ECE-GY 9383
Special Topics in Network Security

12 - Blockchain

Slides credits: Shivendra S. Panwar, Fraida Fund

CSE/ECE zjzhao

NYU | TANDON SCHOOL OF ENGINEERING

“Blockchain”?

“To understand the power of blockchain systems, and the things they can do, it is important to distinguish between three things that are commonly muddled up, namely the bitcoin currency, the specific blockchain that underpins it, and the idea of blockchains in general.”

The Trust Machine, The Economist, Oct 31, 2015

“Telephone”?

1) the idea of having “distance voice” supported by the technology

2) A specific telephone network

3) A specific use case over the network, ex. local call, fax, … …

Blockchain general view

A blockchain is a **digital ledger** (collection of transaction records, ex. on P2P online currency) that is

- "Public”
- Distributed
- Append-only
- Tamper-proof
- Auditable
- Authenticated

Blockchain: the basic idea

1. A transaction record is created
2. The transaction is broadcast to a P2P network (and validated)
3. Groups of transactions are organized into **blocks** (containing list of recent transactions and reference to previous block)
4. **Proof of work** (PoW) is computed and added to the block
5. New block is added to the chain (recall: each block also contains a reference to the previous one)

Blockchain security mechanisms

- Cryptographic **signatures**, ex. ECDSA is commonly used to verify the authenticity of transactions
- PoW-based consensus protocol, which one party (the *prover*) proves to others (the *verifiers*) that a certain amount of computational effort has been expended for securely sequence of transactions

Blockchain application: Bitcoin

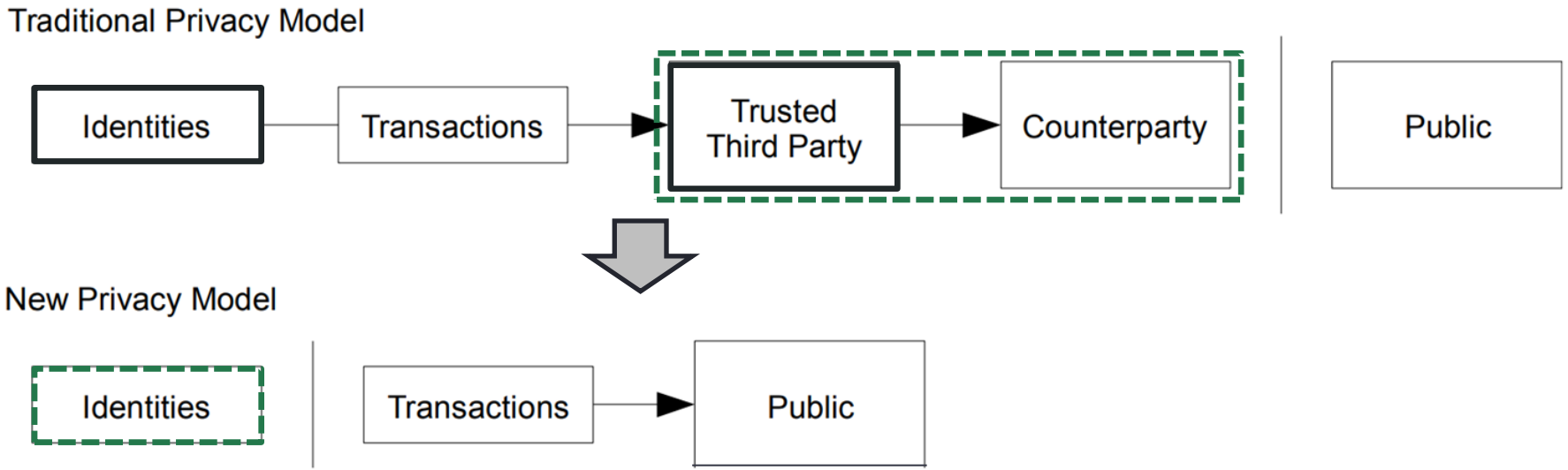
Bitcoin: a digital currency that uses cryptography to address key concerns -

- Can I be sure it is authentic/not counterfeit?
- Can I be sure that it can be spent only once?
- Can I be sure of who it belongs to (and can I prove it belongs to me)?

Also offers privacy, decentralized control.

Ref: https://bitcoin.org/bitcoin.pdf

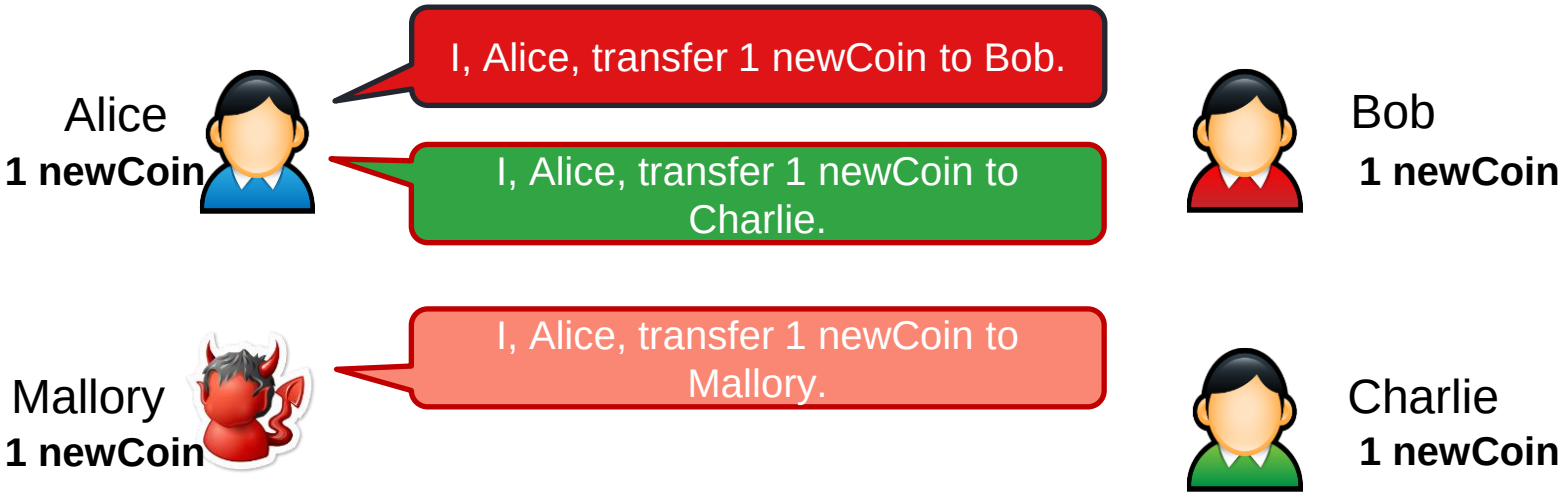
Blockchain application: Bitcoin transaction privacy



Why decentralized, online currency hard?

