Bitcoins and Blockchains

Chester Rebeiro

Assistant Professor
Department of Computer Science and Engineering
IIT Madras

Traditional Currencies

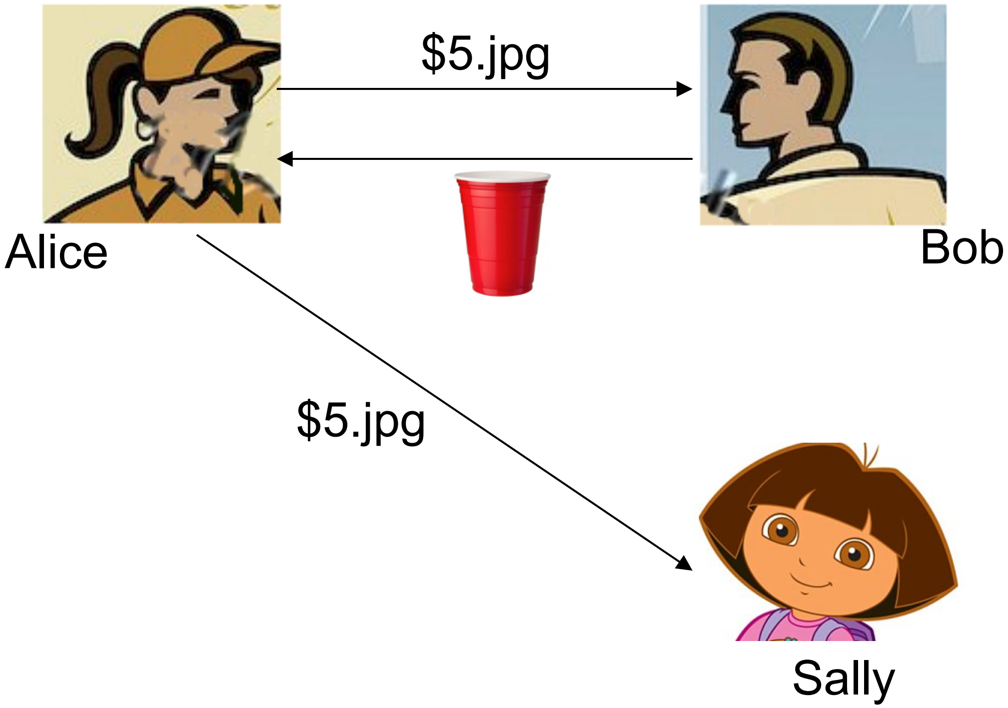
Alice gives bill to Bob, Bob gives coffee to Alice

Characteristics of Paper Money

- No double spending
  - Once Alice given Bill to Bob, she cannot use the same bill for another transaction
- Not Reversible
  - Once transaction is done, cannot be undone
- Transactions need not be between trusted parties
  - Alice and Bob don’t need to trust each other
- Privacy
  - Besides Alice and Bob, no body else knows about the transaction

Electronic Money

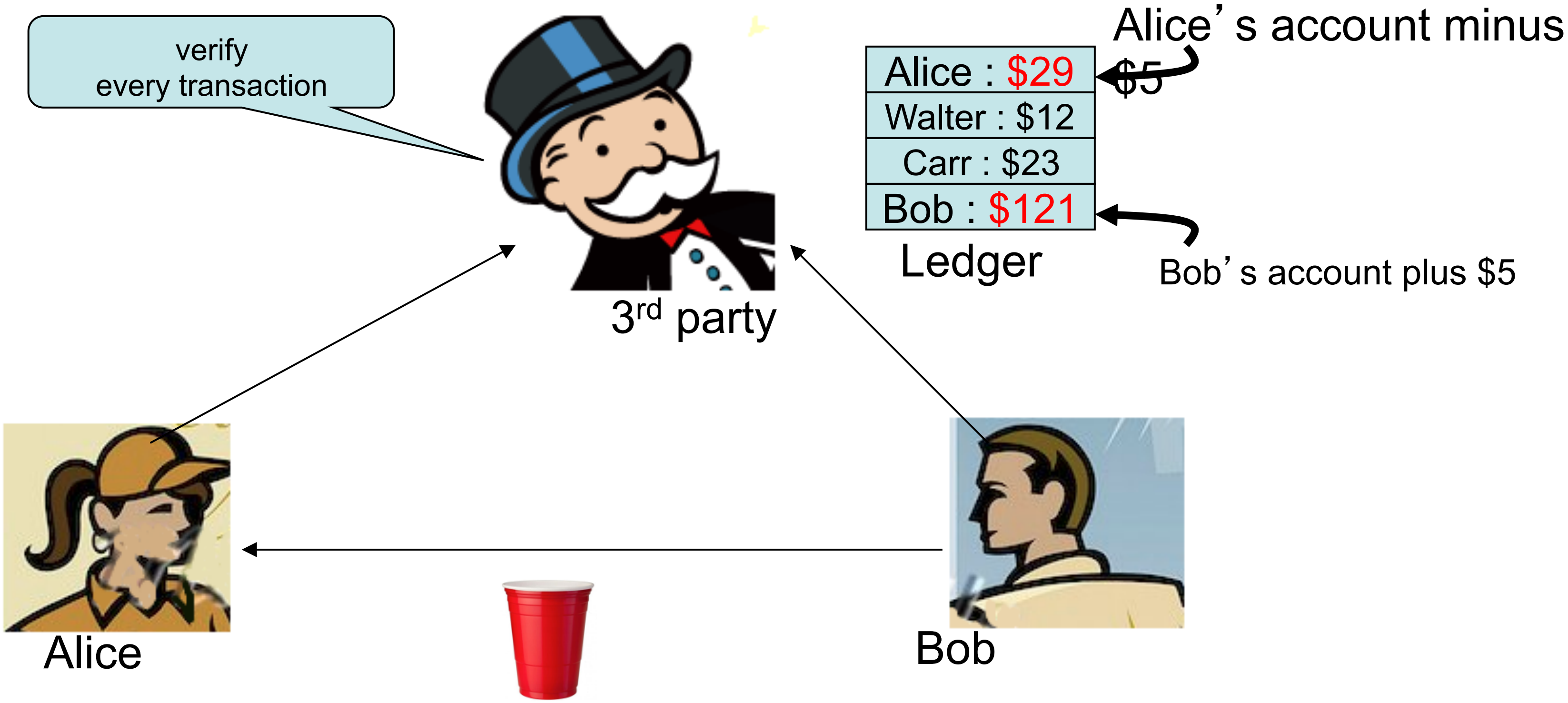
- What if Alice and Bob want to transact over the Internet
- Naïve Approach
  - Alice sends a file ($5.jpg) to Bob



