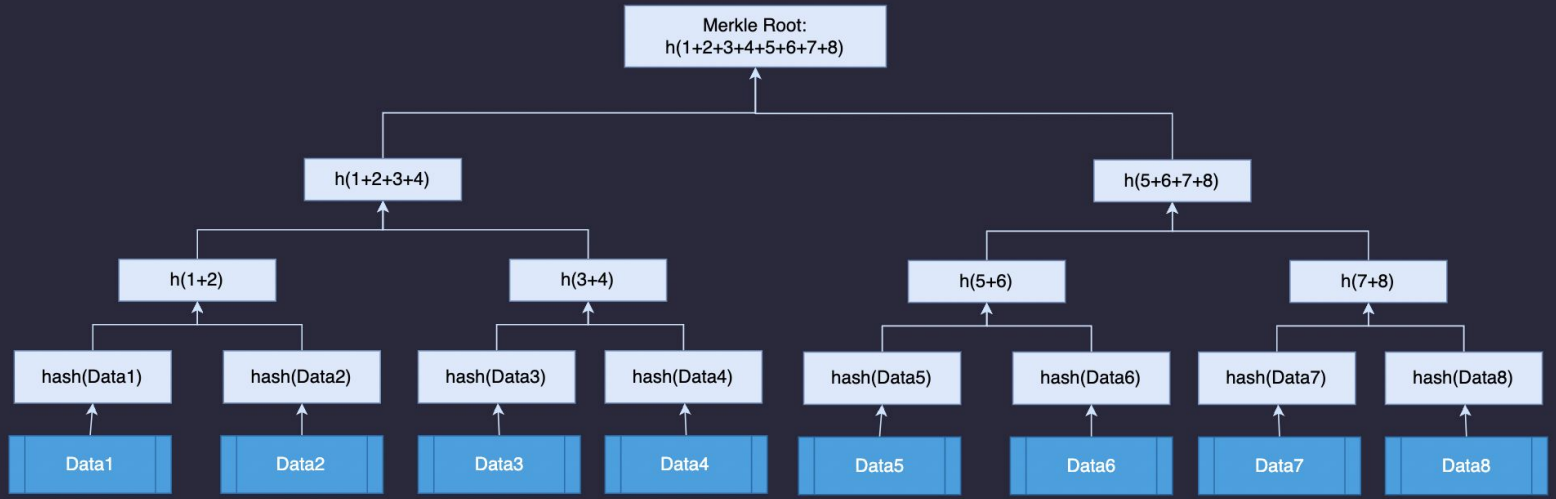
/Merkle Tree

A Merkle Tree is a **tree** where each node has additional data which is being constructed in a special way.