- The most obvious challenge is determining ownership
  - Who owns a given unit of currency?
- Without strong ownership…
  - Forgery – a user can mint arbitrary currency
  - Double spending – how do you validate and enforce transactions?
  - Theft – impossible to separate true and false claims about ownership

Hypothetical currency *newCoin* transaction example

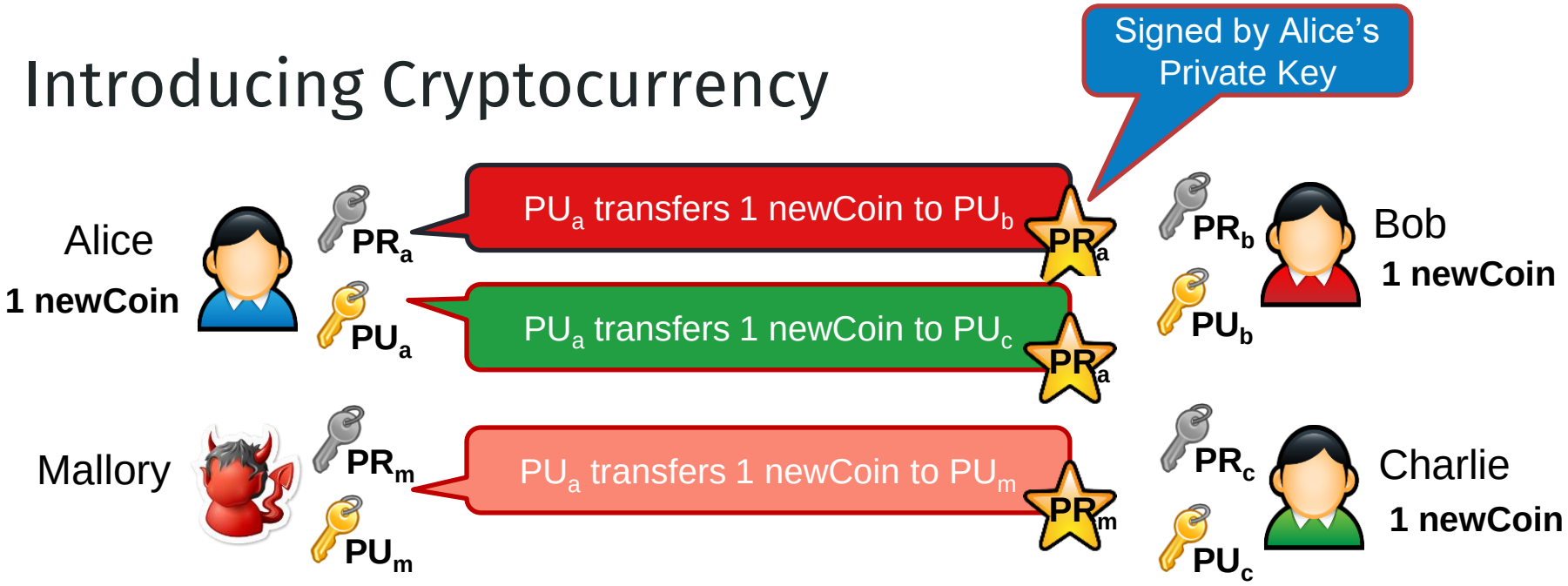


Can transactions be forged?

Can newCoins be stolen?

Can users double spend?

Introducing Cryptocurrency



Can transactions be forged?

Can newCoins be stolen?

Can users double spend?

Bitcoin transaction with Cryptocurrency Wallet

Alice and Bob each have a **wallet** - a collection of triplets.

- Private key (256-bit ECDSA)
- Public key
- Address (25-34 character hash of public key)

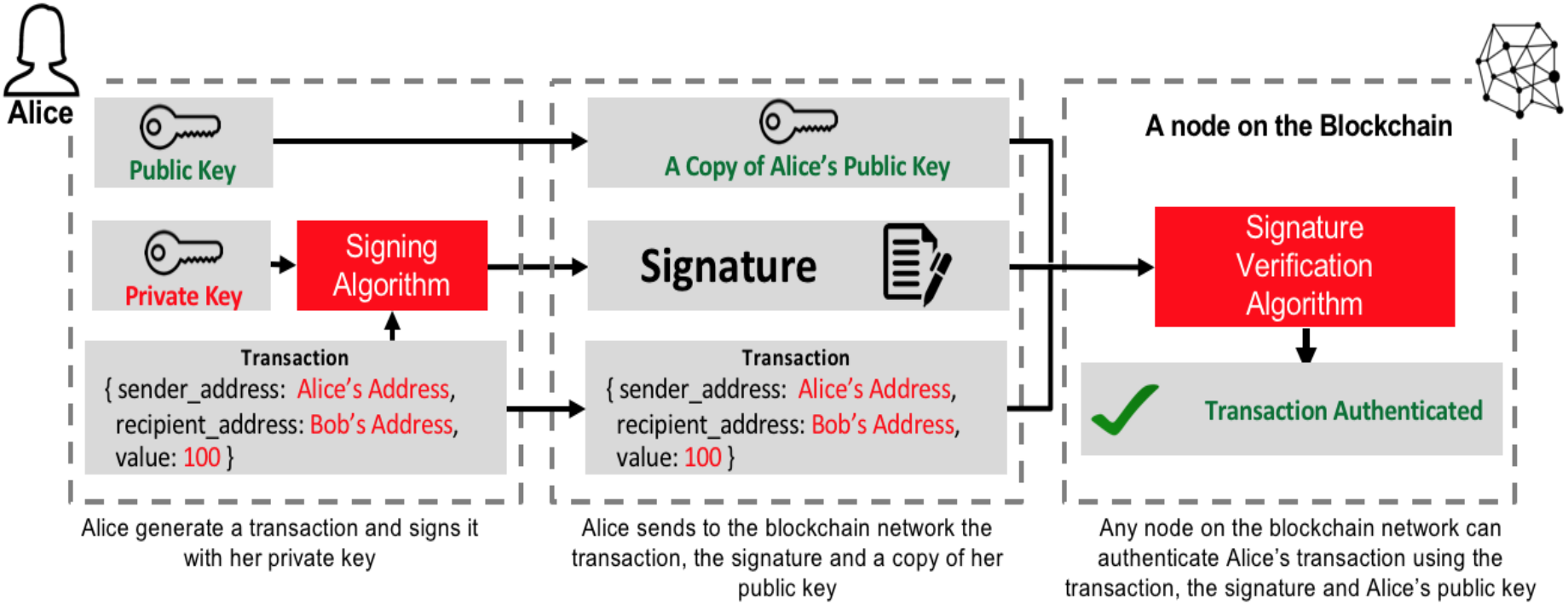
Typically, a master key pair will be used to derive a series of child key pairs, each with corresponding address.