Problems

- **Double Spending**
- **Multiple parties may own $5.jpg**

PayPal (Trusted 3rd Party)



Advantages

Double Spending prevented
Alice and Bob can be untrusted

Disadvantages

Third party can revert transactions
No privacy, since third party is present

Bitcoins

- Crypto currency (called bitcoins (BTC))
- Invented by unkown person or group (goes by the name Satoshi Nakamoto)

- Uses cryptography to achieve
  - Privacy
  - Untrusted transactions
  - Unreversible
  - No double spending

Just as in traditional currency

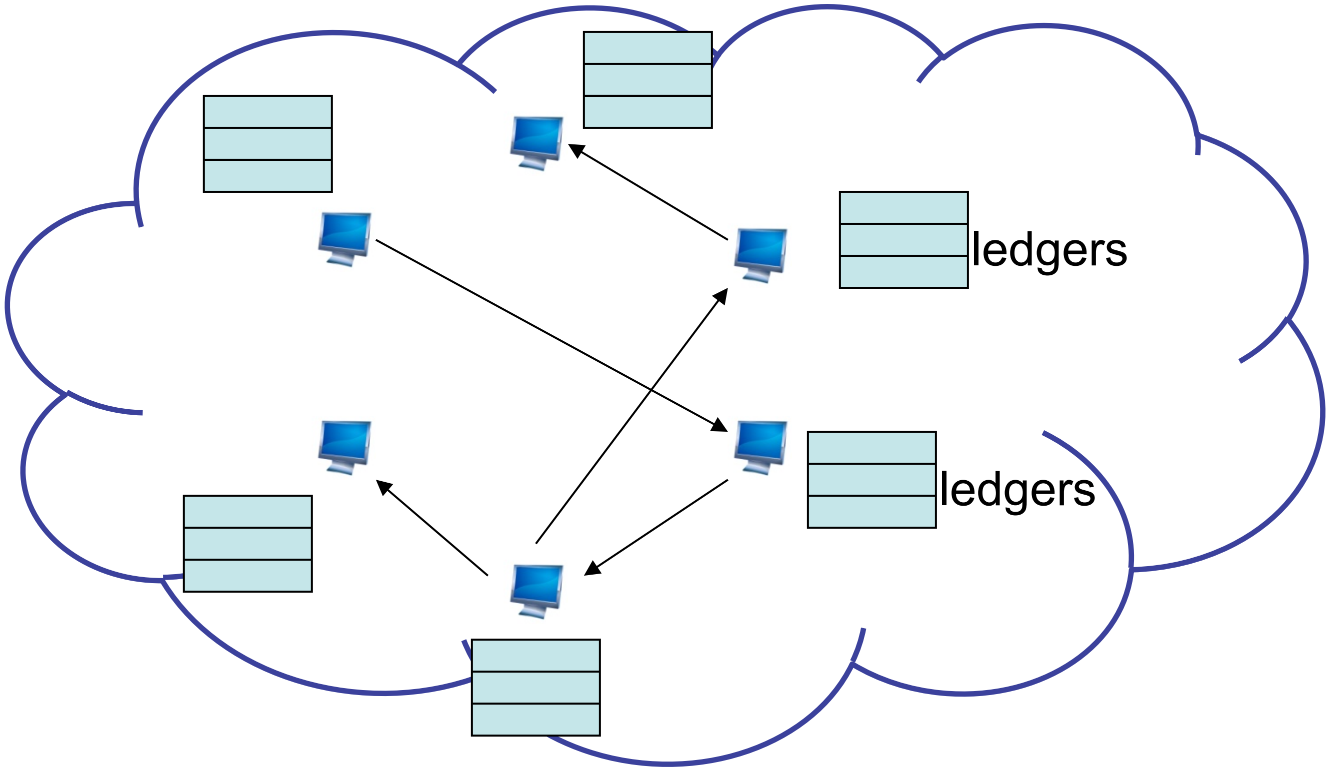
The Bitcoin Irony

- Bitcoins have
  - no bank
  - no trusted third party (like Paypal)
  - no paper money

  - But still works and can achieve **trust** !!!
  - Trust achieved by a large group of connected people who can be untrusted

