CSE 3550/5000: Blockchain Technology

Lecture 3
Bitcoin - Part I

Ghada Almashaqbeh
UConn - Spring 2026

Outline

- Bitcoin.
  - work model,
  - participants,
  - transactions,
  - blockchain,
  - mining.

Bitcoin in a Nutshell I

- A distributed currency exchange medium open to anyone to join.
  - Powered by a peer-to-peer (P2P) network.
- Utilize distributed consensus and basic cryptographic primitives to control the money flow in the system.
  - Proof of work (PoW)-based consensus, hash functions and digital signatures.
- Building blocks:
  - Players: miners and clients.
  - Transactions: messages exchanged.
  - Blockchain: an append only log.
  - Mining: extending the blockchain.
  - Consensus: agreeing on the current state of the Blockchain.

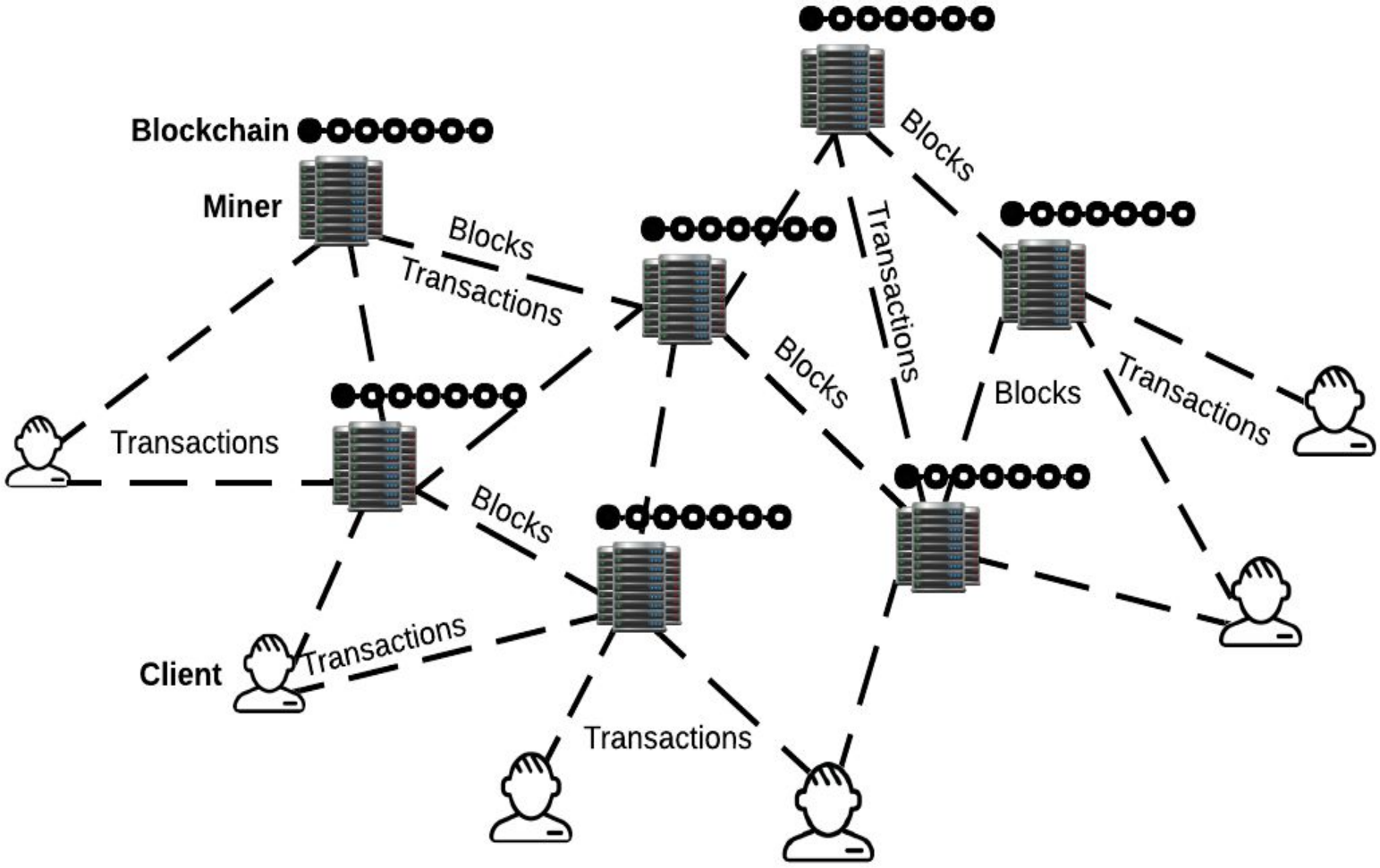
Bitcoin in a Nutshell II

- No real identities are required, just a key pair.
- Owning the private key of the destination address of a currency transfer transaction means you own the currency held under that address.
- Losing the private key of a specific address means losing the coins associated to this address forever.
  - Wallets take care of tracking coins, issuing transactions, etc.
- Digital signatures are used to prove ownership of the private key associated to the coins one wants to spend.
- Everything is logged on the blockchain.

Who is Who in Bitcoin

- Two types of nodes in Bitcoin network:
  - **Lightweight nodes or clients:**
    - Also called thin clients or simple payment verification (SPV) clients.
    - Do not store the whole blockchain, only specific parts to verify the transactions they care about.
    - They rely on the miners to process transactions and retrieve blockchain-related information they are interested in.
  - **Fully validating nodes or miners:**
    - Connect clients to the Bitcoin network.
    - Have a good network connectivity to be able to hear all transactions (hopefully), and tend to be online all the time.
    - Each stores a full copy of the blockchain.
    - Maintain the blockchain by performing mining and consensus

Bitcoin Pictorially



Decentralization in Bitcoin

- **P2P network:** anybody can join and leave anytime.
- **Mining:** open to anyone but requires large computation power and resources.
