Blockchain Technology (CISC 6880)
Lecture 1

Ghada Almashaqbeh
CacheCash

Fordham University - Summer 2019

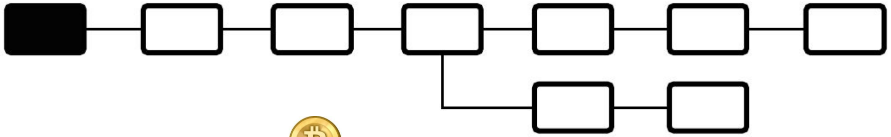
Outline

- Motivation.
- Cryptocurrency definition.
- Cryptographic primitives overview.
- Introduction to Bitcoin.
    - work model,
    - participants,
    - transactions,
    - blockchain,
    - mining,
    - consensus.

Once Upon A Time

Centralized Currency

Decentralized Currency



History

- A whitepaper posted online in 2008: “Bitcoin: A Peer-to-Peer Electronic Cash System”.
- By Satoshi Nakamoto.
- Described a distributed cryptocurrency system not regulated by any government.
- The system went live on January 2009.
- Now “Satoshi Nakamoto” is only associated with certain public keys on Bitcoin blockchain.
- She/He/They was/were active on forums/emails/etc. until 2010.
- Currently there are **2226** cryptocurrencies (https://coinmarketcap.com/).

Cryptocurrencies

- The use of cryptographic primitives and distributed consensus protocols to secure virtual money creation and flow between various parties.
- “A type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community” - European Central Bank.

Cryptographic Primitives Overview

Hash Functions I

- Mathematical functions that take input of any size and produces a fixed size output.
    - They compress the input to produce a shorter output.
    - Usually the output is called a digest.
    - We will deal with fixed length hash functions.
- They are also called one-way functions where computing the hash of some string is easy but reversing the hash to recover the input is hard.
    - Technically: computing the image of some input is efficient (done in polynomial time of O(n) where n is the input size), while computing the preimage is inefficient (non-polynomial or computationally hard).

Hash Functions II

- Security properties:
  - First-preimage resistance: given y where y = h(x) it is computationally hard to find x.
  - Second-preimage resistance: given x it is computationally hard to find x’ such that h(x) = h(x’).
  - Collision resistance: it is computationally hard to find any x, x’ such that h(x) = h(x’).
- Applications:
  - Message authentication codes.
  - Commitment schemes.
  - Hash tables.
  - Password hashing.
  - Merkle trees.