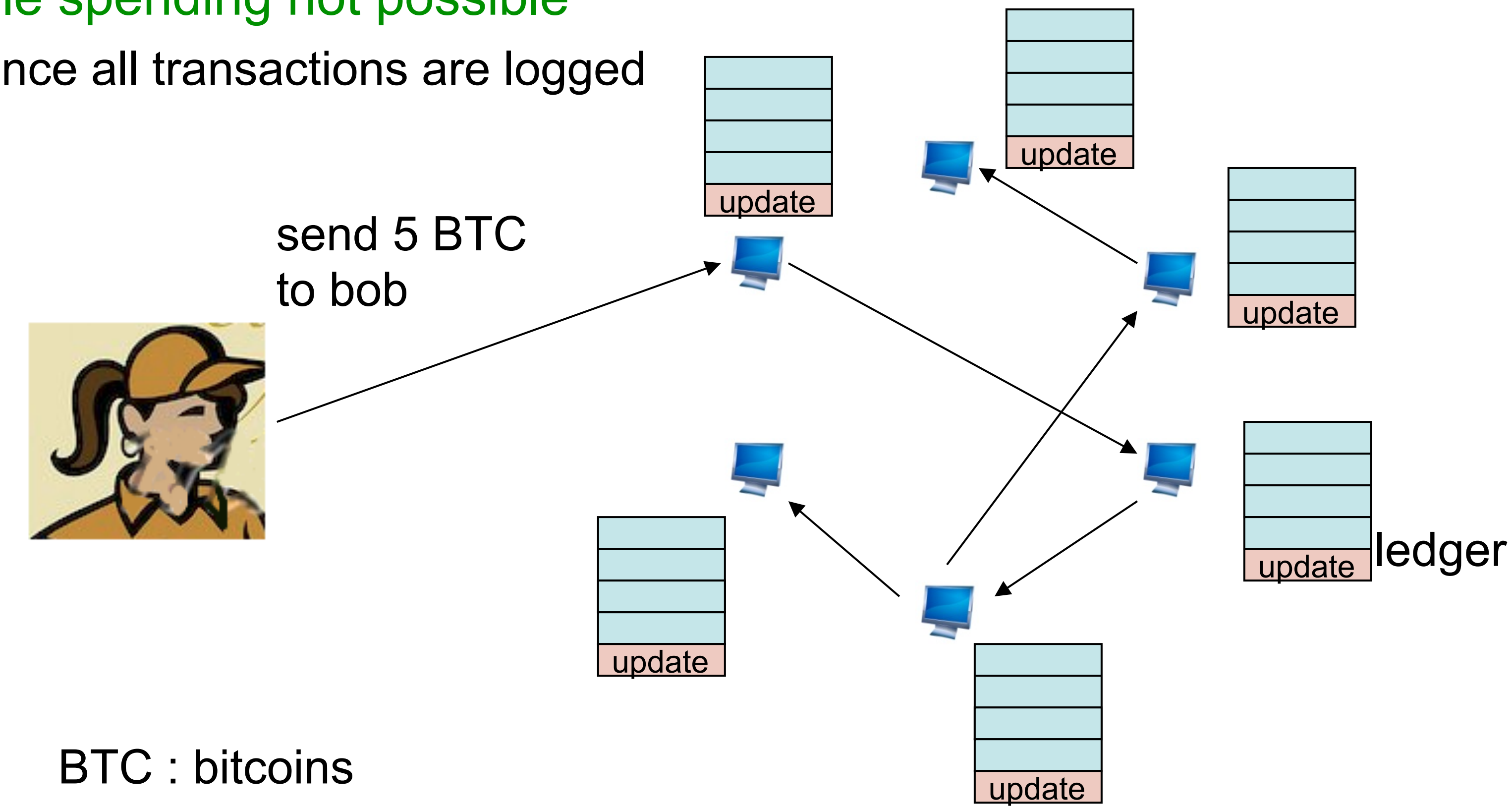
Big Idea

Ledgers maintained by several (1000s) of computers on the Internet



Transactions

- Every transactions logged in all ledgers
- Every transaction is checked if it has been previously done
  - Verification done by 1000s of computers
- Double spending not possible
  - Since all transactions are logged



BTC : bitcoins

Ledgers

Bank Ledger

Alice : $29
Walter : $12
Carr : $23
Bob : $121

minus $5

plus $5

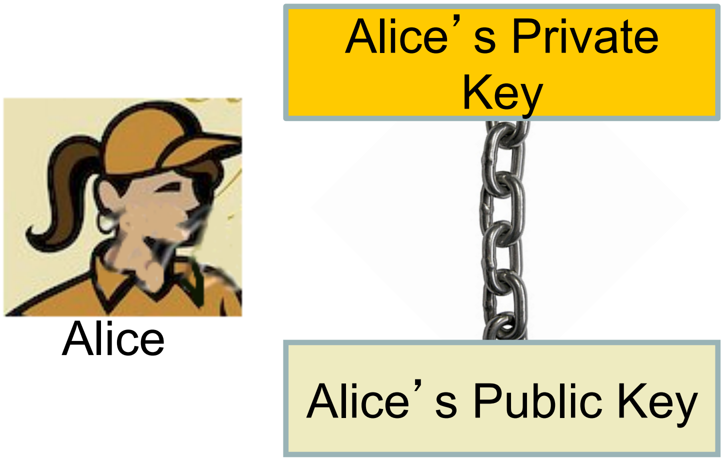
Bitcoin Ledger
(Transactions)

Alice → Bob 5BTC
Bob → Carr 3BTC
Carr → Alice 1BTC
John →Emily .3BTC
Jane -> Alice 4BTC
Joe → Alice 3BTC

called blockchain

Under the hood

Bitcoin Private Keys

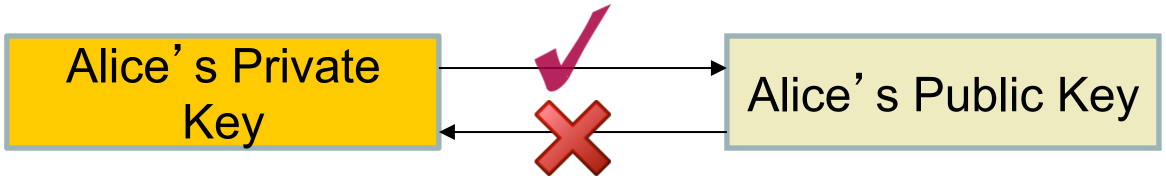


Private keys:

- Most important component
- Used to show ownership of funds
- If lost, money is lost (no way of reterving)
- If stolen, money can be stolen
- Every private key must be unique
- Generating private key, by simply picking a random number from 0 to 2^{256}

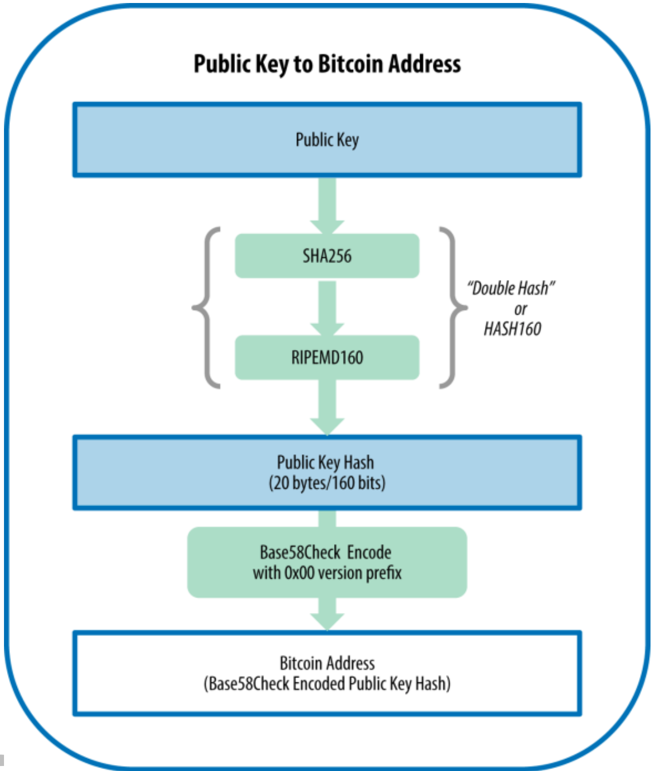
Bitcoin Public Keys

- Derived from the private key by a complex process called elliptic curve scalar multiplication
- Remember oneway ness,



