Today’s Agenda

- Evolution of the web
- Blockchain as a distributed database
  - Framing example: distributed ledger
  - Cryptocurrency
- Blockchain basics
  - Properties
  - Construction
  - Privacy (via Zero-Knowledge Proofs)
- Programmable blockchains
- Non-Fungible Tokens (NFTs)
- Decentralized Autonomous Organizations (DAOs)
- Other applications
Evolution of the Web

- **Web 1.0**
  - "Read only" web
  - Mostly static content
  - Focused on providing information

- **Web 2.0**
  - "Interactive" web
  - Substantial interactivity and participation
  - Fully functional web-based applications
  - Formation of social communities

- **Web 3.0**
  - "Decentralized" web
  - Powered by blockchain technology
  - Ownership and programmability become key factors
Today’s Agenda

• Evolution of the web
• **Blockchain as a distributed database**
  • Framing example: distributed ledger
  • Cryptocurrency
• Blockchain basics
  • Properties
  • Construction
  • Privacy (via Zero-Knowledge Proofs)
• Programmable blockchains
• Non-Fungible Tokens (NFTs)
• Decentralized Autonomous Organizations (DAOs)
• Other applications
What is a ledger?
  • A record of bookkeeping for transactions
  • Examples: credit card bill, accounts payable/receivable, bank deposits/withdrawals, etc.
Distributed Ledger

• Affordances of a ledger
  • Provides a permanent record of activity
    • Can only append to the ledger (not change previous entries)
  • Keep track of account/ownership
    • Example: bank balance is sum of all account deposits/withdrawals
    • Could potentially store other data in it as well

• Centralized vs. Distributed
  • Centralized: one (or a small number of) authorities control system
    • E.g., your bank maintains information about all your account transactions
  • Decentralized: no single entity has control
    • Information is replicated across a number of systems
    • E.g., Bitcoin blockchain (Satoshi Nakamoto, 2008)
      • It's not known who Satoshi Nakamoto really is!
Framing Example: Sharing Costs

- Housemates agree that each night a different person cooks
  - That person buys ingredients and cooks meal for whole house
  - Responsibility rotates across housemates

- Sharing Costs
  - Use paper to keep track of how much each person spent on food
  - Everyone in the house can write on paper
  - Expectation: write when you buy food and exact amount spent
  - Summing over ledger entries can determine each person's total spend

- What needs to be true for this to work?
  - Everyone in the house needs to be trustworthy (i.e., abide by rules)
  - Now, say some of the housemates are not trustworthy, but you don't know who they are

- How might you handle the ledger so you can keep correct records?
Maintaining an Accurate Ledger

- If there's someone in house that everyone trusts, have that person maintain the ledger with verifiable receipts
  - This is a centralized solution – the trusted person is like house "bank"
- Decentralized solution
  - Everyone in house maintains their own copy of the ledger
    - Everyone verifies and records transactions when they come in
    - No one can erase from the ledger (e.g., write in pen)
    - If there are discrepancies between ledgers, go with majority of ledgers
- Does this give you trust in the system?
  - Do you see a problem?
  - What if majority of housemates collude to add the same incorrect transactions to their ledgers? (This is called a "51% attack")
- The decentralized solution parallels what is going on with cryptocurrencies on the blockchain, like Bitcoin
From Ledgers to Currency

• If you have a (decentralized) ledger, you can keep track of tokens that can be exchanged
  • Maintain a record of transactions between entities to determine how many tokens each person has
  • Recall, this is how your bank balance is maintained
  • But rather than a government issuing tokens (e.g., dollars), you create your own token that can be exchanged
    • If there is a limited number of tokens available (scarcity), people may ascribe value to it
    • If value is ascribed to it, it can be exchanged for other things of value, essentially acting as a currency

• Cryptocurrencies are just tokens that are kept track of on distributed ledgers that people ascribe value to
  • Generally, there is a mechanism for limiting the supply of tokens
    • E.g., Bitcoin is limited to 21M tokens
Today’s Agenda

