

CSE 5095-007: Blockchain Technology

Lecture 3 Bitcoin - Part I

Ghada Almashaqbeh
UConn - Fall 2021

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 basic cryptographic primitives to control the money flow in the system.
 - 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.

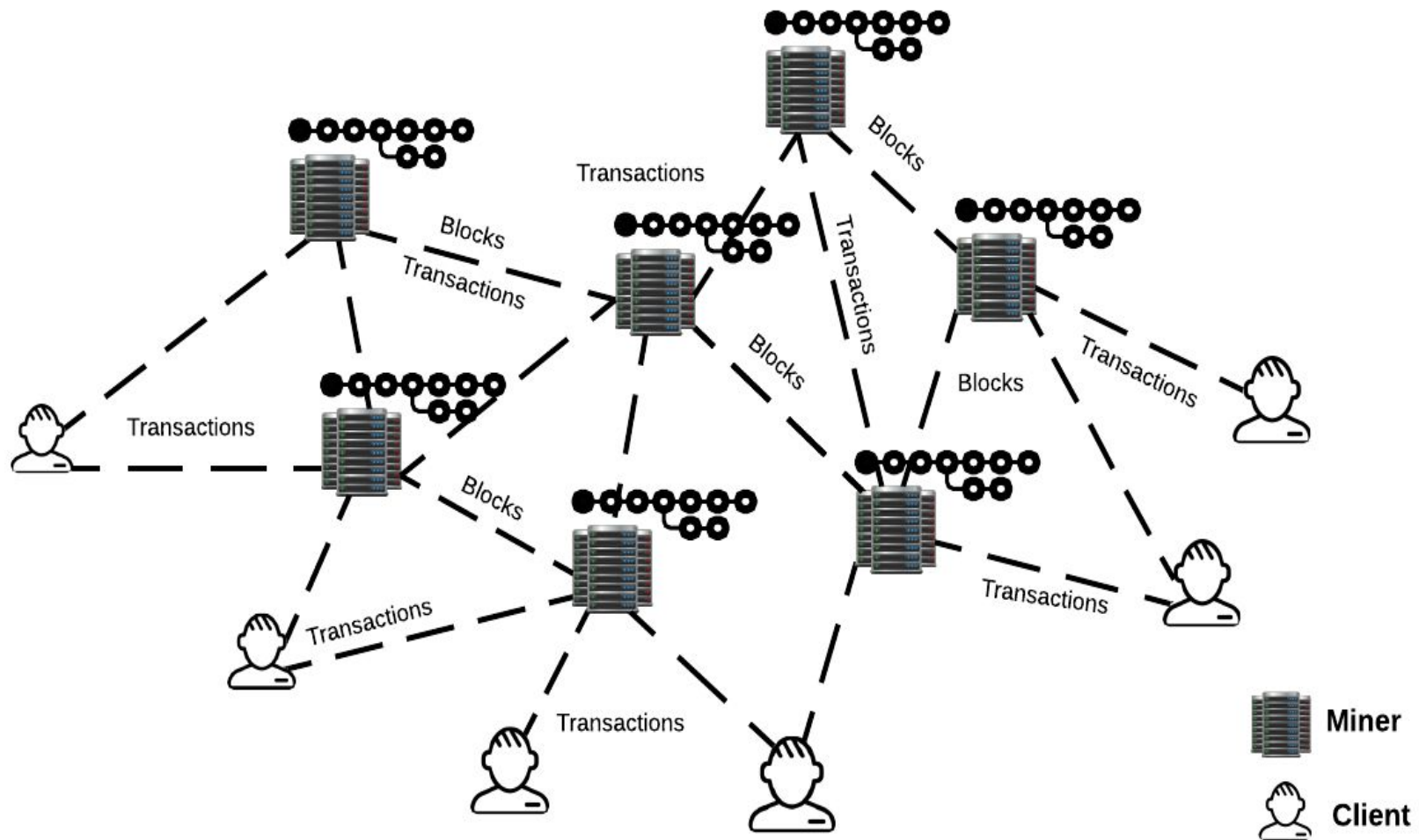
Bitcoin in a Nutshell II

- No real identities are required, just a key pair.
- Owning the private key of the destination address of 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

- **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.
- **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 strings using Base58 encoding, i.e., binary to text encoding, (see [.https://en.bitcoin.it/wiki/Base58Check_encoding](https://en.bitcoin.it/wiki/Base58Check_encoding))
 - E.g: 1B74t1WpEZ73CNmQviecbaciWRnqRhWNLy
- To promote **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.