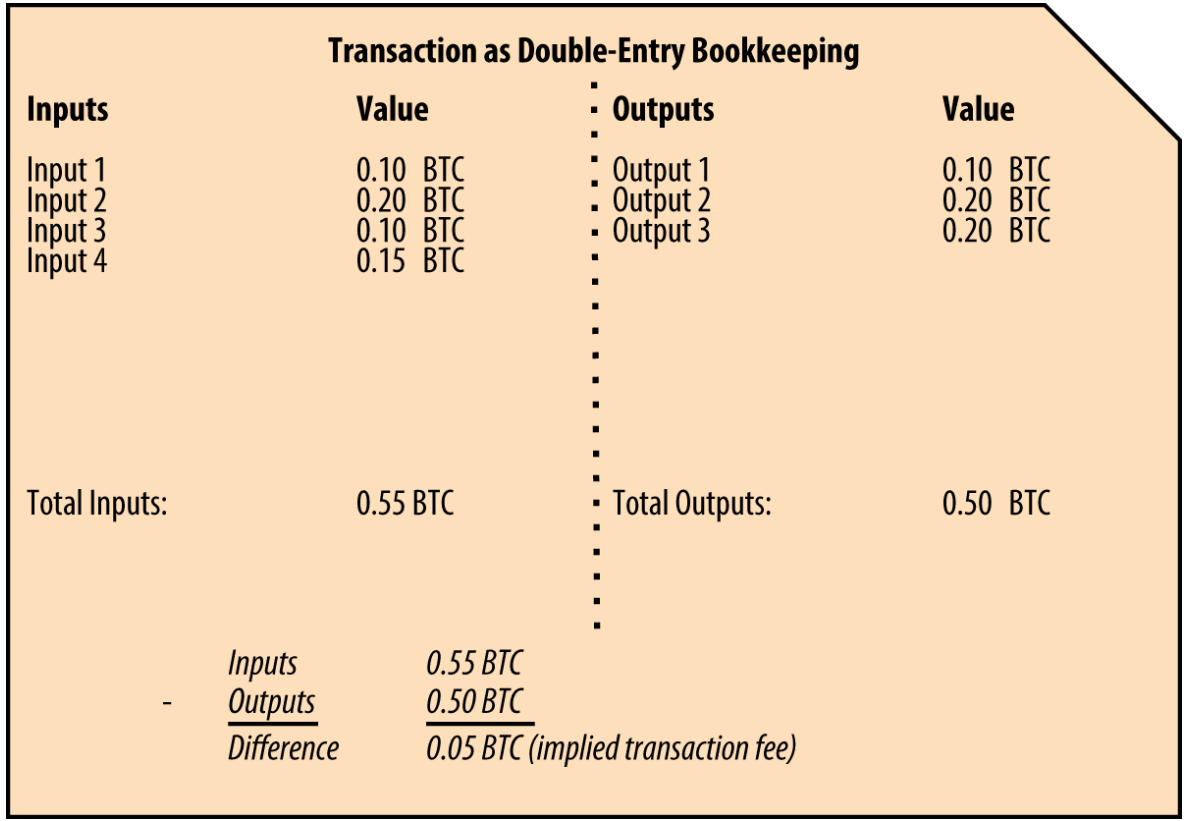
The wallet stores the public and/or private keys that can be used to track ownership, receive or spend Bitcoin

A Bitcoin transaction

- Alice wants to pay Bob
  - Alice has acquired some currency from previous transactions
  - Bob has shared an address with Alice
- The transaction will have **inputs** and **outputs**
  - Difference is implied transaction fee
  - Wallet application, local client or online service, will figure out which previous transactions to use as inputs
  - “Change” can be paid as output to Alice’s address
- Alice’s wallet application creates transaction (in a record)
  - Alice signs by her private key; signature and her public key are included in the record; all used for signature verification to make the transaction authenticated
  - Creates script that says: this amount of currency may be spent by anyone who can produce a signature that could only be produced by Bob’s corresponding private key