• Evolution of the web
• Blockchain as a distributed database
  • Framing example: distributed ledger
  • Cryptocurrency
• Blockchain basics
  • Properties
  • Construction
  • Privacy (via Zero-Knowledge Proofs)
• Programmable blockchains
• Non-Fungible Tokens (NFTs)
• Decentralized Autonomous Organizations (DAOs)
• Other applications
Properties we might want blockchains to have:

- Decentralization
  - No single person/entity/authority controls the system
- Permanence
  - Once data is added on blockchain, it cannot be deleted
- Consensus
  - Participants in system agree on contents of blockchain
  - True, even when there are (< 50%) untrustworthy participants
- Security
  - Transactions cannot be made on behalf of a participant without the participant's authorization
- Liveness
  - All honest participants can add transactions
- (Optional) Transparency:
  - All participants can see the contents of the blockchain
  - Note: some blockchains may be private (i.e., limit participation)
What is a Blockchain?

• As the name implies, a blockchain is a chain of blocks
  • There are different forms of blockchains
  • We'll (mostly) discuss the initial version of Bitcoin blockchain here

• Each block contains:
  • Header information (e.g., timestamp, block number/version, etc.)
  • Data
    • Bitcoin: data includes transactions including the sender, the receiver, and the amount of bitcoin sent
    • Other blockchains: could be other forms of data or even code
  • Hash of the previous block in the chain (except for the first block)
What is a Hash?

No!

What is a Hash?

- Hash functions: \( H(x) \)
  - Input: a variable length string \( x \)
  - Output: a value (usually a number) of fixed length (number of bits)
  - Efficiently computable
  - Simple example: \( H(x) = (\sum \text{ASCII character values in } x) \mod 2^{256} \)
  - More complex example: Google hashes every webpage it sees to a number. This makes it easier to detect if a webpage it just saw is a duplicate of a page already in its index.

- Cryptographic hash functions
  - Collision resistant: computationally infeasible to find values \( x \) and \( y \) such that \( x \neq y \) and \( H(x) = H(y) \)
  - Hiding: Given \( H(x) \), it is computational infeasible to determine \( x \)
  - Puzzle friendly: computationally infeasible to select an input that generates a pre-defined output
  - Bitcoin: SHA-256 cryptographic hash algorithm; outputs 256 bit hashes
Example of a Blockchain

- As the name implies, a blockchain is a chain of blocks
  - There are different forms of blockchains
  - We'll (mostly) discuss the initial version of Bitcoin blockchain here

**Genesis Block**

<table>
<thead>
<tr>
<th>Block 0</th>
<th>Block 1</th>
<th>Block 2</th>
<th>Block n</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block number</td>
<td>Block number</td>
<td>Block number</td>
<td>Block number</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Timestamp</td>
<td>Timestamp</td>
<td>Timestamp</td>
</tr>
<tr>
<td>Nonce</td>
<td>Nonce</td>
<td>Nonce</td>
<td>Nonce</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>Transaction</td>
<td>Transaction</td>
<td>Transaction</td>
<td>Transaction</td>
</tr>
<tr>
<td>Transaction</td>
<td>Transaction</td>
<td>Transaction</td>
<td>Transaction</td>
</tr>
<tr>
<td>Transaction</td>
<td>Transaction</td>
<td>Transaction</td>
<td>Transaction</td>
</tr>
</tbody>
</table>

Nonce ("number only used once"): value used to ensure uniqueness of block
Creating Blocks (simplified)

- There is a pool of validators (miners) who each maintain a copy of blockchain.
- Participants send their transactions to all validators:
  - Each transaction is "digitally signed" by the respective participant.
- A "leader" is selected from the validator pool to add a new block.
- All the other validators then validate the new block.
- The block is added to the blockchain:
  - All validators maintain a copy.
  - The leader is compensated.