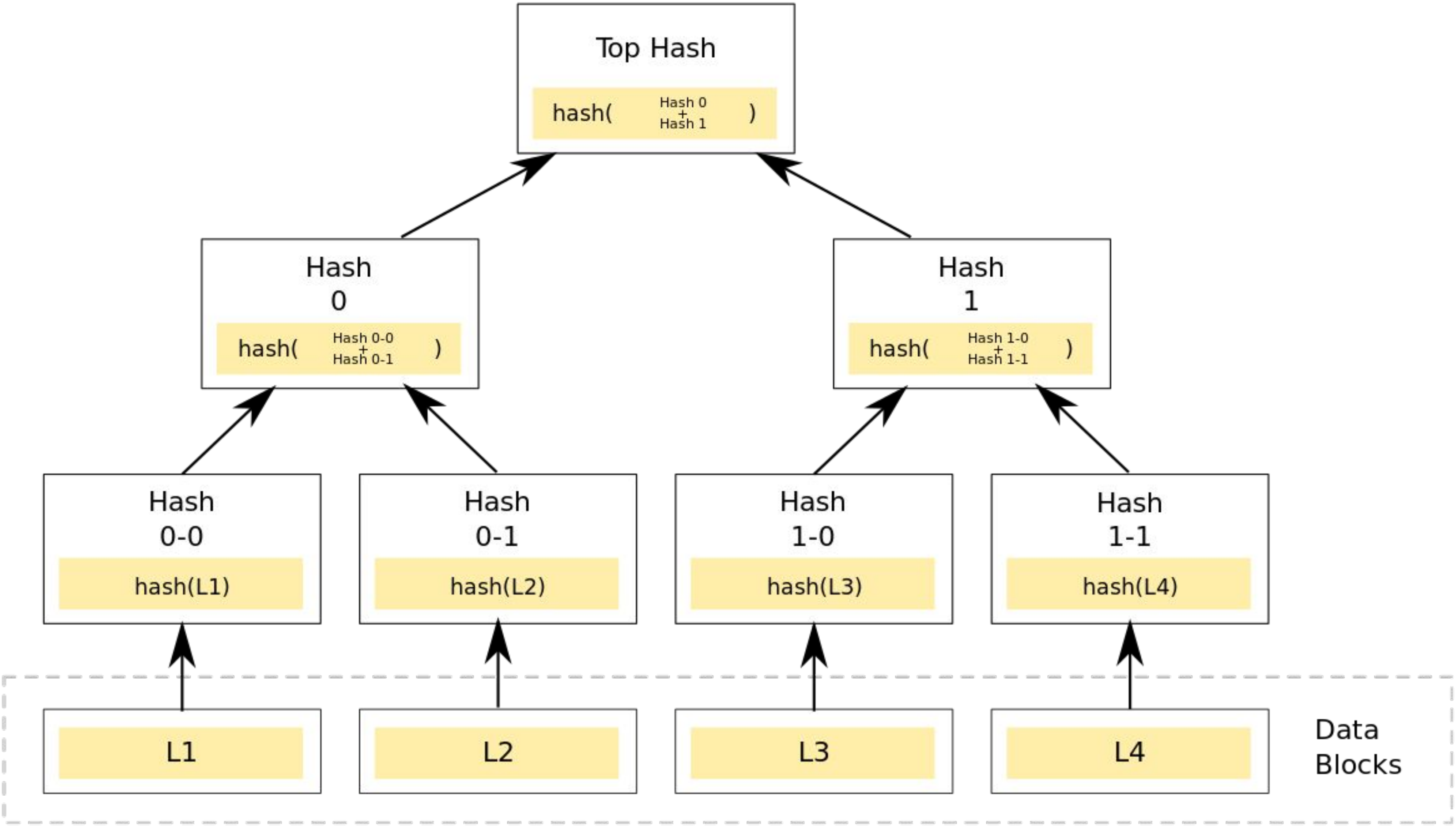
Hash Functions III

- In Theory, hash functions are keyed functions. Meaning that the hash functions is a parameterized by a key (public, known to everyone). Changing the key changes the mapping (or functions output).
- In practice, all used hash functions are fixed-length unkeyed functions (for the same input they always produce the same output).
- Examples: SHA1, SHA2, SHA3, etc.
- Most cryptocurrencies use SHA256 (SHA2 with output size of 256 bit).
    - Bitcoin also uses RIPEMD-160 with output size of 160 bits.
- Some replaced SHA256 with the more secure one SHA3 (or Keccak) with the same output size.
    - E.g., Ethereum.

Merkle Tree

- An efficient solution for data correctness verification.
    - Usually used in distributed systems and file storage.
- It is a binary tree with leaf nodes as input values: L1, L2, …, Ln with depth log n.
- Each internal node in the tree is the hash of its two children.
- The root digest represent the hash of all leaf nodes.
- Verifying the correctness of an input is done by providing a membership path of size log n digests.
    - It requires log n digests and log n hash invocations.

Merkle Tree Pictorially



* https://en.wikipedia.org/wiki/Merkle_tree

Digital Signatures I

- Used to provide message integrity and non-repudiation.
  - Integrity: prevent message tampering.
  - Non-repudiation: bind the sender (or message originator) to the message.
- Work in the public-key setting.
  - Each party creates a key pair, public and private key.
  - Uses the private key to sign the message, while anyone can verify the signature using the public key.
  - The public key usually serves as an ID.
- A digital signature scheme consists of three algorithms:
  - Gen: generate a key pair.
  - Sign: sign a message using the private key (usually it is randomized).
  - Verify: verify the correctness of the signature over the signed message (deterministic).

Digital Signatures II

- Informally, a secure digital signature scheme means that an attacker cannot generate a valid signature over a message without knowing the secret key even if it obtains signatures on other messages.
  - It cannot forge a signature.
- Most of the practical digital signatures constructions are computationally secure.
  - It is computationally hard to forge a signature unless you know the secret key.
- Usually the hash-sign paradigm is used, where the message is hashed first and then the digest is signed.
- Most cryptocurrency systems use ECDSA (Elliptic Curve Digital Signature algorithm).
  - Recently, several systems started to switch to EdDSA (Edwards-curve Digital Signature Algorithm).

Hands-on Exercise 1.1

- Use Openssl on your machine and use the command line to do the following:
    - Hash a message.
        - Change a character in the message and hash again, is the hash different?
    - Generate a public and private key using ECDSA (with ... curve).
    - Sign a message using the private key, and verify the signature using the public key.