Authentication process for Bitcoin transactions



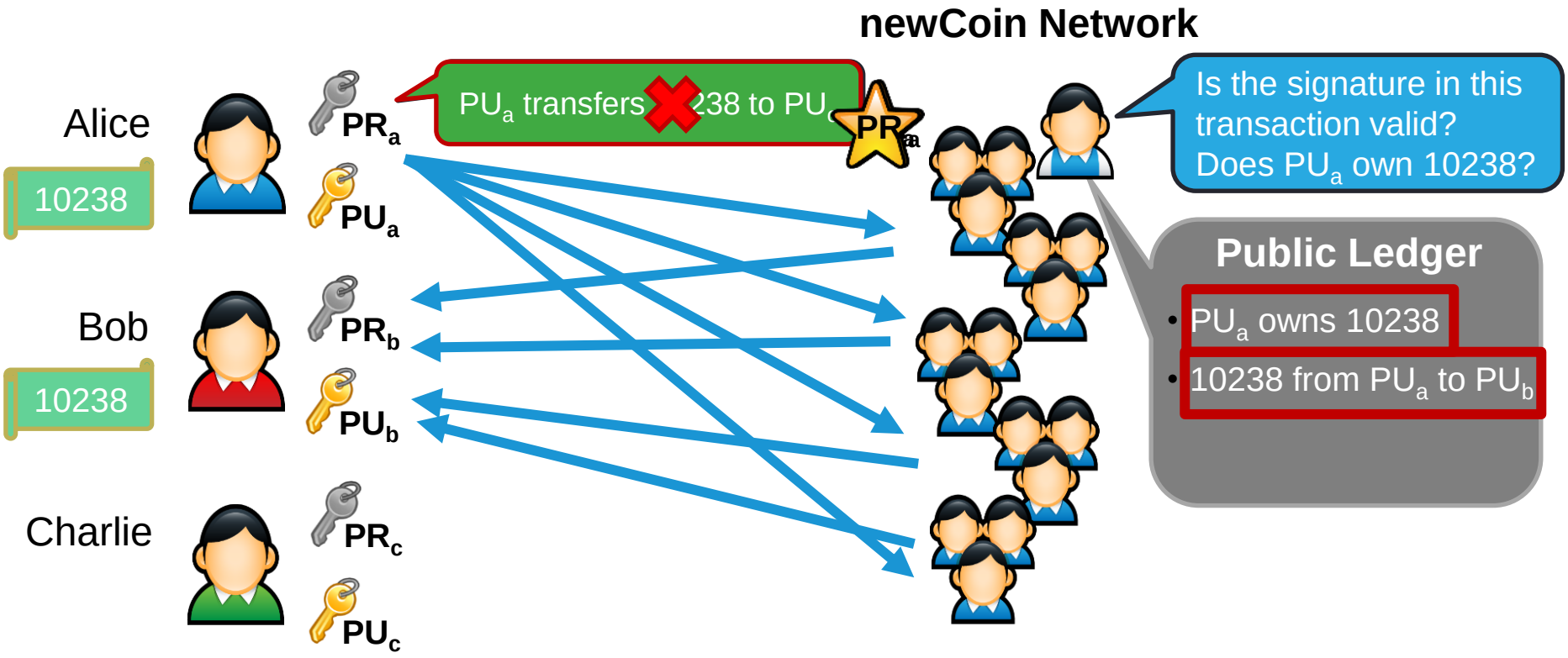

Transaction as Double-Entry Bookkeeping
Inputs
Value
Outputs
Value
Input 1
Input 2
Input 3
Input 4
0.10 BTC
0.20 BTC
0.10 BTC
0.15 BTC
Output 1
Output 2
Output 3
0.10 BTC
0.20 BTC
0.20 BTC
Total Inputs:
0.55 BTC
Total Outputs:
0.50 BTC
Inputs
0.55 BTC
-
Outputs
0.50 BTC
Difference
0.05 BTC (implied transaction fee)


nsaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18
INPUTS From
m (previous transactions Joe has received):
Joe 0.1000 BTC
OUTPUTS To
Output #0 Alice's Address 0.1000 BTC (spent)
Transaction Fees: 0.0000 BTC
nsaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
INPUTS From
7a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
Alice 0.1000 BTC
OUTPUTS To
Output #0 Bob's Address 0.0150 BTC (spent)
Output #1 Alice's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC
nsaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4
INPUTS From
7052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob 0.0150 BTC
OUTPUTS To
Output #0 Gopesh's Address 0.0100 BTC (unspent)
Output #1 Bob's Address (change) 0.0045 BTC (unspent)
Transaction Fees: 0.0005 BTC

A Bitcoin transaction (cont'd)

- Alice's wallet sends transaction to other nodes on Bitcoin network
  - Transaction will be flooded through the network
  - The network become the "bank" to keep track all transactions with a public ledger, a.k.a. blockchain
- Transaction is part of blockchain when it is verified and included in a block
  - Transaction ID, simply the hash of its fields, is used in tracking

Preventing double spending

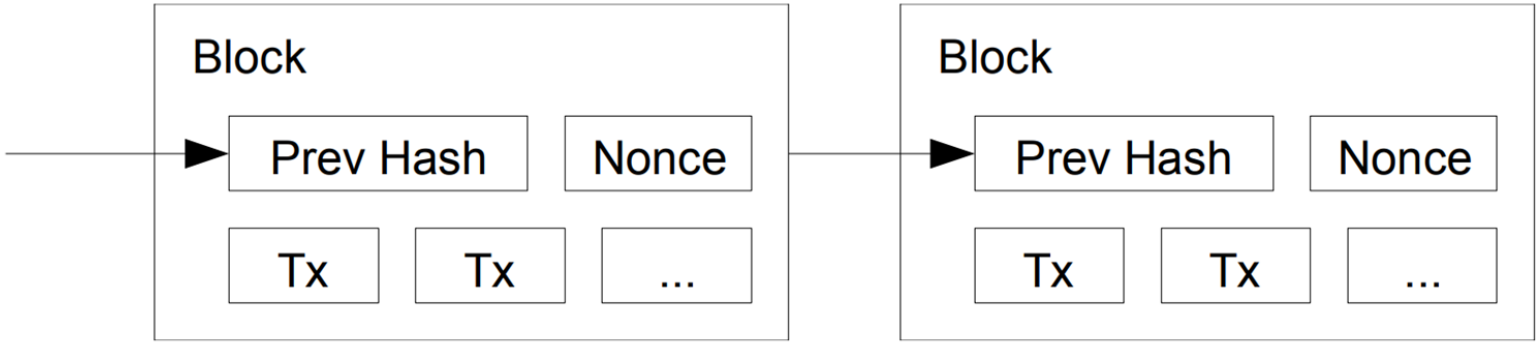


Bitcoin Mining - the process of adding new blocks

- Every ten minutes, network tries to produce a block with pending transactions
- **Miners** solve a cryptographic puzzle to successfully produce a block:
  - Find **nonce** such that, when included in the block, hash of the block is smaller than some **target** value, i.e. begins with *n* zero bits
  - Successful miner gets reward (new coins) and all transaction fees from the block
- Average work required is exponential in *n*
  Target can be adjusted to change difficulty
- Can be verified in a single hash
  Other nodes will verify and add to blockchain

Bitcoin Mining (cont'd)

- Every block in blockchain contains hash of previous block
- To modify a block, must redo the work of that block and all following blocks!



More on the Mining

- In theory, anyone can download bitcoin and start mining
  - Your node will search for blocks
  - But in practice, you will *never win*
- Arms race: CPU < GPU < FPGA < ASICs
  - Real miners use thousands of chips custom designed to solve cryptopuzzles
  - Much faster and more power efficient than general purpose hardware
- Many miners operate in places with cheap/free power and cooling