Thanks to Dan Boneh for the idea behind the animation.
• There is a pool of validators (miners) who each maintain a copy of blockchain
• Participants send their transactions to all validators
  • Each transactions "digitally signed" by respective participant
• A "leader" is selected from the validator pool to add block
• All the other validators then validate the new block
• Block is added to blockchain
  • All validators maintain copy
  • Leader is compensated

Thanks to Dan Boneh for idea behind the animation
Sign Signing Transactions

- Want to ensure that transaction comes from actual entity (person) that is transferring assets
  - I.e., If Alice is sending Bitcoin to Roberto, we need to guarantee that it's actually Alice who is creating the transaction
- Use a cryptographic signature to sign transactions
  - Harness public key encryption that we talked about in privacy unit

Reverse of how we normally do encryption/decryption.
It works because... math!
Leader Selection

• Would like to select a leader such that:
  • Fairness: Everyone has a chance to be selected
  • Unpredictability: Selection has some randomness to it

• Question: Why not just select among all validators randomly?
  • Create multiple validator identities to increase my chances of selection!
  • This is called a "Sybil attack" in the distributed systems community

• Solution: Force validator to use resources to be selected
  • Having multiple identities also multiplies resources consumed

• Bitcoin uses "Proof-of-work"
  • Other mechanisms exist (e.g., Proof-of-stake)
  • We'll talk about that in a bit
Mining Bitcoin: Proof-of-Work

- Basic idea: make each validator solve a cryptographic puzzle
  - Solving the puzzle takes significant computing resources
  - First validator to solve puzzle is chosen as leader
  - Validating solution to the puzzle is computationally efficient (for others)

- Recall block structure

- Puzzle: find a value for nonce, \(a\), so the hash of data in block and nonce \((d \text{ and } a)\) is less than \(t\)
  - Formally: \(H(d \cdot a) \leq t\)
  - Infeasible to invert \(H\), so must try different (sequential) values for \(a\) until solution found
  - Once a solution nonce is found, it is easy for other validators to determine it is valid
  - Difficulty of problem (e.g., setting \(t\)) adjusted so blocks added at rate of one every 10 minutes
Chain Forking

• It's possible that two validators will each solve puzzle to become leader at nearly the same time
  • Each will try to add a block to its version of blockchain
  • This can cause a "fork"

• When fork occurs, longest chain wins
  • The blocks on longest chain should be considered canonical
  • Blocks on shorter chains (from fork point) should be ignored
  • Shorter chains should be abandoned (not added to)
  • Implies that chain can only be hijacked if some entity can add blocks at faster rate than rest of network (51% attack)

• Confirmation schemes exist to try to mitigate this situation
  • Don't actually consider a block permanently added to blockchain until confirmed by some number of validators
Bitcoin Mining: Rewards

- Selected leader get reward for their work
  - Leader is paid in Bitcoin created by network
    - Like an inflationary tax on the whole system

- Number of Bitcoin received as reward is halved every four years
  - Currently, 6.25 BTC reward (at $20K/BTC → $125K)
  - Next halving in 2024, when reward will become 3.125 BTC

- Final halving in 2140, when supply of Bitcoin will reach 21M maximum
  - Currently, roughly 19.3M Bitcoins exist

- After that, transaction fees ("gas fees") will be used for rewards
Bitcoin Mining: Energy Consumption

- Proof-of-work consumes tremendous energy

"Bitcoin, the world’s largest cryptocurrency, currently consumes an estimated 150 terawatt-hours of electricity annually — more than the entire country of Argentina, population 45 million."


Image: Bitcoin electricity consumption based on data from the University of Cambridge (last updated: 11.03.2021. Source: Cambridge Bitcoin Electricity Consumption Index. https://cbeci.org/). Maximum, minimum, and an (estimated) best-guess value are plotted over time and compared to the electricity consumption of various countries. License: CC BY-SA 4.0
What About Privacy?