- `thisNode.data = hash( leftChild.data | rightChild.data )`



/Merkle Tree

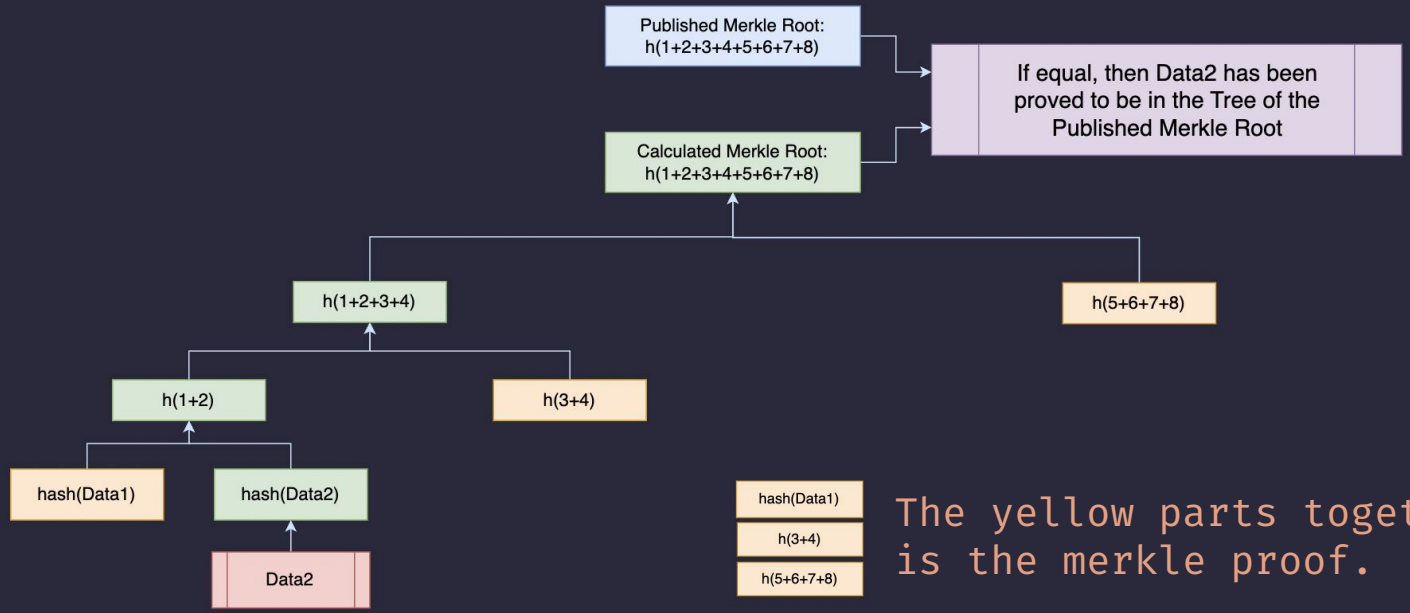

Merkle Root:
h(1+2+3+4+5+6+7+8)
h(1+2+3+4)
h(5+6+7+8)
h(1+2)
h(3+4)
h(5+6)
h(7+8)
hash(Data1)
hash(Data2)
hash(Data3)
hash(Data4)
hash(Data5)
hash(Data6)
hash(Data7)
hash(Data8)
Data1
Data2
Data3
Data4
Data5
Data6
Data7
Data8

/Merkle Tree

With Merkle Root, we don’t need to publish the whole tree, but just the root.

Now let’s say I want to prove Data2 exists in the tree associated with the Merkle root that was published. Wat do?

/Merkle Proof



The yellow parts together is the merkle proof.

/Applications of Merkle Tree in Blockchain

Data storage on Blockchain is very very expensive. (why?)

Merkle Tree is an efficient way to store a large quantity of data with the cost of later computation.

Applications:

- Aggregating transactions
- Storing state
- airdrops/reward claiming
- Proof of liability
- ..

/Public Key Cryptography

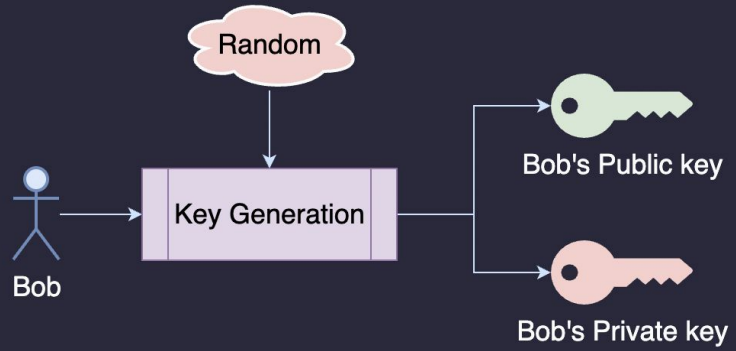
Quick survey:

- How many people know about public key cryptography; symmetric encryption v.s. Asymmetric encryption?