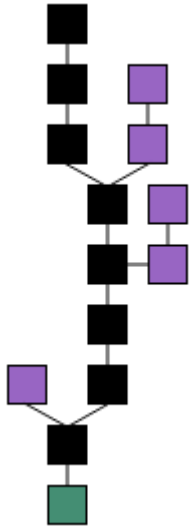
Bitcoin Finney attack

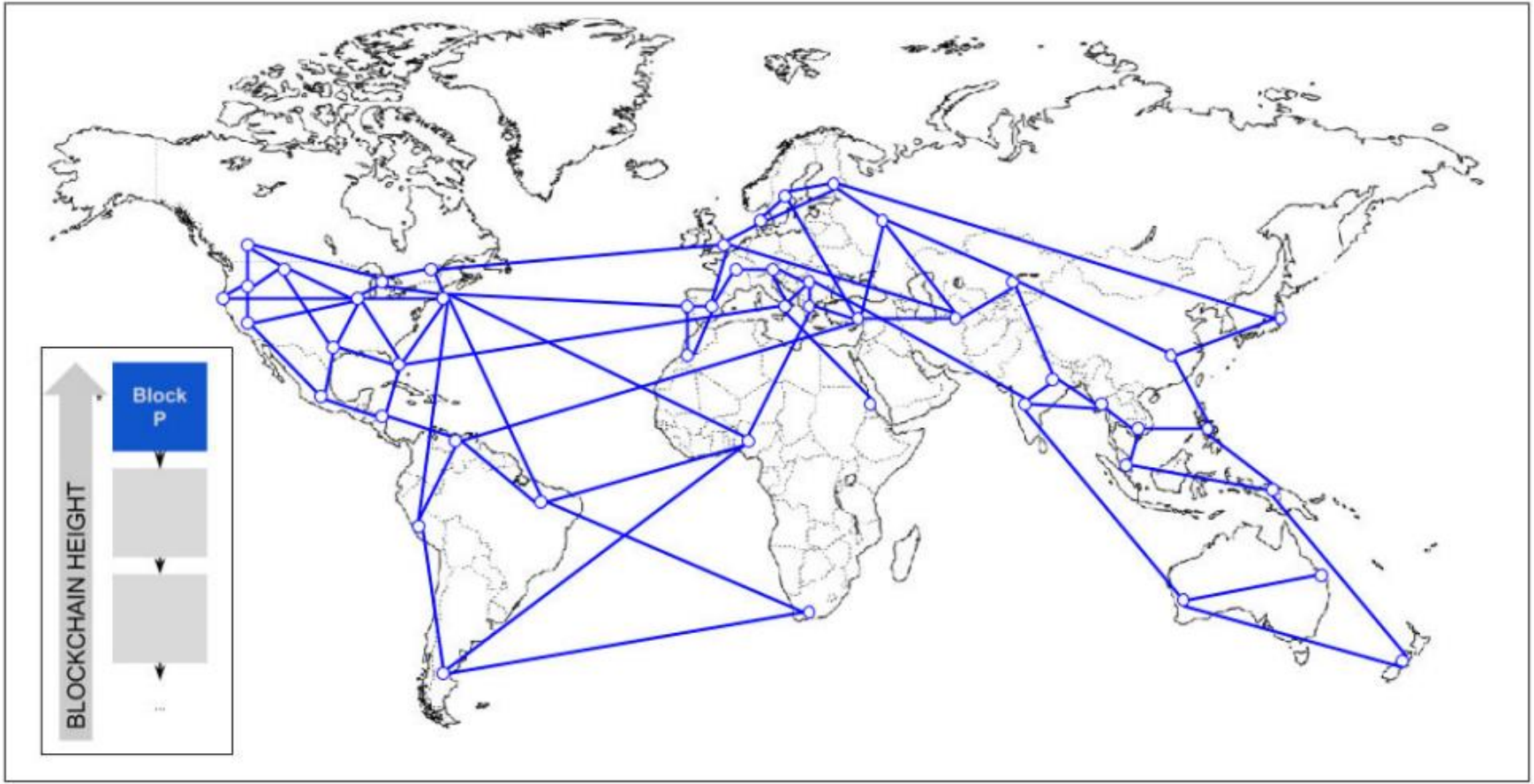
- Finney attack:
  - Attacker mines a block in which he/she spends coin, but doesn't broadcast it
  - Attacker purchases some good (irreversibly) with that same coin
  - Attacker broadcasts pre-mined block
- Suppose time from finding the block until the attacker sends payment and the merchant accepts it is t, and average time to find a block is T - attack will fail with probability t/T, and attacker also will lose out on reward for mining block.
- Solution: merchants should not accept 0-confirmation blocks.