• Can have public or private blockchains
  • Public chains (e.g., Bitcoin) allow virtually anyone to read them
  • Permissioned/private chains control access to who can read them
    • E.g., company might want to maintain inventory on a private chain
• What if we want to keep private data on a public blockchain?
• One solution: Zero-knowledge proofs
  • zk-SNARK: Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
  • Allows for indicating a property is true (proof) without revealing any other information (zero-knowledge)
  • Examples:
    • Verify your citizenship without revealing passport
    • Show you can afford a mortgage for $X without revealing salary
• For details on how this is possible, take CS251
Today’s Agenda

• Evolution of the web
• Blockchain as a distributed database
  • Framing example: distributed ledger
  • Cryptocurrency
• Blockchain basics
  • Properties
  • Construction
  • Privacy (via Zero-Knowledge Proofs)
• Programmable blockchains
• Non-Fungible Tokens (NFTs)
• Decentralized Autonomous Organizations (DAOs)
• Other applications
Programmable Blockchains

• So far, we've only considered storing data on blockchain
  • What if we could also store code?
  • And that code was executable
  • And execution could generate new blocks on the chain

• Welcome to the Ethereum Blockchain
  • 2013: Initial paper on concept by Vitalik Buterin
    • He was 19 years old at the time
  • 2014: Initial Ether (ETH), Ethereum's coin, sold to fund project
    • You could buy it with Bitcoin
  • 2015: Ethereum blockchain officially launched
  • 2022: Ethereum moved from Proof-of-Work to Proof-of-Stake for its consensus mechanism ("the merge")
    • Cut power consumption by 99%
Proof-of-Stake

- Rather than be selected leader based on work (puzzle solving), validators stake coins for chance to become leader
  - Ethereum requires 32 ETH to be staked to potentially become validator
    - Stake is governed by a smart contract
    - Staker added to a rate-limited queue of potential validators
  - When validators are activated, they are given blocks to check for validity
  - For valid blocks, each validator sends attestation (vote) to network
    - Votes of random committee of validators determine block validity
  - A leader is chosen randomly from validators to add/propagate new block
    - Leader gets paid ETH for adding the new block
    - If validator acts in bad faith, their stake can be burned

- Users create transactions with "tips" for validators
  - Tips are paid for including that transaction in a block
  - Makes it more likely the transaction will get priority
Ethressum Blockchains

- Blocks can contain executable code
  - Ethereum Virtual Machine (EVM) processes code in blocks
  - Sometimes called "Blockchain computer"
  - Code on blockchain also referred to as "smart contracts"
- Many basic concepts similar to Bitcoin blockchain
  - Key difference: its like "state machine" rather than "distributed ledger"
    - Note: a computer is just a form of state machine
  - State is maintained on the blockchain
  - When code is executed (i.e., transactions/commands), state is updated
- You pay "gas fees" for transactions
  - Basically, paying for work being done to process your transactions
  - Code can generate a lot of transactions
- No maximum on number of Ether (but subject to debate)
  - Set to create no more than 18M Ether each year
  - In early 2023, over 120 million ETH in circulation
Programming the Blockchain

- Languages like Solidity exist for programming on Ethereum
- Example: a stylized auction application
  - Auction has owner who is seller of item
  - Provide function to allow users to bid in auction (sending amount of bid)
    - Check timestamp that auction is not closed
    - If the bid is greater than current maximum bid, update maximum bid and max bidder (these are part of program state)
    - Users can raise bid by sending incremental money
  - When auction ends, do final accounting
    - Owner can withdraw amount of winning bid from winning bidder
    - All others withdraw their non-winning bid amounts
    - If digital asset, transfer ownership
- Why would bidders send in money, rather than just bid amount?
  - Guarantees that sufficient funds exist
  - All the code is public, so non-winners know they can get money back
Today’s Agenda

• Evolution of the web
• Blockchain as a distributed database
  • Framing example: distributed ledger
  • Cryptocurrency
• Blockchain basics
  • Properties
  • Construction
  • Privacy (via Zero-Knowledge Proofs)
• Programmable blockchains
• Non-Fungible Tokens (NFTs)
• Decentralized Autonomous Organizations (DAOs)
• Other applications
Non-Fungible Tokens (NFTs)