/Public Key Cryptography - Key Generation

Anyone can generate a pair of keys with random inputs

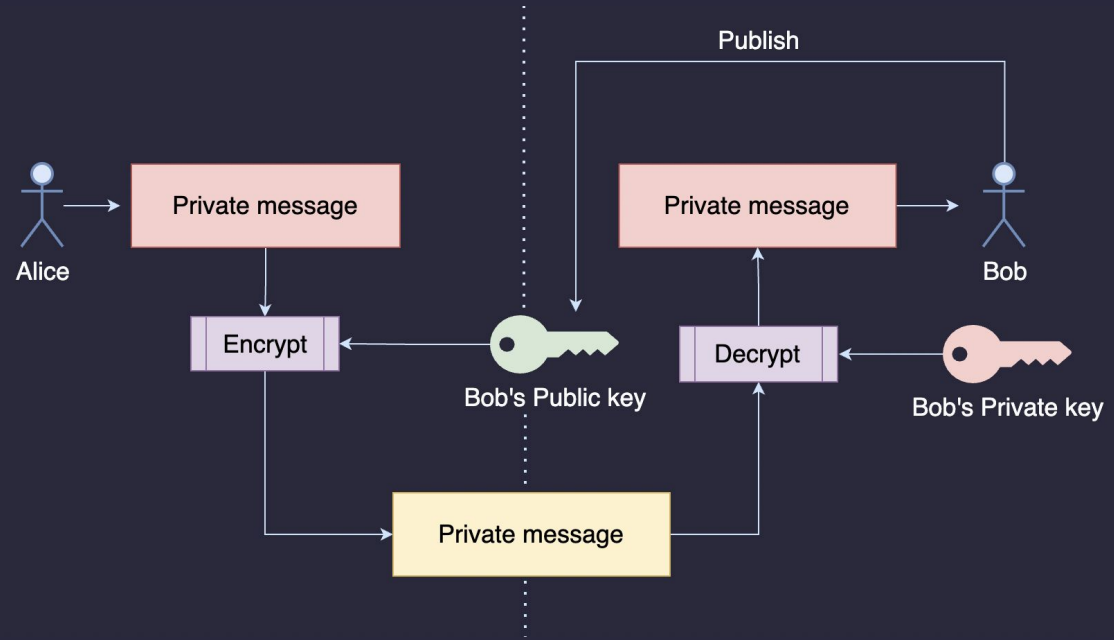
- Public key
- Private key



https://www.kerryveenstra.com/cryptosystem.html

/Public Key Cryptography - Encryption / Decryption

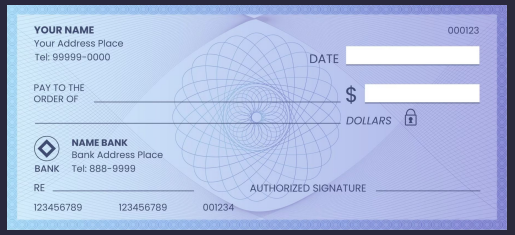
Bob publishes his public key so that others can use it to encrypt message.