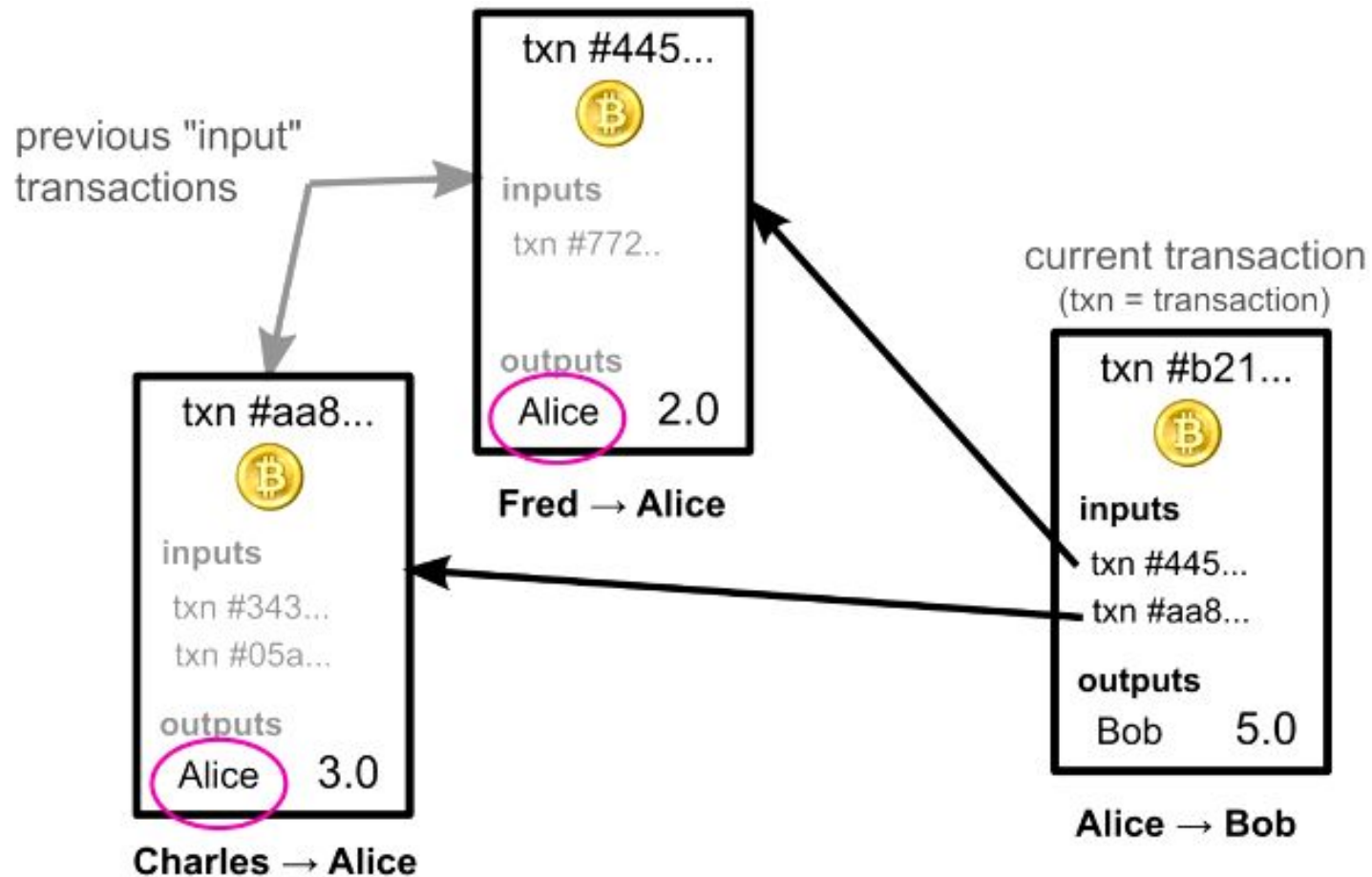
Bitcoin Transactions

- 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 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.

UTXO Model

- UTXO - Unspent transaction output.
 - 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 :)
- 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 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.