- Non-fungible: basically, it is a unique item
  - E.g., dollars in bank are fungible, since one can replace another
  - An original piece of art is non-fungible, as it can't be replaced by another
- Non-fungible token: used as indicator of ownership over a digital asset
  - Jack Dorsey sells first Tweet for $2.9M in March 2021
- The buyer tried to resell it in April 2022 for $48M in auction
  - Highest bid was $280 (that's measured in dollars, not millions)
  - Auction wasn't taken seriously
NFTs are Actually Big Business

And There Are Apes, Bored Ones

When I checked this listing on March 6, 2023, 1 ETH = ~$1,500
So, 72.072 ETH is more than $110,000

Today’s Agenda

• Evolution of the web
• Blockchain as a distributed database
  • Framing example: distributed ledger
  • Cryptocurrency
• Blockchain basics
  • Properties
  • Construction
  • Privacy (via Zero-Knowledge Proofs)
• Programmable blockchains
• Non-Fungible Tokens (NFTs)
• Decentralized Autonomous Organizations (DAOs)
• Other applications
Decentralized Autonomous Organizations (DAOs)

- DAO: decentralized organization where token-holders participate in decision-making of the organization
  - Idea created in 2016

- Generally rely on smart contracts to define activities (based on decisions of the organization)
  - Voting power often weighted by number of tokens someone has in the organization

- Organization may have a treasury
  - How treasury is used is determined by votes for token holders
  - Treasury may be formed by selling tokens in organization
  - Aligning incentives: having larger stake (tokens) in DAO often means you have more to lose if you engage in bad behavior
Examples of DAO: The DAO

- The DAO launched in April 2016
  - Meant to be an investor-directed venture fund
  - Members would vote on proposed projects to fund
    - Would get return based on payment terms from projects funded
- Raised $150M through token sales
- Attack on The DAO in June 2016 resulted in theft of $50M (ETH)
  - Smart contract for DAO required 28 day holding period before release
- Eventually, funds were recovered
  - Required a controversial fork of Ethereum blockchain to rollback transactions
- The DAO's token was delisted in September 2016
ConstitutionDAO

- ConstitutionDAO launched in November 2021
  - Aimed to buy original copy of US Constitution

- Raised $47M (in ETH)

- But lost to a bid of $43.2M in auction
  - Insufficient funds to insure and store document if they bid higher
  - Buyer was Ken Griffin, CEO of Citadel (hedge fund)

- ConstitutionDAO tried to return funds
  - Ethereum fees for refund could be substantial

License: Public domain.
Today’s Agenda

• Evolution of the web
• Blockchain as a distributed database
  • Framing example: distributed ledger
  • Cryptocurrency
• Blockchain basics
  • Properties
  • Construction
  • Privacy (via Zero-Knowledge Proofs)
• Programmable blockchains
• Non-Fungible Tokens (NFTs)
• Decentralized Autonomous Organizations (DAOs)
• Other applications
Other Applications of Blockchain

- Payment system for unbanked populations
  - Potential hedge against inflation for some currencies
- Supply chain/inventory management
  - Tracking goods in supply chain
- Insurance
  - Smart contracts for reporting claims and compliance
- Healthcare
  - Tracking anonymized patient data
- Real estate
  - Ownership records and verification
- Identity management
  - Verification of citizenship, birth records, drivers license, etc.
- Voting
  - Verifiable record of voting with identity verification
“From the beginning, one of our primary motivations has been to empower students to be the curators of their own credentials,” says Registrar and Senior Associate Dean Mary Callahan. “This pilot makes it possible for them to have ownership of their records and be able to share them in a secure way, with whomever they choose.”

The Institute is among the first universities to make the leap, says Chris Jagers, co-founder and CEO of Learning Machine. “MIT has issued official records in a format that can exist even if the institution goes away, even if we go away as a vendor,” Jagers says.