Introduction to Bitcoin

Bitcoin in a Nutshell I

- A distributed currency exchange medium open to anyone to join.
  - Powered by a peer-to-peer (P2P) network.
- Utilize basic cryptographic primitives to control the money flow in the system.
- Main components:
  - 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.

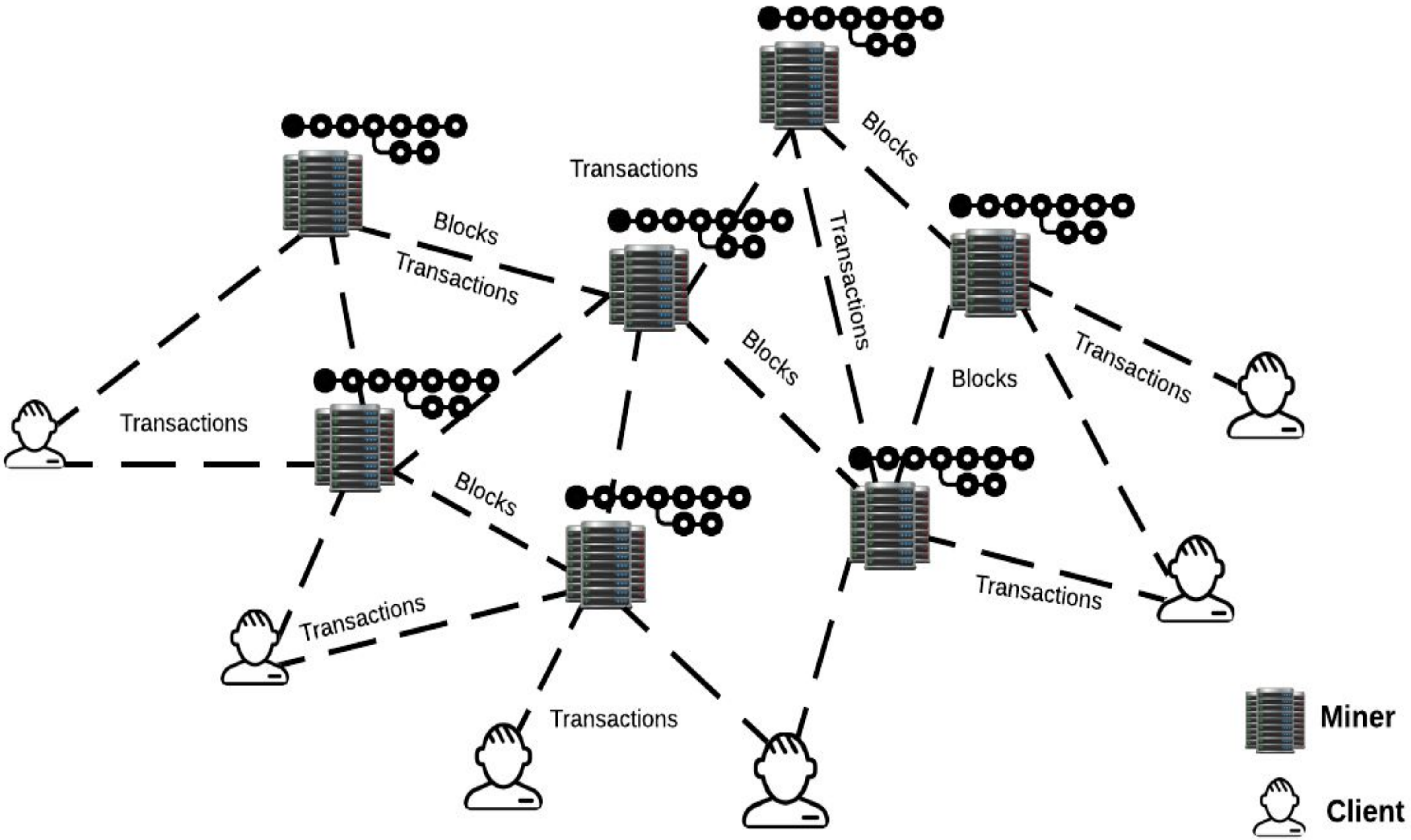
Bitcoin in a Nutshell II

- No real identities are required, just a key pair.
  - Usually the hash of the public key is the participant’s address.
- Owning the private key of the destination address of currency transfer means you own the currency value of 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, issue transactions, etc.
- Digital signatures are used to prove your ownership of the private key associated to the coins you want to spend.
- Everything is logged on a public ledger called a blockchain.
  - Built basically using a linked list and hash pointers.