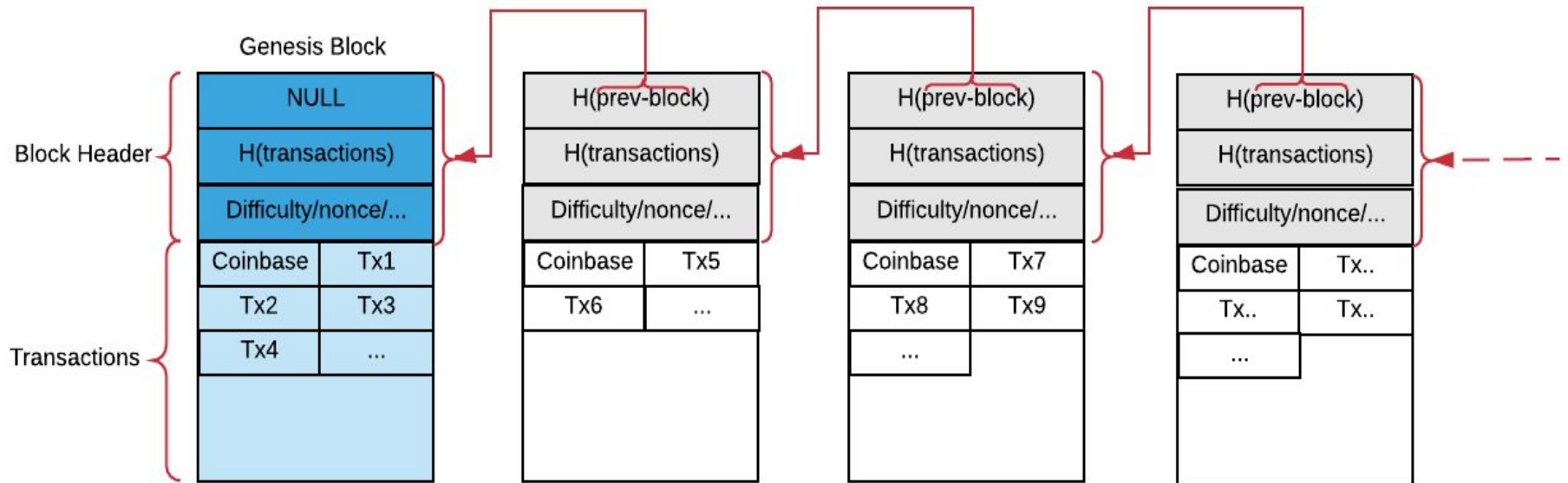
Block Header

- Consists of:
 - 4 bytes → Version: 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 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 value equals to the mining reward destined to the miner who mines the block.

The Blockchain Structure



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,

$\text{SHA-256}(\text{SHA-256}(\text{new block header})) < \text{Difficulty Target}$

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

Mining Rewards

- Miners mint 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 a coinbase transaction.
 - This transaction becomes legitimate when the block is confirmed on the blockchain.
- Currently the incentive is 6.25 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 are around 18.8 million.

Transaction Fees

- Tips for blocks creators.
 - The issuer of a transaction selects 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 will become (implicitly) mandatory.
- When mining, miners give higher priority to transactions that include high tips.

Miners Hardware

- Started by normal users and their CPUs mining, then GPUs mining, and then the ASIC (applications Specific Integrated Circuits) mining.
 - Now there are mining pools with huge data centers.
- Example: Bitfury miner center: <http://www.bitfury.org/>