- **Updates on the used software:** done by the community developers (through the Bitcoin foundation) with proposals submitted by anyone.
- **Maintaining the public ledger:** maintained by all miners within the network.
  - No centralized bank.
- **Transactions:** announced publicly to everyone.
- **Minting new coins:** miners can do that based on their contribution to mining, i.e., mining new blocks leads to minting new coins.
  - No central authority.

Digital Signature Schemes and Hash Functions used in Bitcoin

- Bitcoin uses ECDSA (Elliptic Curve Digital Signature Algorithm) over the secp256k1 curve.
  - A few years ago, support for Schnorr signatures have been added due to their efficiency. Still, the main scheme to be used is ECDSA.
- Mainly SHA256 for everything that needs hashing, and RIPEMD for address generation.
  - Both are assumed to be CRHF, and for SHA256 be a OWF as well—for formal security purposes, SHA256 is modeled as a random oracle (work in the ROM).
  - We will not get into the details of the internal design of these functions.

More on ECDSA

In the first hands-on HW, you will experiment with hashes and ECDSA.

- Bitcoin uses ECDSA (Elliptic Curve Digital Signature Algorithm) over the secp256k1 curve.
  - A few years ago, support for Schnorr signatures have been added for efficiency. Still, the main scheme used is ECDSA.
- ECDSA is based on the hardness of the discrete logarithm (DL) problem.
  - Informally, for a cyclic group G with order p and generator g, where DL is hard, given $y = g^x$, it is hard for a PPT adversary to find x.
- Used in the hash-then-sign paradigm.
- DSA works over prime fields (integers), ECDSA is the elliptic curve version of DSA.

Bitcoin Addresses I

- Used by users (clients and miners) over the Bitcoin network.
  - Remember real identities are not required!
- A Bitcoin address is a 160-bit hash of the public key of an ECDSA key-pair.
  - The public key size is 512 bits.
  - The address is the public key hashed twice: first using SHA256, which produces a digest of size 256 bits, the hash the output using RIPEMD160 (RACE Integrity Primitives Evaluation Message Digest) to produce a 160-bit digest.
- Additional bytes will be added to (prefix and postfix) to indicate whether this is a mainnet, testnet, etc., address resulting in a 25 byte binary address.