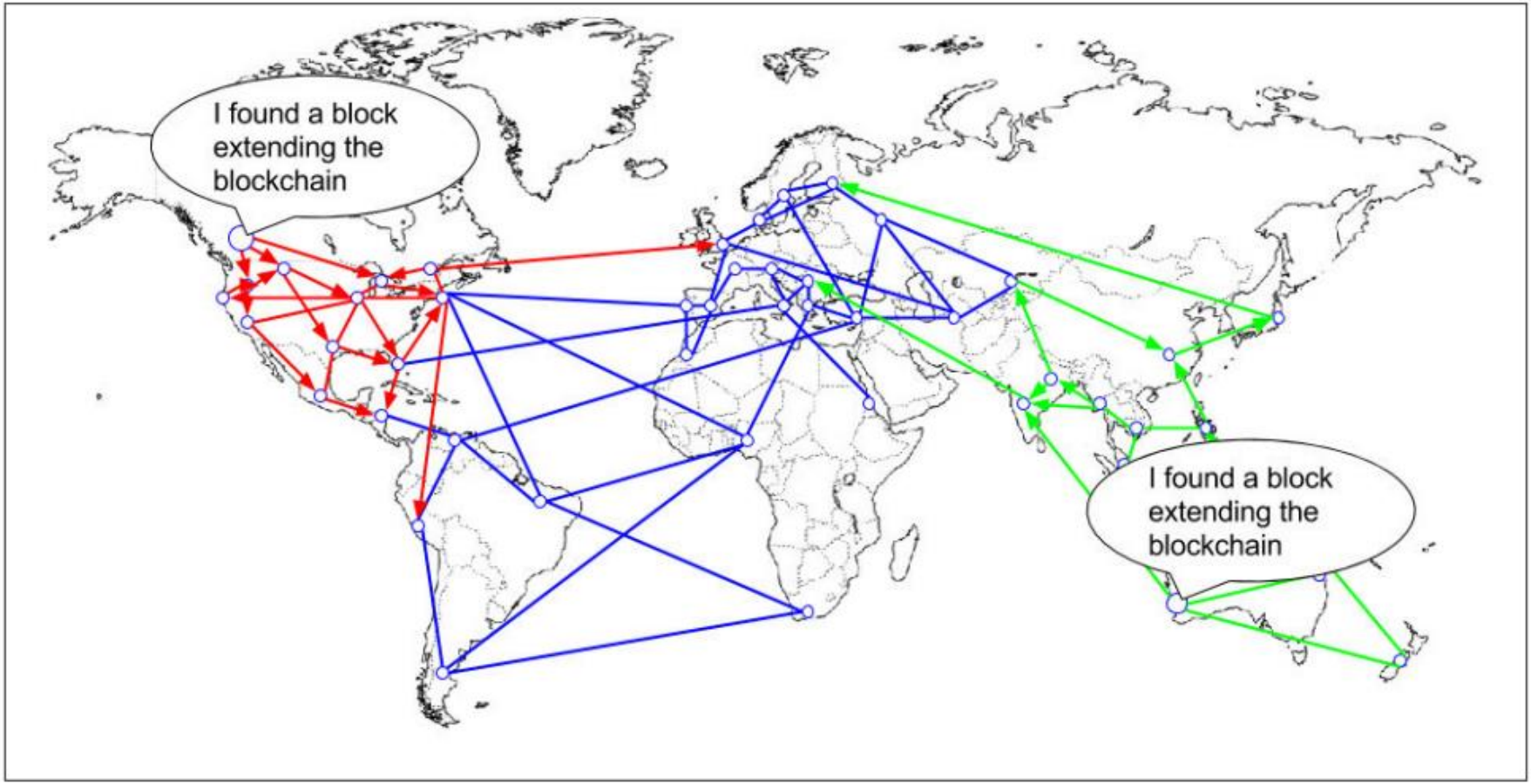
Rules for Bitcoin transaction

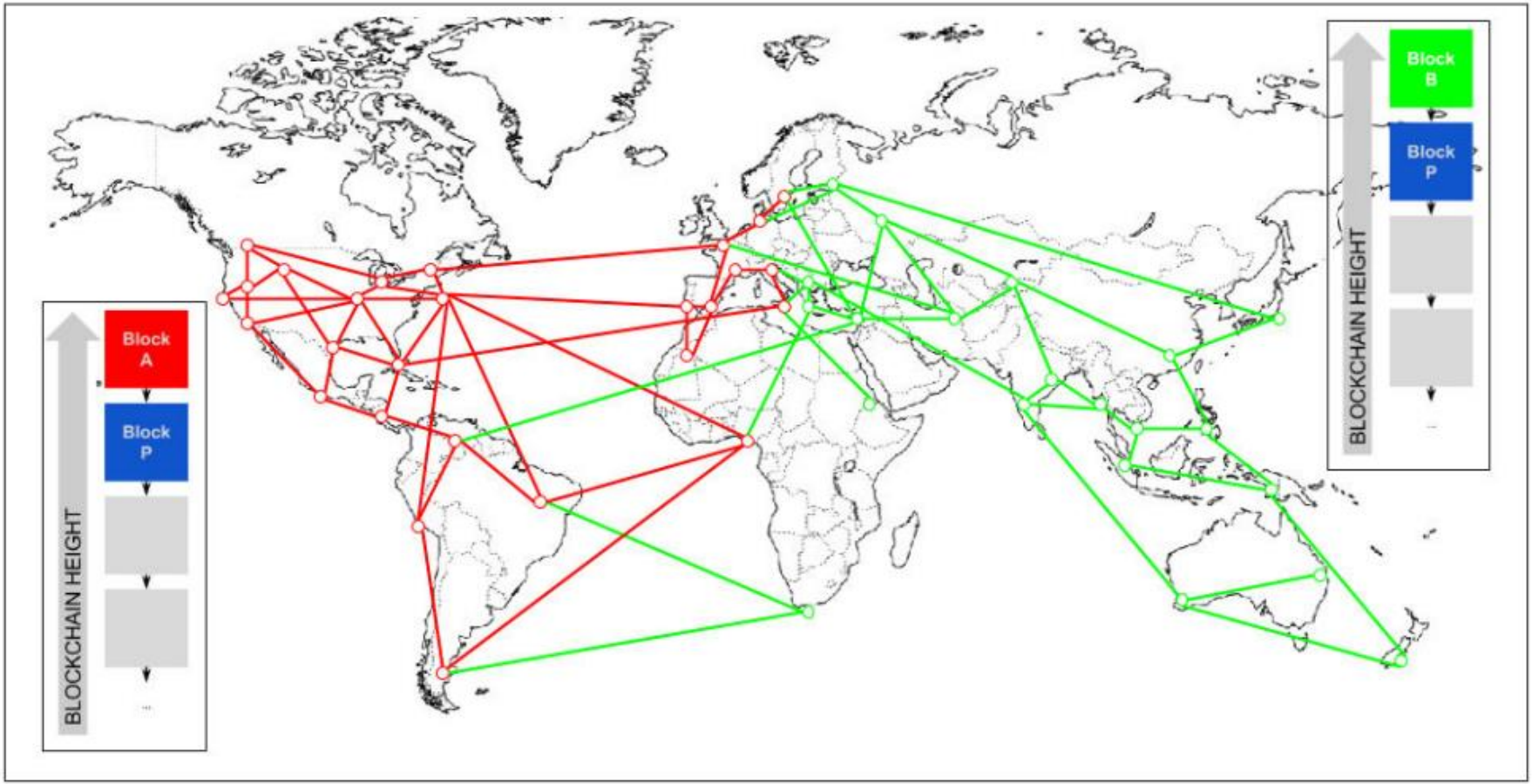
- Recipient won’t accept input until some number of additional blocks have been added to the blockchain
- (Also, miner cannot spend reward until some number of additional blocks have been added to the blockchain)