Bitcoin Addresses

- Share with anyone who wants to send you money (appears in transactions as the recipient of funds)
- Derived from the public key

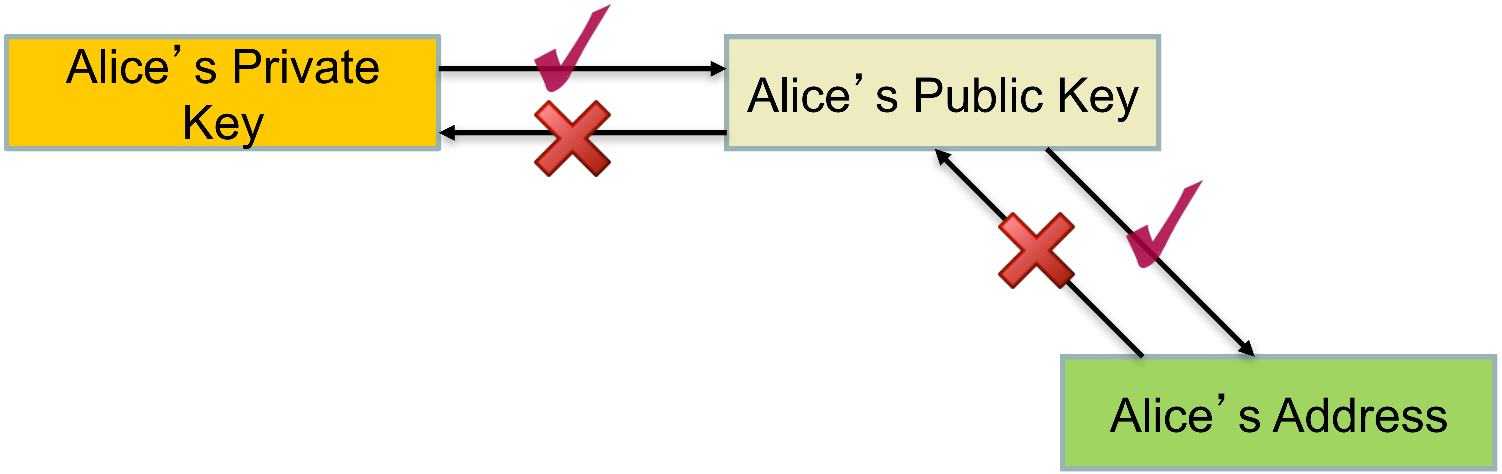


Bitcoin address

1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy

Bitcoin address (QR code)

More Oneways

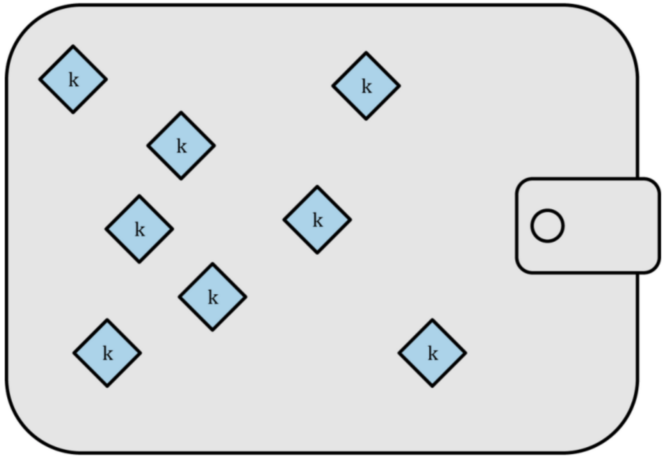


Alice generates the private key

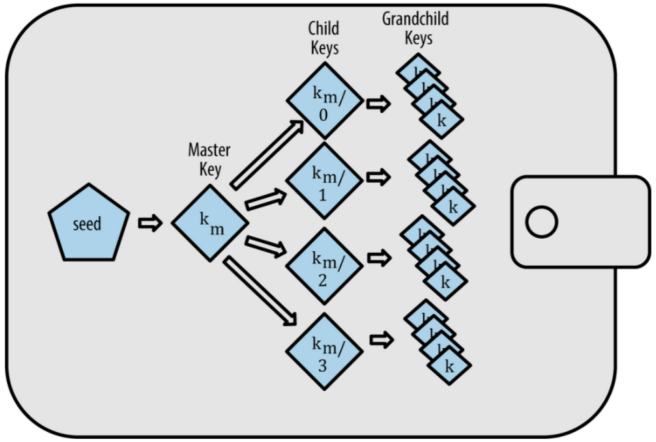
Only Alice can generate the public key and address

Wallets

- Collection of secret keys owned by a user
- Different types of wallets possible