Bitcoin Addresses II

- For readability, addresses are represented in alphanumeric strings using Base58 encoding, i.e., binary to text encoding.
  - E.g: 1B74t1WpEZ73CNmQviecbaciWRnqRhWNLy
  - Done to make it easier for humans to type.
  - see https://en.bitcoin.it/wiki/Base58Check_encoding for details.
- Resulted Bitcoin address will start with either 1 or 3.
  - 1 for individual addresses as output destination.
  - 3 for scripts addresses as output destination (script hash).
- To promote ***privacy/anonymity***, it is advised to generate a different address (or different key pair) for each new transaction.
  - Will look more into anonymity issues of Bitcoin later.

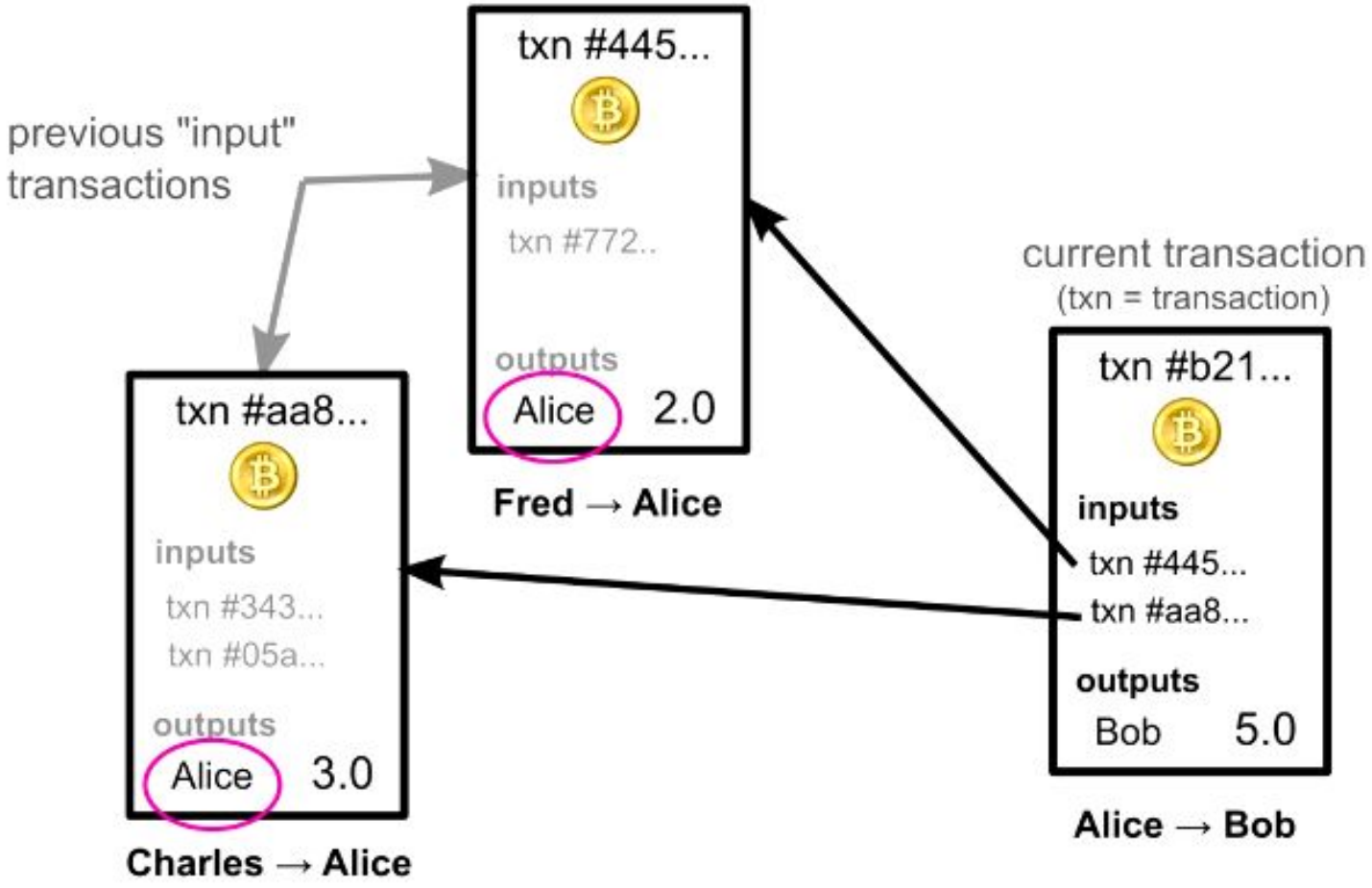
Bitcoin Transactions

- Transactions represent the digital tokens, or virtual coins, in Bitcoin.
- A new transaction is issued by any node as follows:
  - Fill the following fields:
    - Input section: list of pointers to previous unspent transactions owned by the sender.
    - Output section: the addresses of the receivers or the hash of the output script.
  - Sign the whole transaction (including the output section) using the private keys associated with the inputs—one signature per input.
    - So you may use different inputs associated to different keys (aka addresses) that you own.
- The sender then broadcasts the transaction over the network.