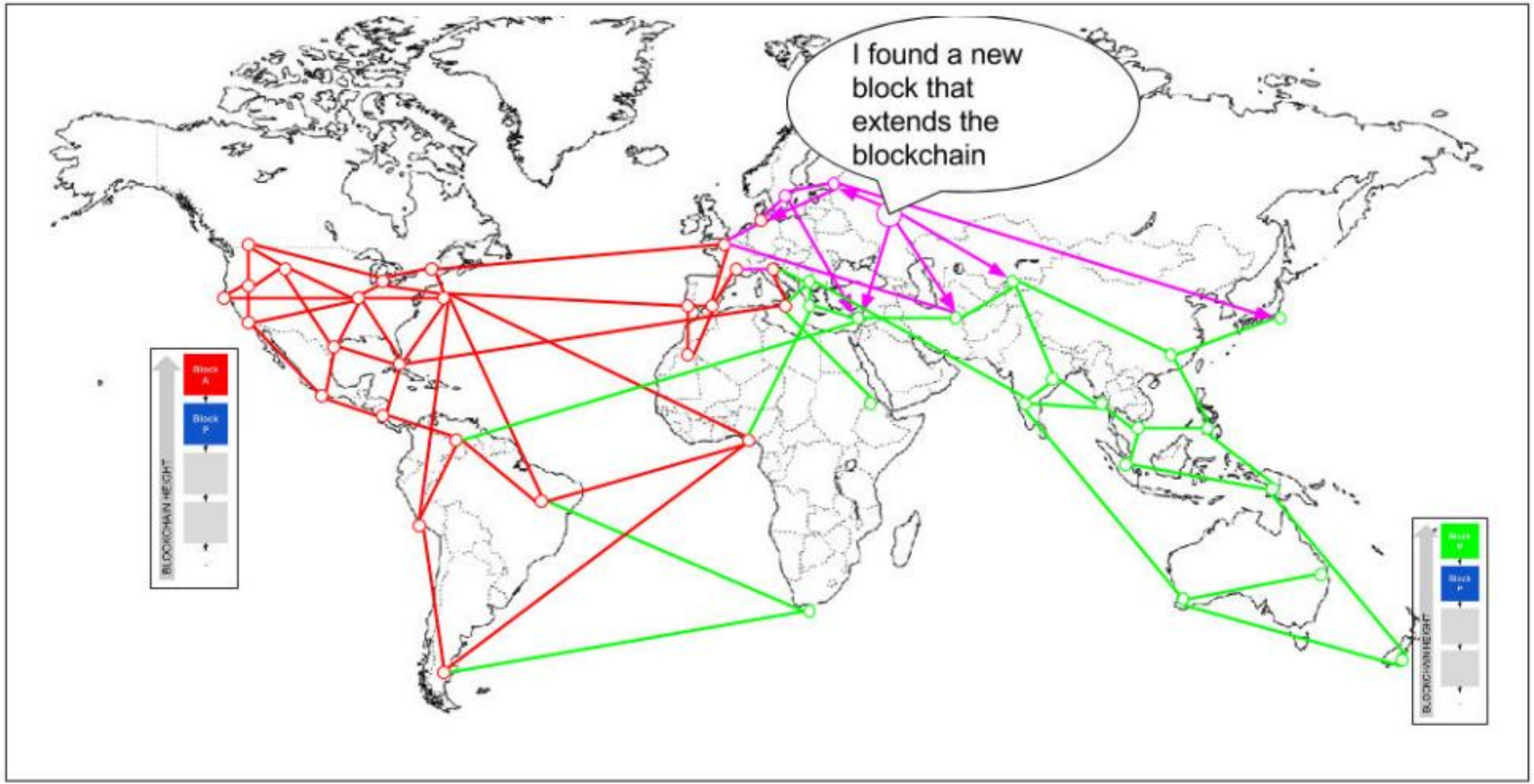
  Prevents double-spend with network fork
  Longest-chain rule

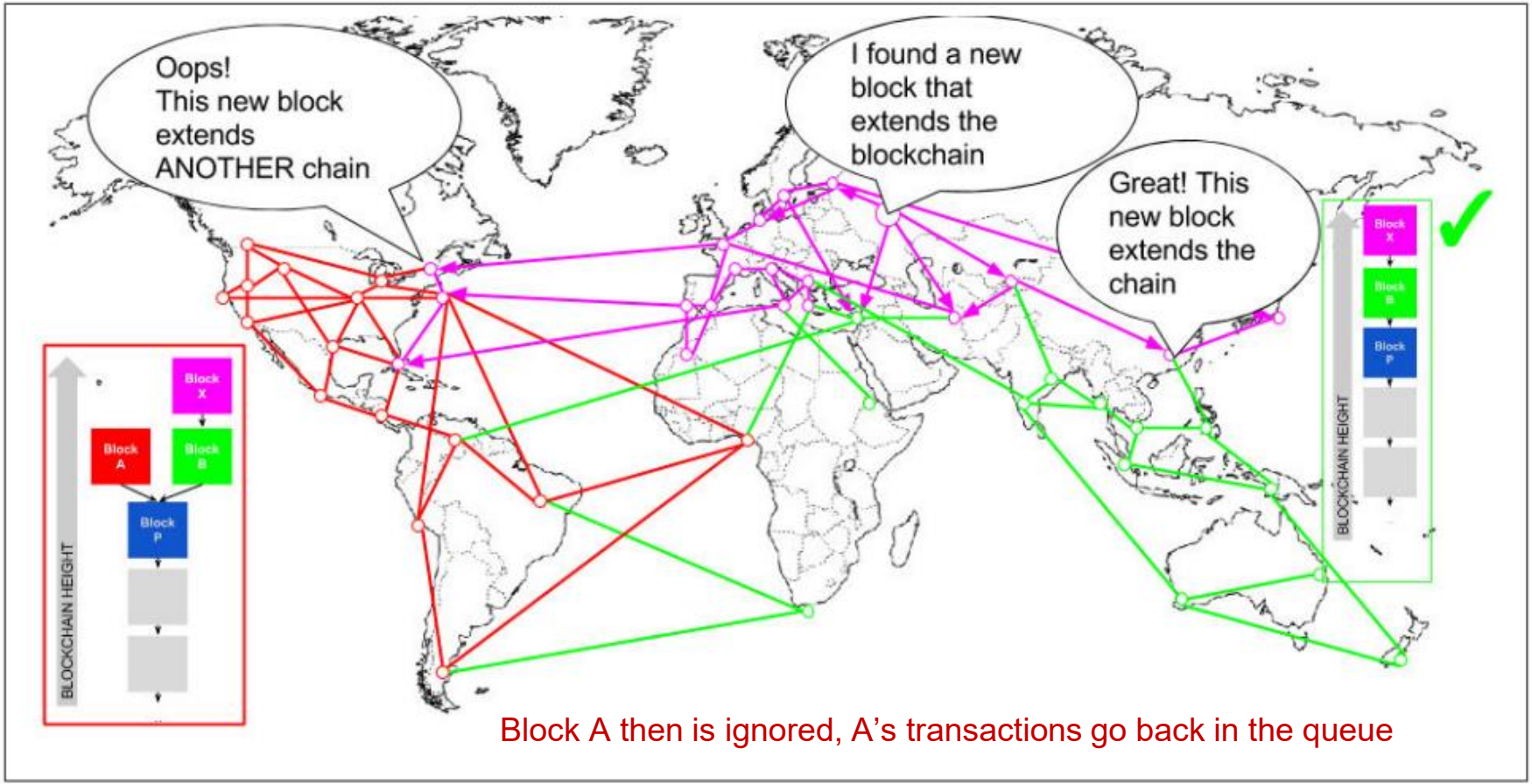



BLOCKCHAIN HEIGHT
Block
P
...