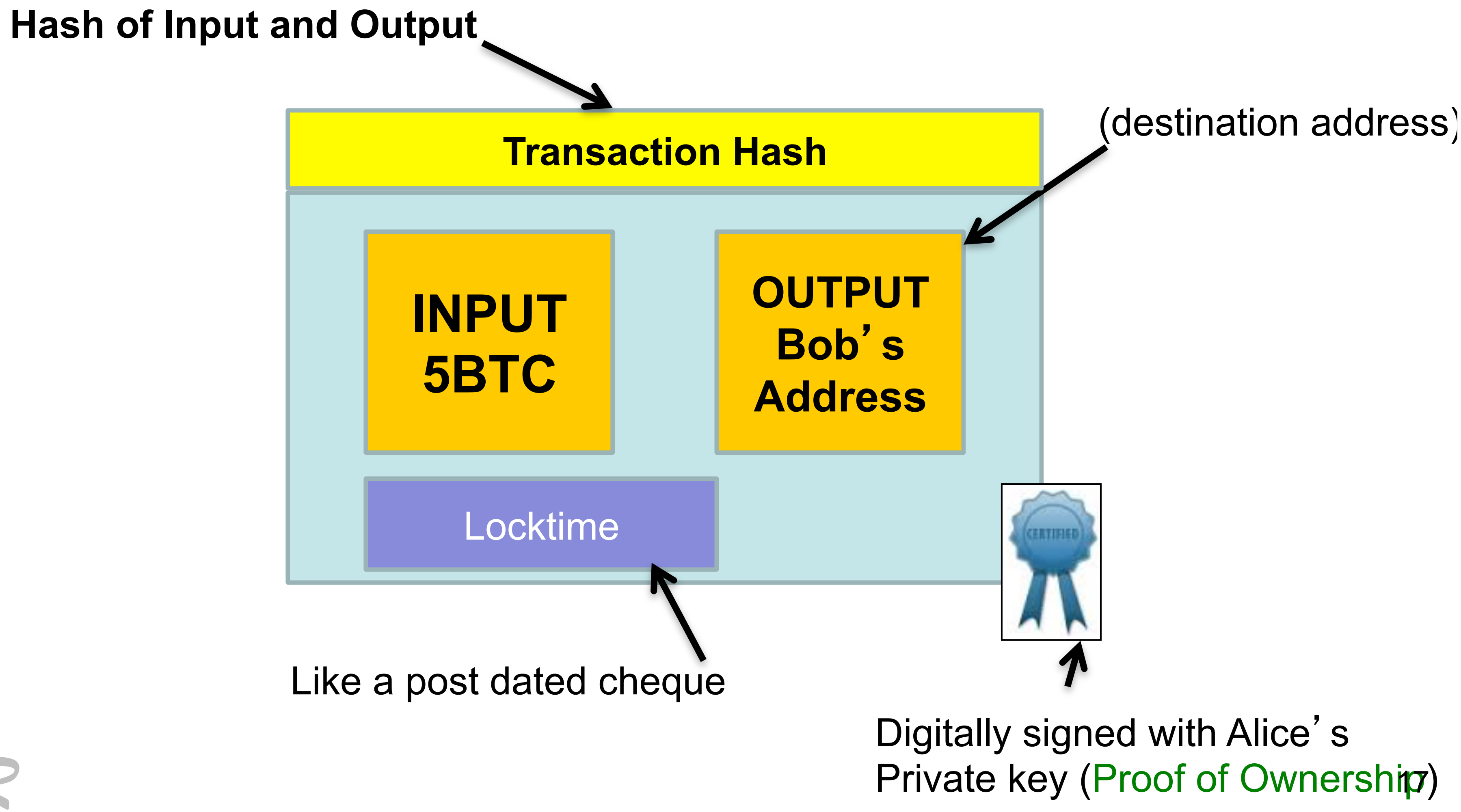
Randomly generated private keys



Keys generated in a hierarchy

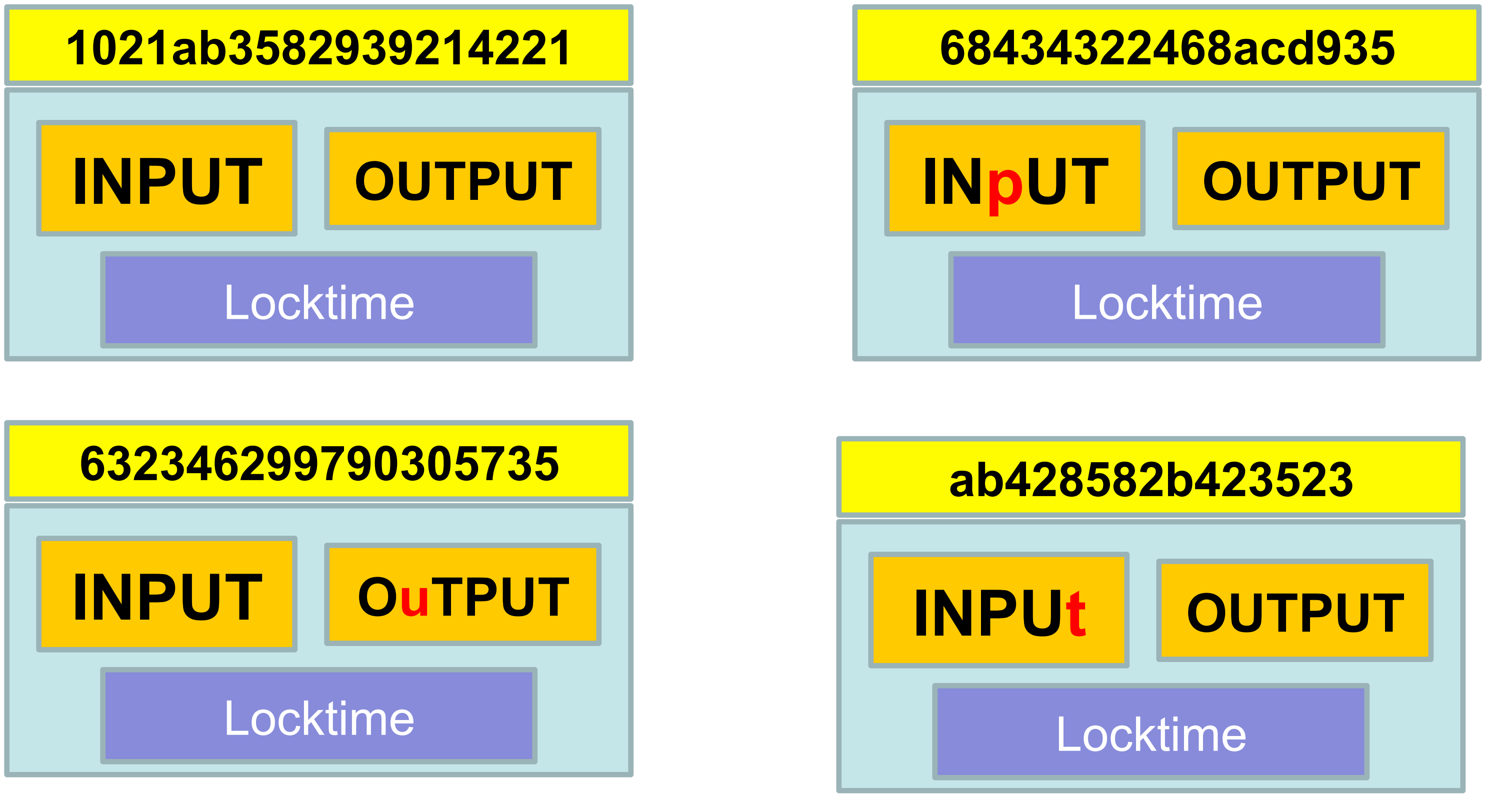
Bitcoin Transactions

How does Alice transfer 5 bitcoins to Bob?