UTXO Model

- Bitcoin adopts the UTXO - Unspent Transaction Output.
  - No notion of accounts, track chains of transactions to report balance.
    - Wallets do that transparently for users.
- You cannot spend a portion of an input. All of the total input values will go to the output.
  - Like paying for a $2 cookie with a $100 bill :)
- Solution?? Direct the change to an address you own.
  - A transaction can have multiple inputs and multiple outputs.
- Transactions are irreversible.
  - A merchant who wants to issue a refund has to issue a new transaction that spends the payment transaction he received from the customer back to this customer.

Bitcoin Transactions - Pictorially



Source: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

The Public Ledger or Blockchain

- Append only log contains a full record of all transactions.
  - These transactions are recorded in blocks.
  - The blockchain is a linked list of these blocks, linked by their hashes.
- Miners extend the blockchain by mining new blocks.
  - Solve a proof-of-work puzzle.
  - Collect monetary incentives.
- Each block has a header and a body.
  - Header includes meta data, while the body include the list of transactions recorded in a block.

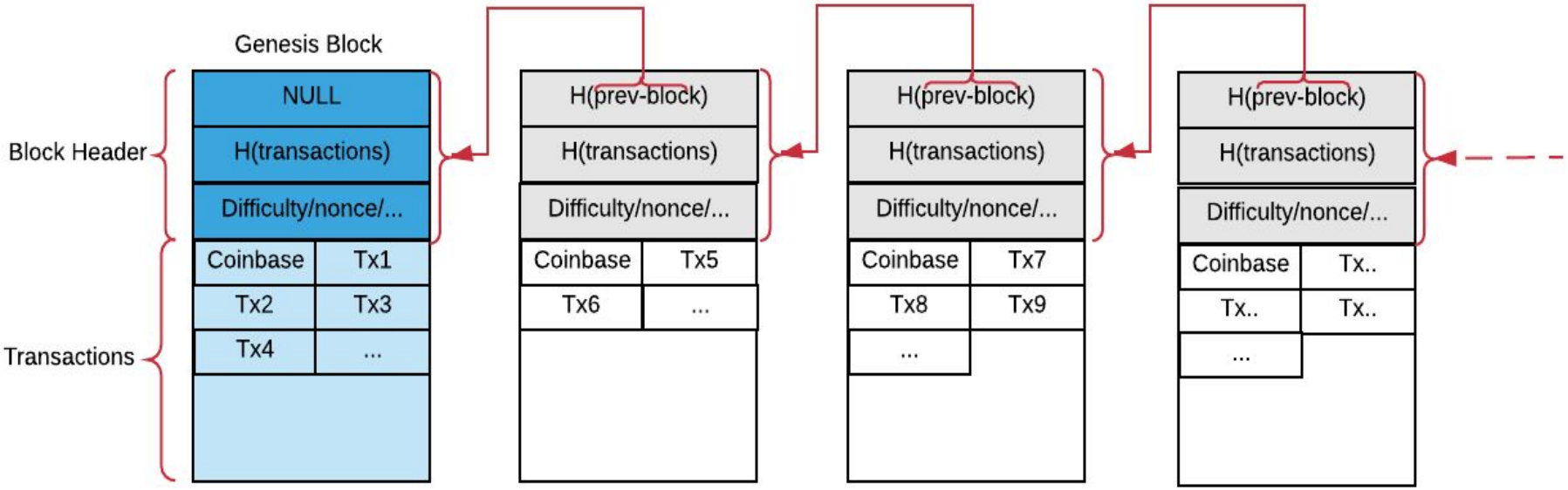
Block Header

- Consists of:
  - 4 bytes ➔ Version: The version number of the software run by the miner
  - 32 bytes ➔ Previous Block Hash: A reference to the hash of the previous (parent) block in the chain
  - 32 bytes ➔ Merkle Root: A hash of the root of the Merkle-tree computed over the transactions recorded in the block
  - 4 bytes ➔ Timestamp: The approximate creation time of the block (seconds since 1970-01-01T00:00 UTC)
  - 4 bytes ➔ Difficulty Target: The Proof-of-Work algorithm difficulty target for this block
  - 4 bytes ➔ Nonce: A random value used for the Proof-of-Work algorithm