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.
    - The vast majority of Bitcoin nodes are lightweight ones.
    - Do not store the whole blockchain, only specific parts to verify the transactions they care about.
    - They trust the miners in generating trusted and true blocks.
  - **Fully validating nodes or miners:**
    - Must stay permanently connected to the system.
    - Have a good network connectivity to be able to hear all transactions (hopefully).
    - Store a full copy of the blockchain.

Bitcoin Pictorially



Decentralization in Bitcoin

- **Peer to peer 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.
- **Creating new coins:** miners can do that based on their work.
    - no central authority.

Bitcoin Addresses I

- Define users over the Bitcoin network.
- A Bitcoin address is a 160-bit hash of the public portion of an ECDSA key-pair.
    - Recall that ECDSA is used for digital signature in Bitcoin with key size of 512 bit.
    - The address is the public key hashed twice: using SHA-256 followed by RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest).
- An additional byte is needed since all Bitcoin addresses should start with either 1 or 3.
    - 1 for individual addresses as output destination.
    - 3 for scripts addresses as output destination (script hash).

Bitcoin Addresses II

- For readability, addresses are represented in alphanumeric (using Base 58 encoding, binary to text encoding) - E.g: 1B74t1WpEZ73CNmQviecbaciWRnqRhWNLy
- Must have private key to access the fund.
- QR codes (quick response codes) are used as an easy way to exchange addresses and perform transactions through the wallets.
- To enhance privacy, it is advised to generate a different address (or different key pair) for each new transaction.
    - Will look more into privacy issues and transactions linkability in Bitcoin.