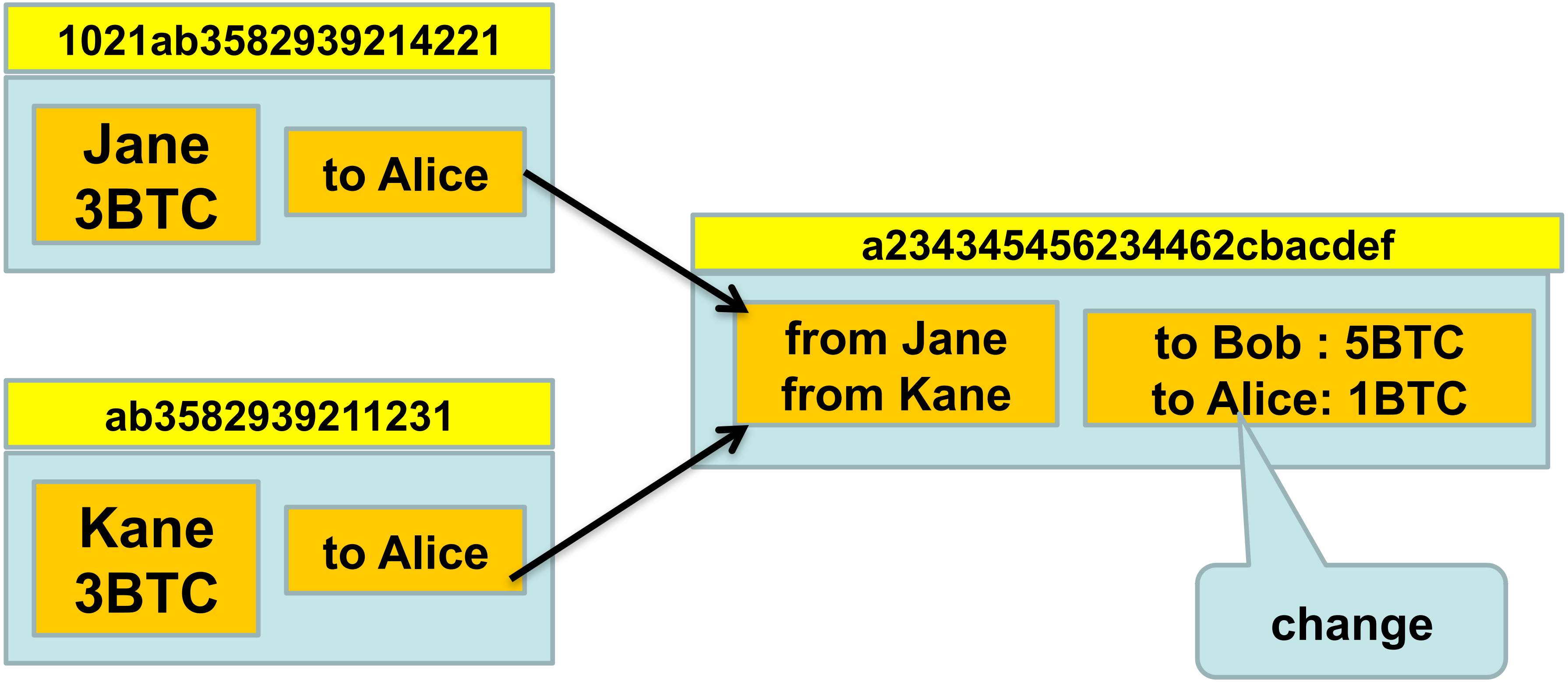
Transaction Hash

- A transaction hash uniquely identifies a transaction
- Even **a small change in the transaction will cause a complete change in the transaction hash**