Block Body

- The content of a block is a set of transactions including:
  - Standard transactions broadcast by the users in the network.
    - Only valid and unspent ones are included.
  - Coinbase transaction with a value equals to the mining reward destined to the miner who mined the block.

The Blockchain Structure



Tx stands for Transaction

Mining I

- Miners extend the blockchain with new blocks (and mint new currency).
- Done through proof of work (PoW).
- Miners solve a hash puzzle,

  SHA-256(SHA-256 (new block header)) < Difficulty Target

- For secure hash functions, the only way to find the hash with a given property is to try nonce values until a desired hash is found.
  - Hence it is solving a hash puzzle.
- Verification is very easy, other miners check the validity of all transactions in a block, and then verify the solution of the hash puzzle.
  - The latter is a single hash invocation.

Mining II

- Difficulty is adjusted periodically, roughly, every two weeks.
  - Keeps the block generation rate constant, 1 block every 10 minutes.
  - Accommodates the increasing computation power of miners.
    - New strong miners may join the network, hence, they will be able to solve the puzzle faster.
    - Affects the security of the blockchain, strong miners could be able to rewrite the blockchain and change the system view.
- Miners are incentivised to mine to collect:
  - Mining rewards,
  - and transaction fees.

Mining Rewards

- Miners mint new coins as a reward for their work.
- Each miner includes a special transaction destined to itself as a reward.
  - Called a coinbase transaction.
  - A miner can spend its reward when the block it mined, and so containing the coinbase transaction, is confirmed on the blockchain.
- Currently the incentive is 3.125 BTC and it halves every 210,000 blocks (approximately every 4 years).
  - It started with 50 BTC.
- Total Bitcoins to mine is capped by 21 million BTC.
  - now there is around ~19.9 million BTC in circulation.

Transaction Fees

- Tips for miners who succeed in mining confirmed blocks.
  - The issuer of a transaction can select to include a transaction fee that goes to the miner who mines the block that will contain this transaction.
- This is done by setting the input value to be larger than the output value by the tip amount.
- Optional (it is a tip), but when mining rewards disappear they might become (implicitly) mandatory.
- When mining, miners give higher priority to transactions that include higher tips.
  - As a matter of act, transaction fees are a sort of must now. No fees, no priority.

Miners Hardware

- Started with CPU mining, then GPU mining, and then ASIC (Application-specific Integrated Circuits) mining—i.e., custom-designed hardware for mining rather than general purpose hardware..
  - Now there are mining pools with huge data centers.
- Now mining require huge data centers. Check https://bitfury.com/crypto-infrastructure/datacenters to see some examples.
  - Of course you can install the miner software on your own laptop and join the Bitcoin network to mine, but the chance you will win the mining race is pretty much negligible.

User Experience with Bitcoin

- **First:** Install a wallet (e.g., visit https://bitcoin.org/en/choose-your-wallet).
- **Second:** Buy Bitcoin, multiple options:
  - Cryptocurrency exchanges, such as Binance, Coinbase, etc., even banks.
    - Many are operating Bitcoin ATMs, check to see their locations: https://coinatmradar.com/
  - Find people in your area to buy their BTC.
  - Sell a product for Bitcoin.
- **Third:** Spend your BTC ☺️
  - Simply scan the address of the merchant and use your wallet to create a payment transaction.
  - Increasing number of merchants are accepting BTC (and other cryptocurrencies as well) for payments.

Useful Resource

- Bitcoin wiki is a very helpful resource to dive more into the technical details and specifications of Bitcoin's protocol and implementation.
  - https://en.bitcoin.it/wiki/Main_Page
  - Search for any topic you want and it will return all pages in the wiki about that topic.