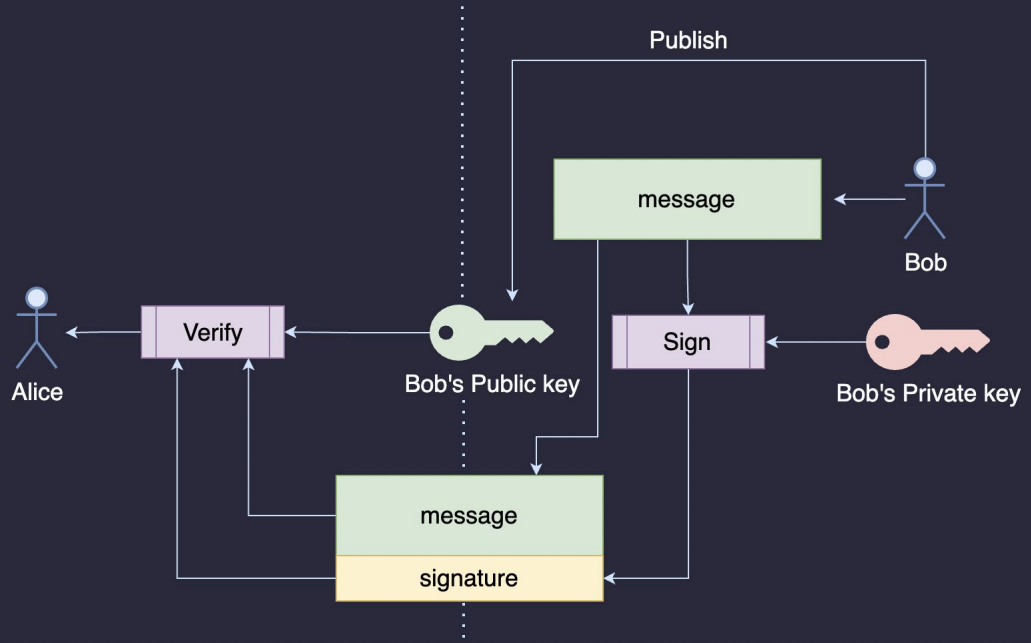


/Public Key Cryptography - Digital Signature

Bob publishes his public key so that others can verify that he “signed” a message.

Alice can be convinced that Bob did “sign” the message using the “Verify” algorithm.





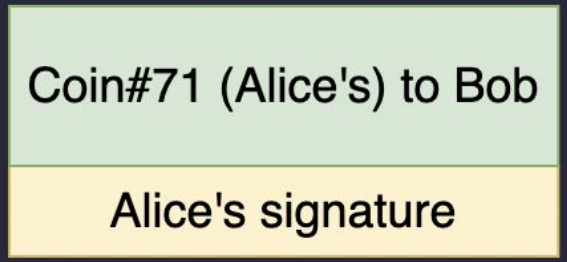
/Other Cryptographic schemes...

- Homomorphic Encryption
- Zero Knowledge Proofs
- Multi Party Computation
- Threshold Signature

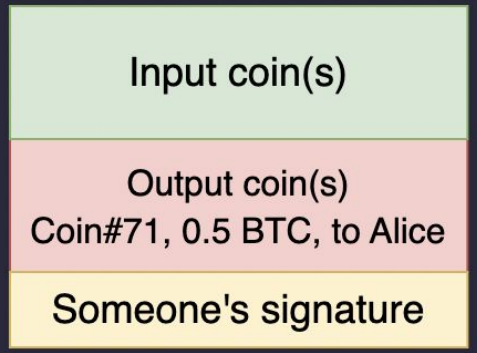
<Bitcoin 101>

/What is a transaction? (simplified)

- All messages on the blockchain are transactions. They all look like “Alice sends Coin#71 to Bob”.
- Different coin have different value
- If the message is “Alice sends Coin#71 to Bob”, how do we know if it is valid?



/What is a transaction in Bitcoin - UTXO (simplified)

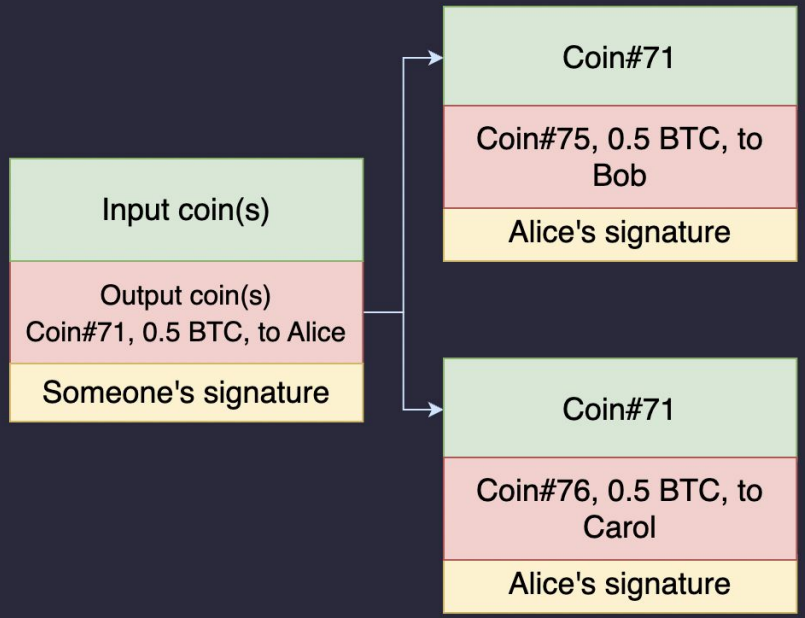


/What is a coin in Bitcoin - UTXO

- UTXO - Unspent Transaction Output
- “We define electronic coin as a chain of digital signatures”