Transaction Input

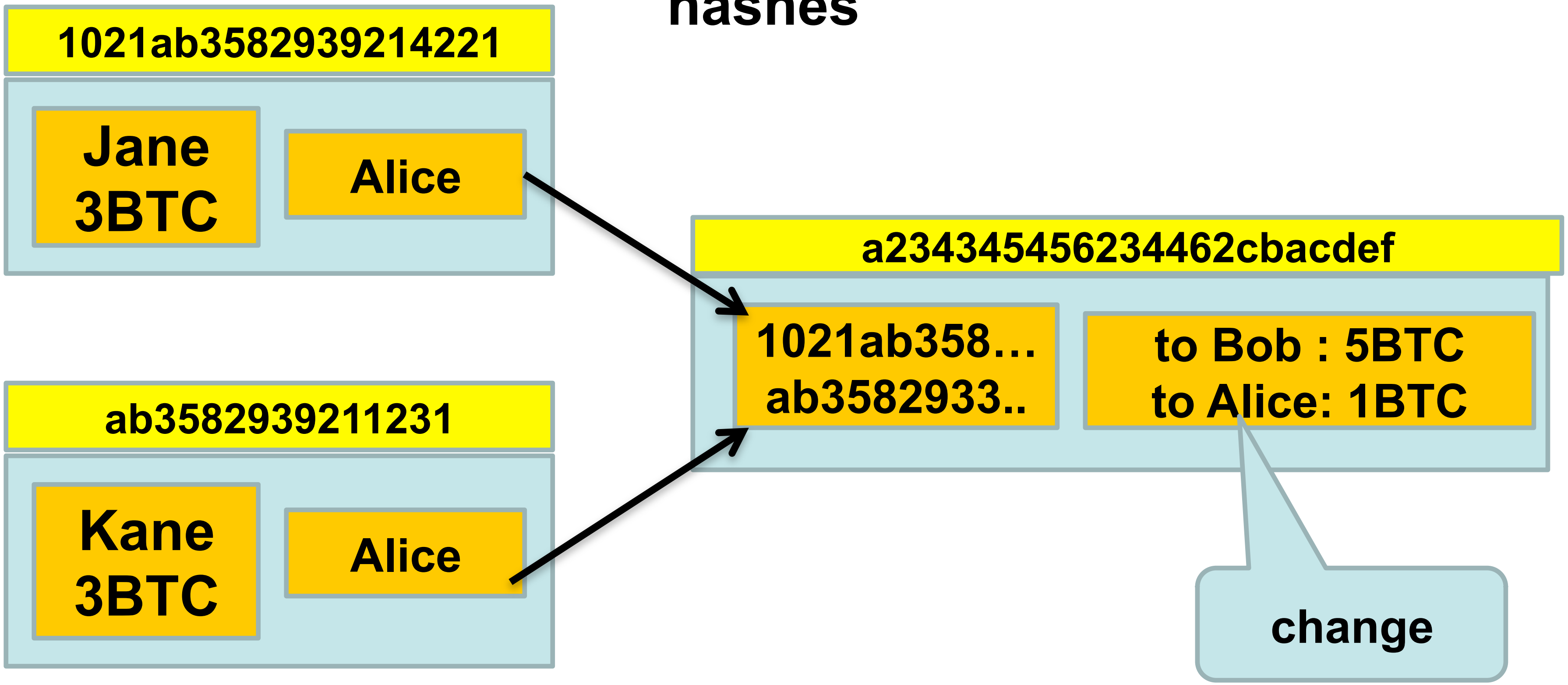
Where did Alice get the 5BTC from?



From unspent previous transactions
(which are recorded in current transaction)

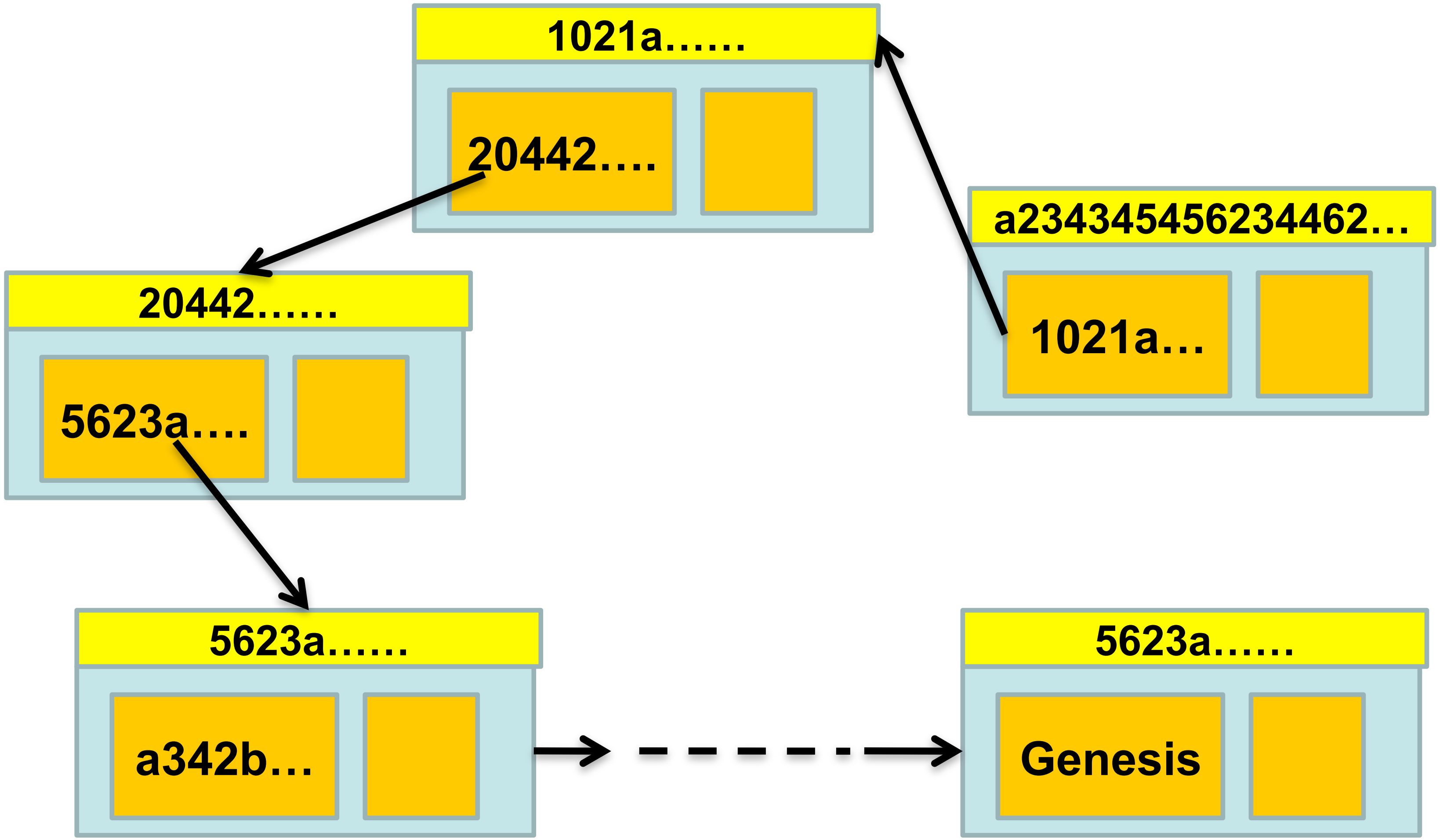
Transaction Input contd.