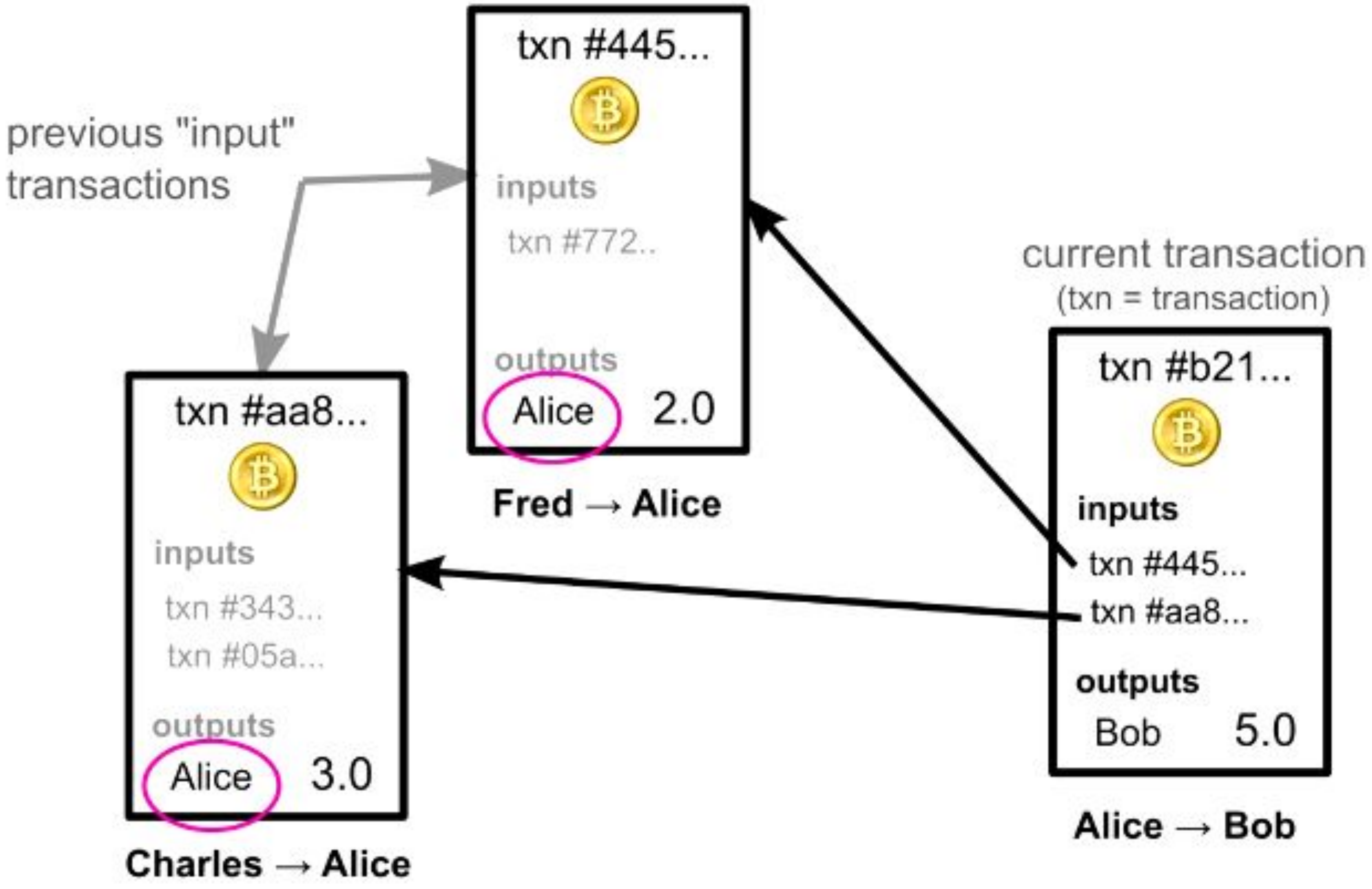
Bitcoin Transactions I

- Transactions represent the digital token, ot virtual coins, in Bitcoin.
- A coins can be spent by providing a signature using the private key associated with the destination address of the transaction.
- 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 address of the receiver or the hash of the output script.
  - Sign the whole transaction (including the output section) using the private keys associated with the inputs.
- The sender then broadcasts the transaction over the network.

Bitcoin Transactions II

- No notion of accounts, track chains of transactions.
  - Wallets do that transparently for users.
- You cannot spend a portion of an input. All the input values will go to the output.
  - Like paying $2 cookie with a $100 bill.
- The solution?? Return 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 original payment transaction back to the customer.

Bitcoin Transactions - Pictorially



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

In Class Discussion 1.1

- Steve Ursell.

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.

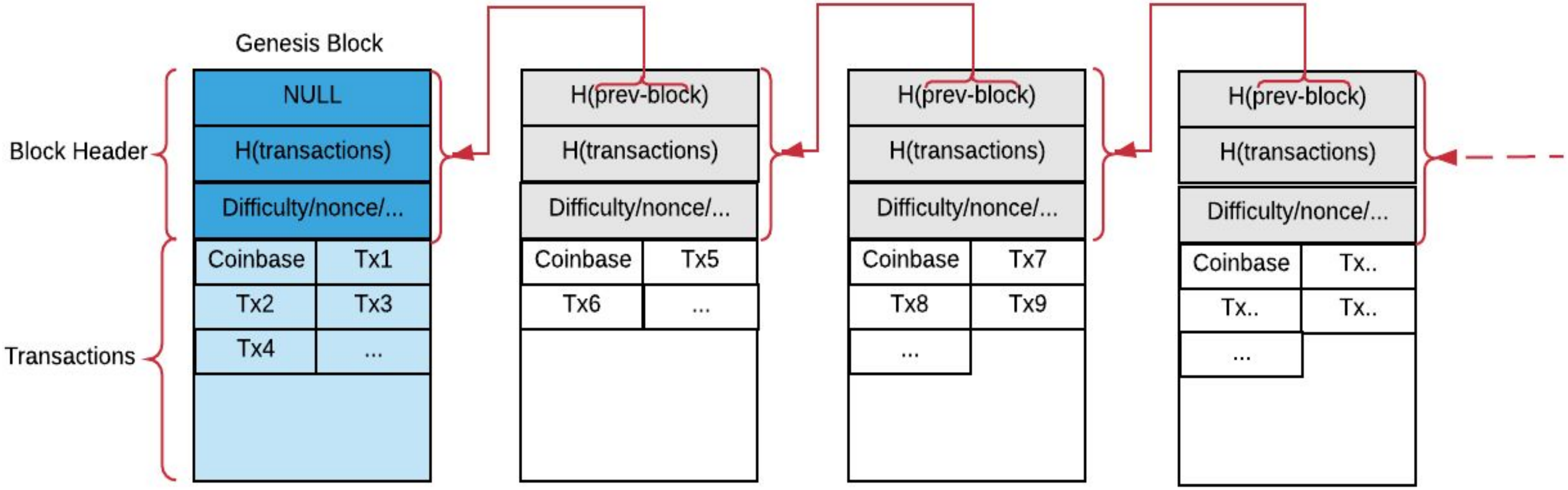
Block Header

- Block header:
  - 4 byte ➔Version: A version number to track software/protocol upgrades
  - 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 of this block’s transactions
  - 4 bytes ➔ Timestamp: The approximate creation time of this block (seconds from Unix Epoch)
  - 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 the 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 value equals to the mining reward destined to the miner who mines the block.