/What is a coin in Bitcoin - UTXO

/Double Spending Attack



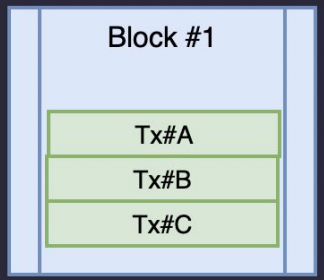
/Need someone to verify

- Someone's work:
  - Collect transactions
  - **filters out conflicting transactions and decide** which one to rule out
  - verify that the transactions are valid
  - Decide the ordering of the transactions
  - publish the result.

- Banking system?
  - Imagine trying to cash out two cheques, both with the size of the account's full balance.

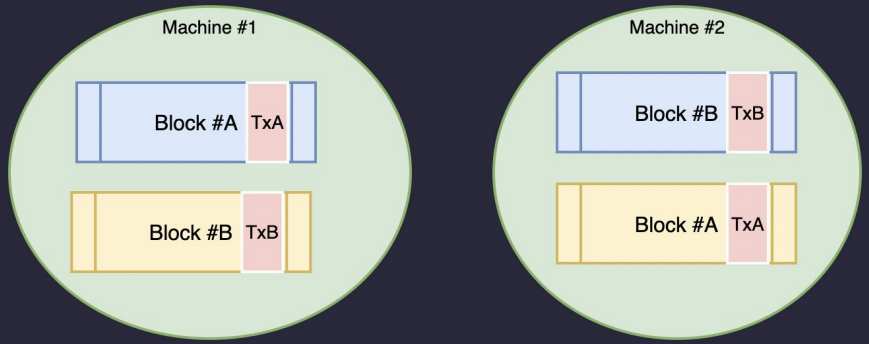
/Let Anyone verify

- Anyone can come in and verify transactions
  - Collect transactions
  - filters out conflicting transactions and decide which one to rule out
  - verify that the transactions are valid
  - Decide the ordering of the transactions
  - Package the collected transactions together and publish the result. (Block!)



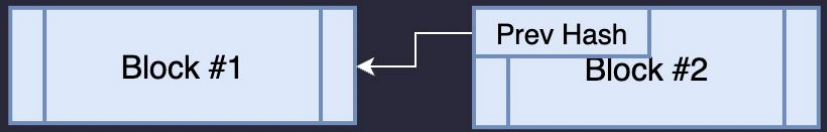
/Let Anyone verify

- Problem with decentralized system is that everyone may get block in different orders because of:
  - Network delay
  - Location
  - Network Partition



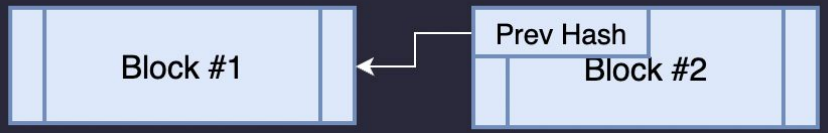
/The notion of time

- Blocks need to have **order** too, cannot consider them valid if they themselves are valid
- We need the notion of “**time**”, but not necessarily in a analog way.
- **Hash** can be used to establish order.



/The notion of time

- When packaging the block, the machine also need to specify the last block it is referring to by including the hash of the previous block.
- Now they are “Chained” together, forming a **Blockchain**!