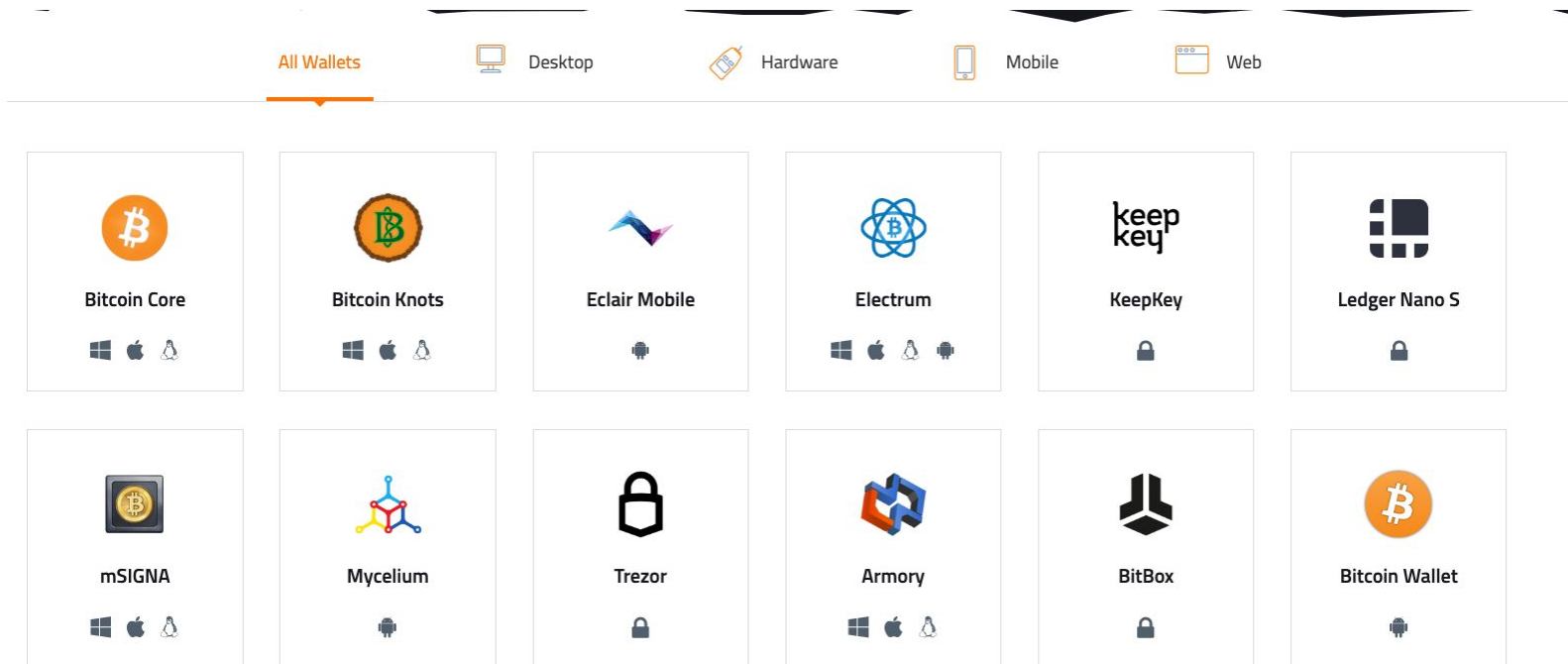


Want to Mine Bitcoin

- 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).

Want to Use Bitcoin I

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

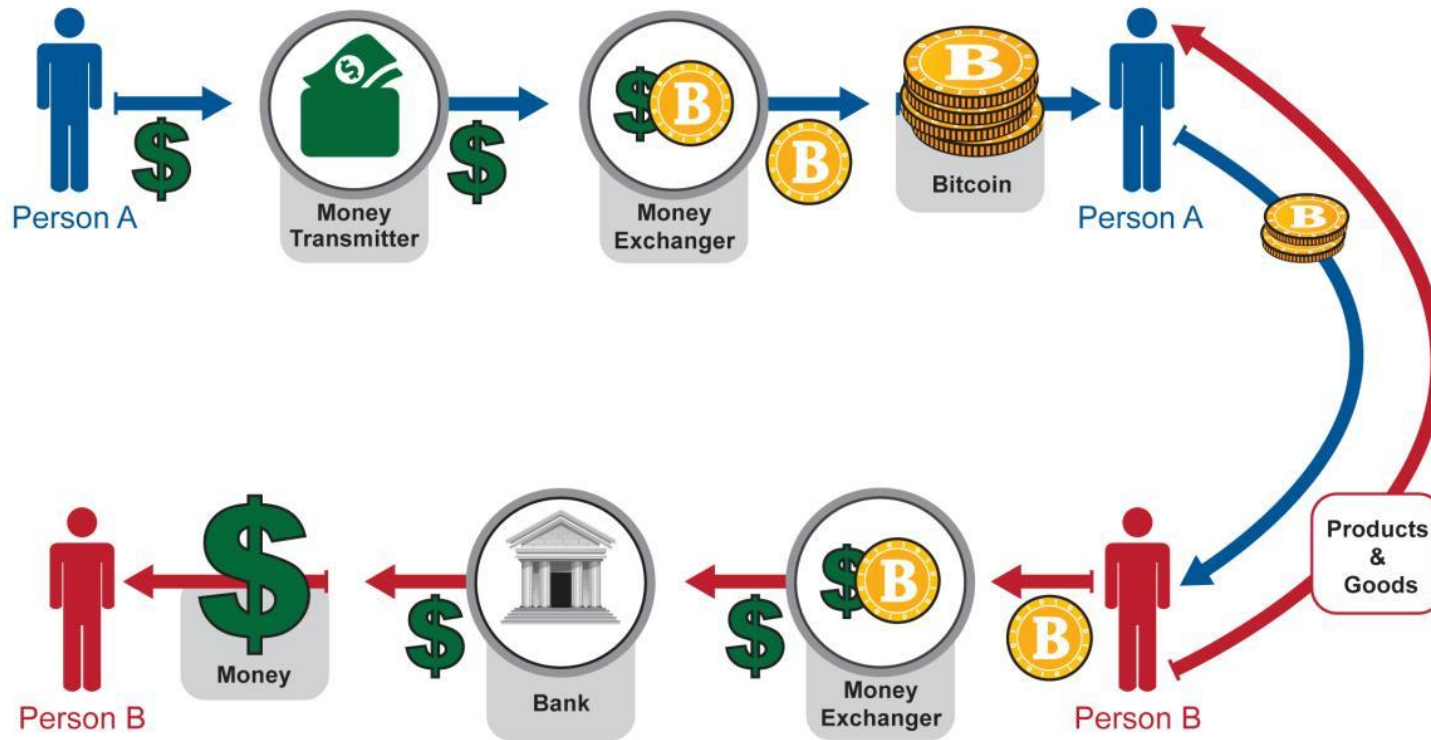


Want to Use Bitcoin III

- **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.



Bitcoin and Fiat Currency



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

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

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.