The Blockchain Structure



Double Spending and Blockchain

- Spend the same currency more than once.
  - All what costs the owner to do so is to produce a new signature.
- Handled by logging all transactions on the blockchain.
  - Miners can check whether a transaction has been already spent or not.
- Network propagation delay may allow race condition between transactions.
  - Also manipulating the transaction fee.
- To address this issue, usually it is advised not to act (like sending a product or stock shares) until the transaction is confirmed.
  - In Bitcoin this happens when the block containing this transaction is buried under 6 blocks.

Mining I

- The miners extend the blockchain with new blocks (and mint new currency).
- Done through proof-of-work.
  - Needed to prevent Sybil attacks.
- 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 the specific property is to try nonce values till a desired one is found.
  - Hence it is solving a hash puzzle.
- Verification is very easy, other miners check the validity of the included transactions and then verify the solution of the hash puzzle.

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 its view.
- Miners are incentivised for mining by:
  - Mining rewards.
  - Transaction fees.

Mining Rewards

- Miners create new coins as a reward for their work on the block chain.
- Each miner includes a special transaction destined to himself as a reward.
  - Called coinbase transaction.
  - This transaction becomes legitimate if it is in a successfully produced block that exists in a long block chain branch.
- Currently the incentive is 12.5 BTC and it halves every 210,000 blocks (approximately every 4 years). Started with 50 BTC.
- Total Bitcoin to mine is capped by 21 million BTC.
  - now there are around 17 million.

Transaction Fees

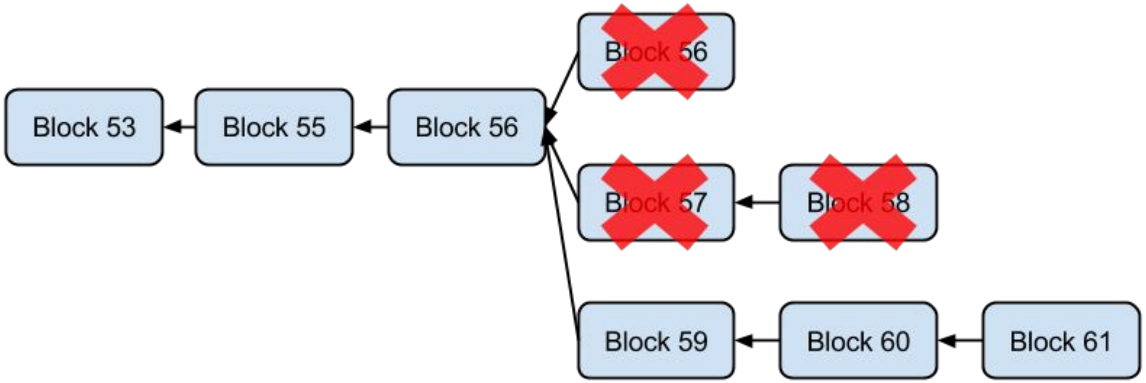
- Tips for blocks creators.
- The issuer of the transactions selects to include a transaction fee that goes to the winner miner.
- This is done by having the input Bitcoin value to any transaction larger than the output Bitcoin value by the tip amount.
- Voluntary (it is a tip) but it is expected to become mandatory as we reach the maximum allowed Bitcoin circulation.
- Miners give higher priority to transactions that include higher tips in mining.

Miners Hardware

- Started by normal users and their CPUs mining, then GPUs mining, and then the ASIC (applications Specific Integrated Circuits) mining.
- Example: Bitfury miner center: http://www.bitfury.org/

Consensus

- Miners hold , hopefully, consistent copies of the blockchain.
  - Only differ in the recent unconfirmed blocks.
- A miner votes for a block implicitly by building on top of it.
  - Mining power requirement handles Sybil attacks.
- Forking the blockchain means that miners work on different branches
  - Caused by network propagation delays, adversarial actions, etc.
  - Resolved by adopting the longest branch.