/Let Anyone verify

- Anyone can come in and verify transactions
  - Collect transactions
  - filters out **conflicting transactions** and decide which one to rule out
  - verify that the transactions are valid
  - Decide the ordering of the transactions
  - publish the result.
- Why would anyone do this?
- “Anyone”? What if they are malicious?

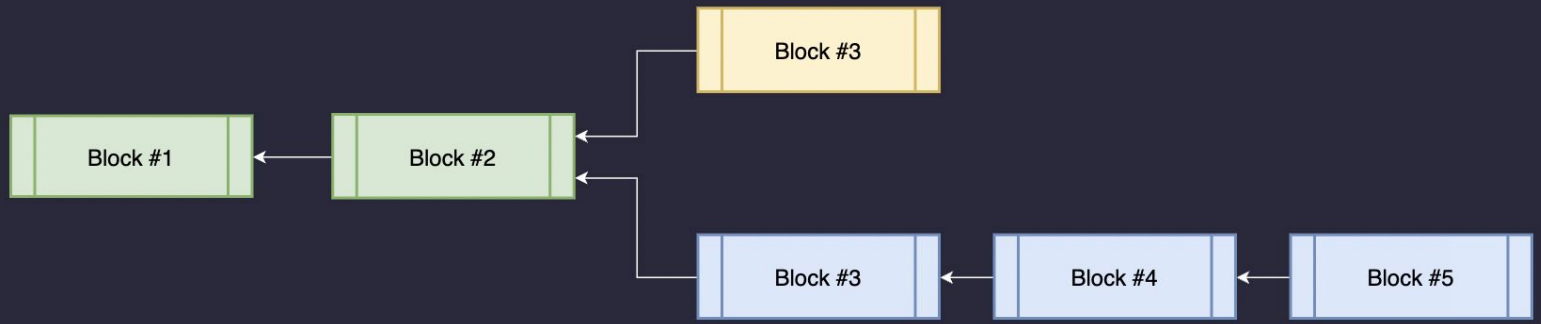
/Let Anyone verify ⇒ Economic approach

- Why would anyone do this?
  - Because they get rewarded
- “Anyone”? What if they are malicious?
  - Let’s penalize malicious party

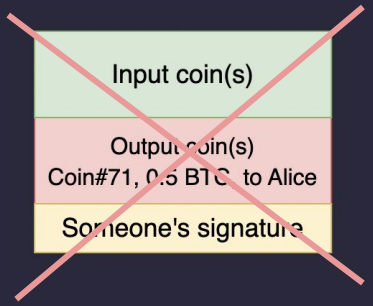
/Proof of Work: an economical defense

- Make it costly for verifiers to publish the block.
  - Proof of Work from “Hashcash” paper
  - Solve a puzzle (the puzzle itself is meaningless)
    - Create a hash with some amount of 0 digit in the front, with a fixed data and a controllable number. ⇒ Computation power is needed
- If you do dishonest work, your work will be ignored.
- Rule: Always work on the longest chain to create a new block after