I found a block extending the blockchain
I found a block extending the blockchain

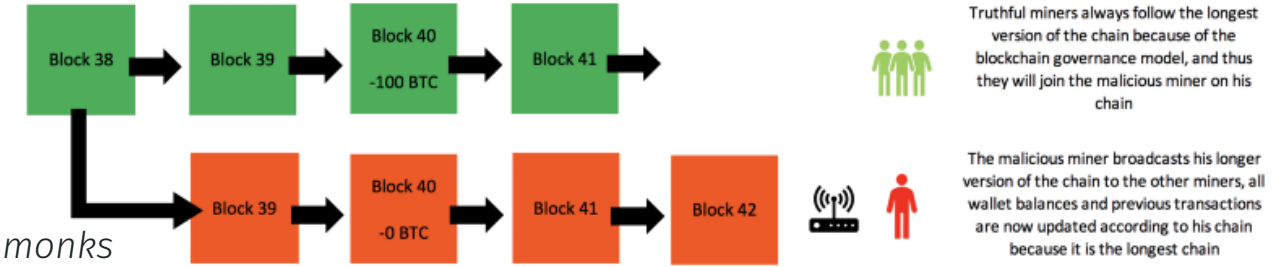

Block
A
Block
P
BLOCKCHAIN HEIGHT
Block
B
Block
P
BLOCKCHAIN HEIGHT


I found a new block that extends the blockchain
BLOCKCHAIN HEIGHT
Block A
Block P
BLOCKCHAIN HEIGHT


Oops!
This new block extends ANOTHER chain
I found a new block that extends the blockchain
Great! This new block extends the chain
Block X
Block A
Block B
Block P
BLOCKCHAIN HEIGHT
Block X
Block B
Block P
BLOCKCHAIN HEIGHT
Block A then is ignored, A's transactions go back in the queue

Bitcoin attack: Majority attack (51% attack)

- Attacker submits a transaction which pays merchant
- Attacker privately mines a blockchain fork in which a double-spending transaction is included
- After waiting for *n* confirmations, the merchant sends the product
- If/when the attacker has found more than *n* blocks, he releases his fork, it is accepted by the network, and he regains his coins



Source: *Coinmonks*

Probability of success depends on attacker's hashrate as proportion of network hashrate, and number of confirmations required by merchant.

Bitcoin attack: Majority attack (cont’d)

Having 51% of the hashrate *does not* allow attacker to:

- Reverse other people's transactions without their cooperation
- Create coins without doing the work
- Send coins that never belonged to him

But this may result in control of all future blocks by attack

- Network needs to be diverse to prevent this kind of attack

Bitcoin vulnerabilities

- User must still rely on a third party to convert Bitcoin to other currencies
  Bitcoin exchange or merchant may compromise user privacy
- Wallet can be stolen
  - Hackers get private keys, transfer bitcoins to themselves
- Bitcoin weakness discussion: https://en.bitcoin.it/wiki/Weaknesses

Emerging blockchain application – crypto collectibles

- Bitcoin is fungible (exchangeable and divisible); Bitcoin transaction is non-fungible (unique and not interchangeable record)
- NFTs, cryptographic Non-Fungible Tokens, can be stored in a blockchain pointing to digital assets on their unique properties, verifiable via the ledger
- NFTs are popularly used to commodify digital collectibles/assets in art, music, sports, and other popular entertainment
- NFTs can be auctioned, treaded in NFT markets
- Diff. blockchain uses its own token standard. Ex. ERC-20 tokens by Ethereum

References

- “Mastering Bitcoin: Unlocking Digital Cryptocurrencies”, Andreas M. Antonopoulos
- "Bitcoin: A peer-to-peer electronic cash system,” Satoshi Nakamoto
- Bitcoin Wiki, https://en.bitcoin.it/wiki/Main_Page
- Breaking Analysis on NFTs, https://wikibon.com/breaking-analysis-nfts-crypto-madness-enterprise-blockchain/

BACKUP SLIDES

Is Bitcoin Secure?

- Can I fake a transaction? (i.e. steal your bitcoins)
  - No, you would need access to the victim's private key
- Can I edit the blockchain? (i.e. remove or modify old transactions)
  - No, all blocks are linked by their hashes
  - Changing historical block B_t would require changing all blocks $[B_t, B_{current}]$
- Can I repudiate a transaction? (i.e. deny that I paid you)
  - No, all of your transactions are signed by your private key
  - Plus, you can't go back and change previous blocks
- Can I mint money out of thin air?
  - Yes, but only through legitimately solving a cryptopuzzle (i.e. a coinbase txn)
  - All peers can validate that your block (and the minted coins) are correct

What About Double Spending?

- Can I double spend?
  - Sort of – you could publish two new transactions with the same inputs
  - But, the network will only accept of them *eventually*
- However, there may be a period of time where both new transactions are committed
  - If the blockchain forks, both transactions may exist concurrently
- When should a recipient conclude that a transaction is truly accepted?
  - Wait for *C* confirmations, i.e. blocks **after** the transaction in question
  - The longer the chain, the less likely it will be replaced by a fork
    - If a vendor requires 6 confirmations and an attacker controls 10% of the networks hashing power, the attack will succeed 0.02428% of the time

CPU Monopoly

- What if I control 51% of the networks hashing power?
  - All bets are off
  - Attacker can control all future blocks
    - Monopolize creation of new coins
    - Double spend
    - Deny arbitrary transactions

- Network needs to be diverse to prevent this kind of attack

Incentives, Revisited

- Why do nodes accept transactions?
  - Coinbase transactions and transaction fees
  - Essentially, monetary rewards

- Why do nodes “accept” a new block?
  - Couldn’t they just ignore it and keep mining the old one?
  - No incentive: mining is guessing, so it’s not like you are “close”
  - Also, all other nodes will switch to new block
    - To succeed, you now need to mine two blocks in a row

What About Anonymity?

- Are bitcoin transactions truly anonymous?
  - No, transactions are pseudonymous
  - Everyone is identified by their public key(s)
- The blockchain (all transactions ever) is public
  - Current owner of any coin can be determined
  - The provenance of any bitcoin can be ascertained (past ownership)
- Related question: are bitcoins fungible?
  - *Fungible* – mutually interchangeable
  - Physical dollars are fungible, one is just as good as another
  - Since the provenance of bitcoins can be tracked, they may not be fungible
    - E.g. if coin *X* is stolen, user may refuse to accept *X* in future transactions in retaliation