Source: http://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/

Hands-on Exercise 1.2

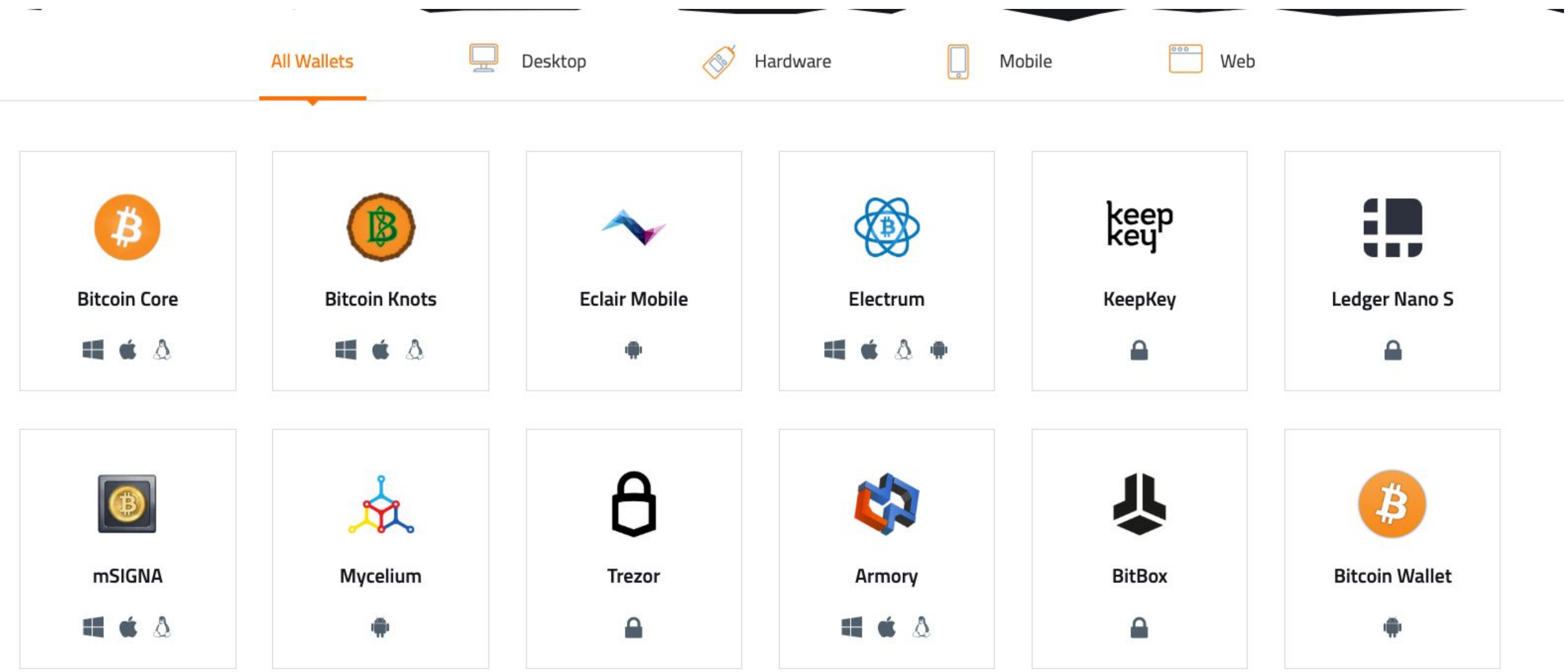
- Go to https://blockchain.info/
  - What is the blockchain height?
  - Can you find the hash of a specific block?
  - Open the Charts tap and explore things there.
  - What are the orphaned blocks? Are they invalid ones??
  - Find some website (or it could be the same one) that can display the content of specific transactions.
  - Look at the total number of transactions per day, is this a good rate? Compare it to the rate supported by Visa or masterCard for example!!
  - There is a figure for Hash rate distribution. Any idea what does that mean?

In Class Discussion 1.2

- Philip Tenteromano.

Want to Use Bitcoin I

- **First:** Install a wallet (e.g., visit https://bitcoin.org/en/choose-your-wallet).



All Wallets Desktop Hardware Mobile Web

Bitcoin Core

Bitcoin Knots

Eclair Mobile

Electrum

KeepKey

Ledger Nano S

mSIGNA

Mycelium

Trezor

Armory

BitBox

Bitcoin Wallet

Want to Use Bitcoin II

- **Second:** Buy Bitcoin, multiple options:
  - Cryptocurrency exchanges, such as Bitstamp, Coinbase, etc.
  - Use a classified service to find people in your area to buy their Bitcoins, such as LocalBitcoin.com
  - Sell a product for Bitcoin.
  - Use a Bitcoin ATM in your city, see: https://coinatmradar.com/