/Longest Chain Principle

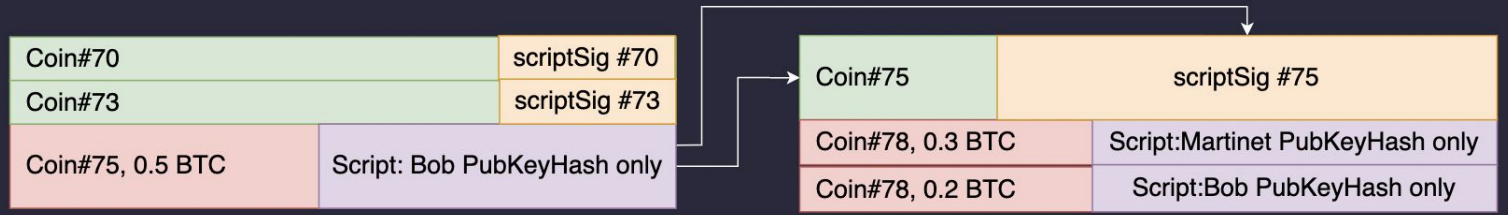


/Bitcoin Scripts



- P2PKH (Pay-to-Public-Key-Hash)
- P2SH (Pay-to-Script-Hash)
- …

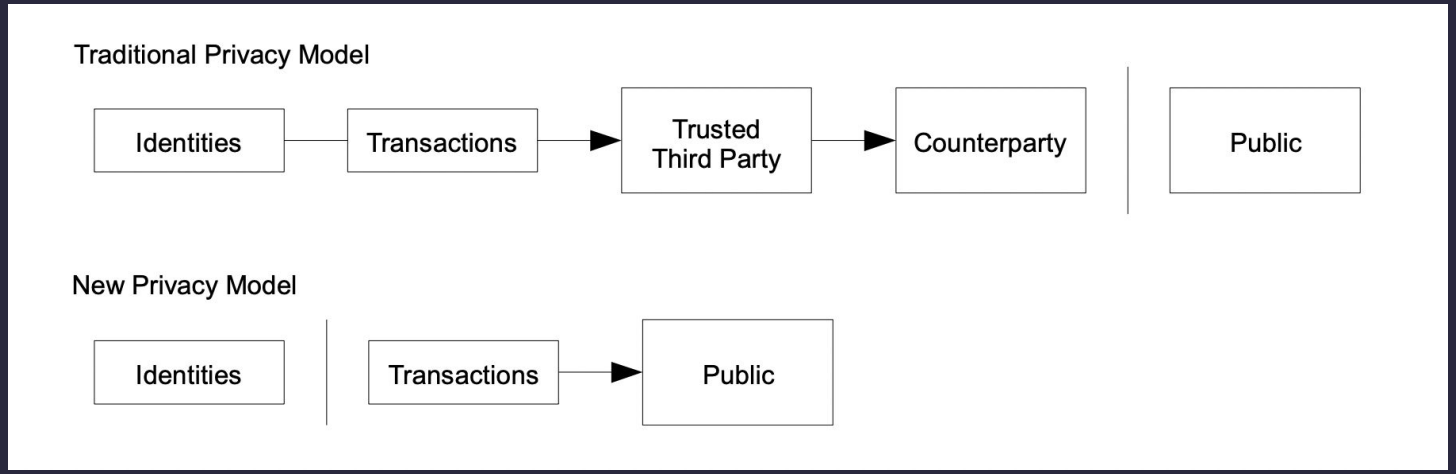
Can perform some operations but **NOT Turing complete**.



/Notes about Bitcoin

- A Ledger with simple scripts
- Currency comes in the form of “Coin” (UTXO)
- Totally focused on being a financial instrument with no additional features in the beginning.
  - MultiSig (unlock funds with multiple signatures), Timelock (unlocking funds after certain time) etc are possible via scripts and other additional fields in the tx format.

/How about anonymity in Bitcoin?



/From Bitcoin (2008) to Ethereum (2015)

- BTC Forks for adding some functionalities
  - Namecoin, ...
- Why not make it Turing Complete?

<Final Logistics>

/AI Policy

- Yes, you can use AI but:
  - You are responsible for understanding and explaining everything submitted.
  - Strongly suggest NOT to use it to code and setup the projects in the beginning to enhance understanding.

- Not Allowed to use AI for:
  - Quizzes

/Course Community & Assignment #1

- My email: martinetlee@gmail.com
  - If you write to me, please have **“[BDAF2025]”** in the title. I have a filter so it will pop out for me.
  - Quite busy so might not be able to reply asap. Possible to miss the message so if it is urgent feel free to ping me on Discord.
- Course discussion can be done asynchronously in the Discord community. I’ll post some resources, and if you find interesting resources, share there too!
  - *something something course participation wink wink ;)*
- Assignment #1 is due in ~2 **week**

/Course Community & Assignment #1

Discord Community

Assignment and the course page is already be announced on Discord.

Assignment 1 Summary:
you are going to implement a simple escrow contract in Solidity.

/THAT'S A WRAP! 🎤 (mic drop)