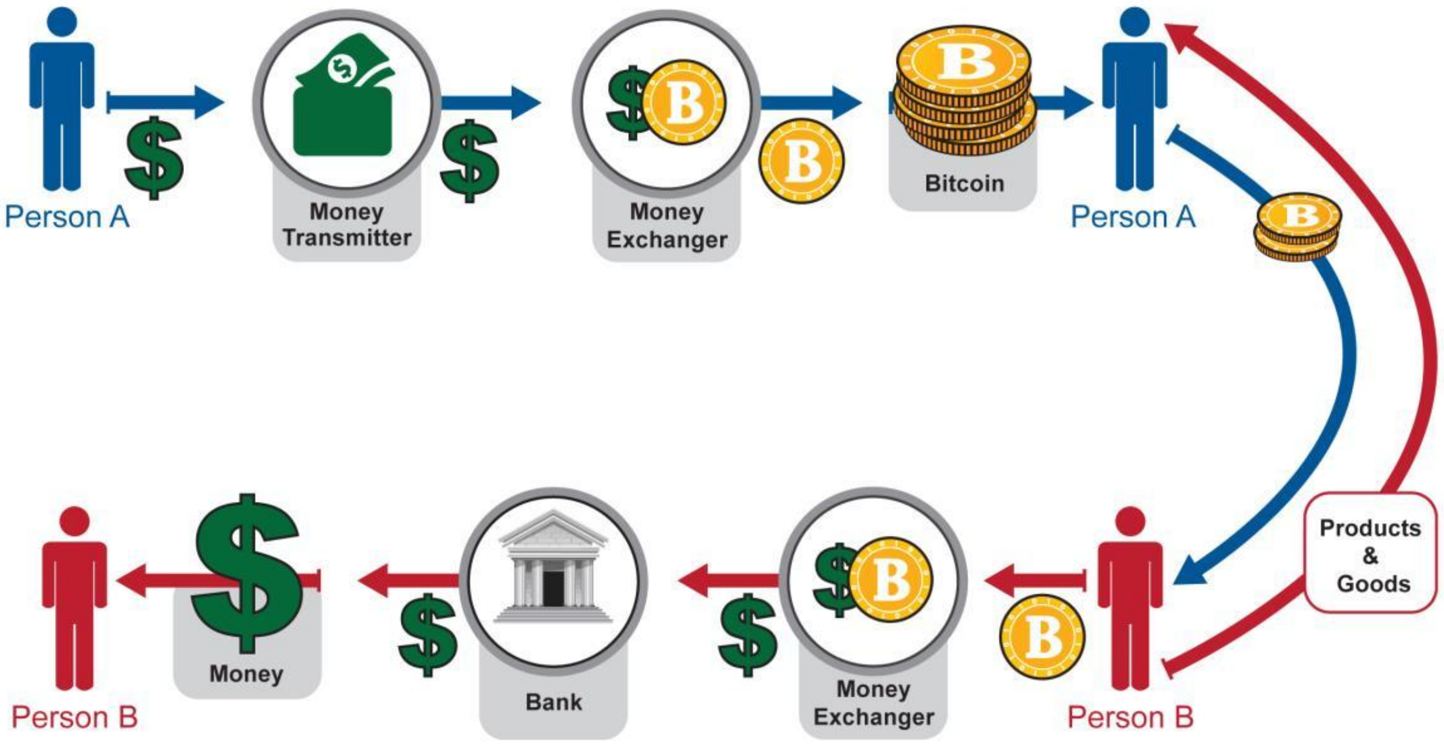
Want to Use Bitcoin III

- **Third:** Spend your bitcoins 😊 (https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/)
- Simply scan the address of the merchant and use your wallet to create a payment transaction.
- The technicality is as described before.

User Responsibility

- Maintain your set of private keys.
  - Remember without your private keys you cannot spend your previous transactions.
  - Your wallet takes care of this so be sure of selecting a trusted one.
- Change your public key periodically.
  - To hide your identity.
  - To make sure that your private key is not compromised.
- Be careful when and who to trust while using your Bitcoin.
  - Exchanges, merchants, etc.

Bitcoin and Fiat Currency



Source: http://www.fincen.gov/

For a full list of Bitcoin exchanges see: https://en.bitcoin.it/wiki/Category:Exchanges

Want to Mine Bitcoin

- Get a machine with good specifications.
- Download Bitcoin core code (see https://bitcoin.org/en/download),
- Run the miner module that does the following:
  - Discover the network by finding miners around to connect with them.
  - Retrieve a full copy of the blockchain from the discovered peers.
  - Get in sync with the network and start pooling transactions and mine new blocks.
- Costly process, nowadays individuals cannot mine on their own, they join mining pools instead (more about this later).

Hands-on Exercise 1.3

- Find a merchandize website that accepts payments in Bitcoin.
  - Pretend to buy something, move forward until the payments step and inspect the interface to pay using Bitcoin.
  - The required info to enter.
  - Other cryptocurrency options.
  - Any special instructions about payments confirmation, user identity, etc.

Course Project Proposal

- Quick overview.