Just record the previous transaction hashes



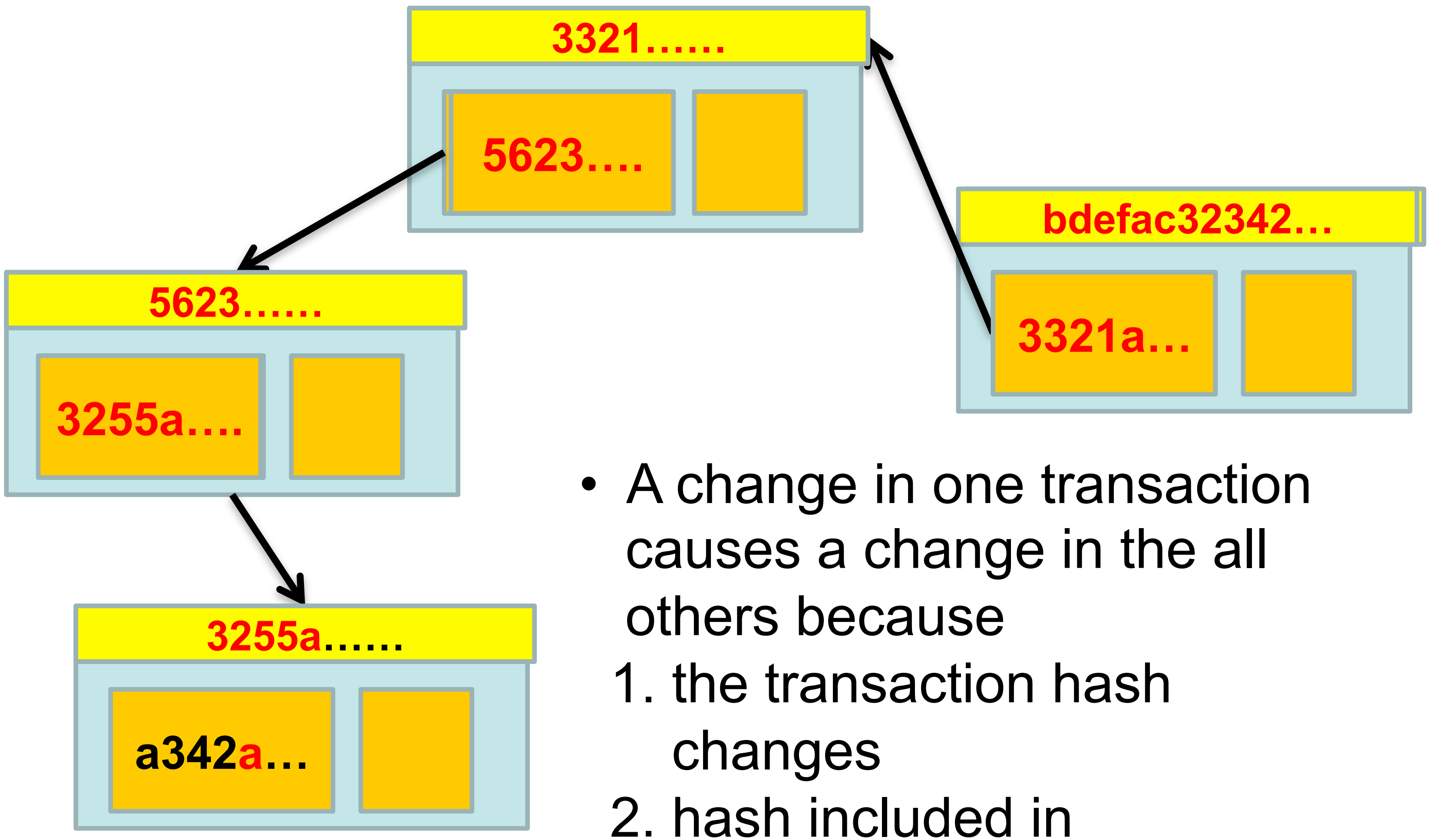
Transaction hash uniquely identify transactions

The Chain of Transactions



First transaction ever created

Cascaded



- A change in one transaction causes a change in the all others because
  1. the transaction hash changes
  2. hash included in subsequent transactions so subsequent hashes change

Bitcoin Ledger

is actually a list of transaction hashes so privacy is maintained

Alice → Bob 5BTC
Bob → Carr 3BTC
Carr → Alice 1BTC
John →Emily .3BTC
Jane -> Alice 4BTC
Joe → Alice 3BTC

Is actually →

23343…..
434134…..
43684…..
21232…..
67847…..
656464….

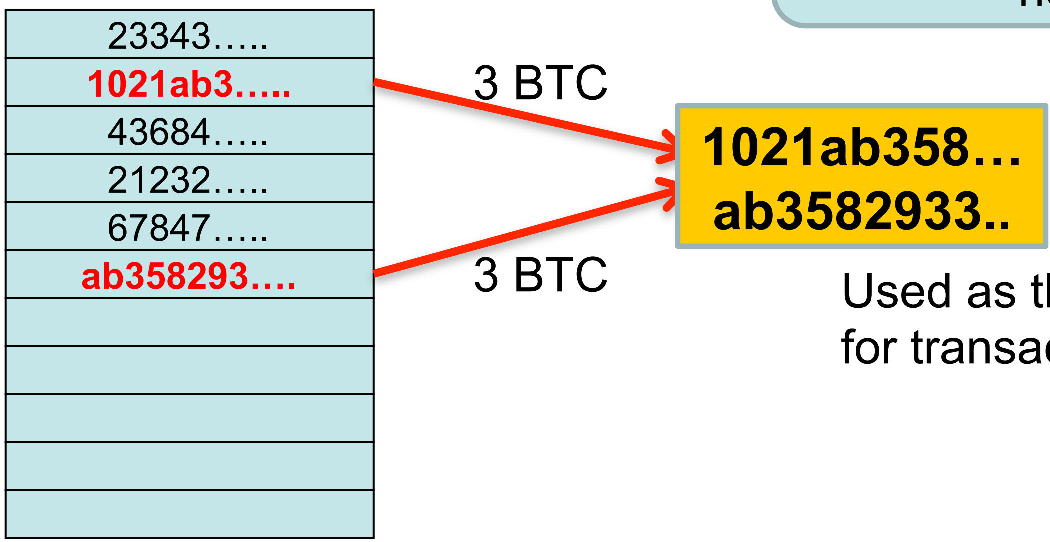
Bitcoin Ledger
(Transaction hashes)

The ledger contains all bitcoin transactions ever made since Bitcoins started

Transaction Input

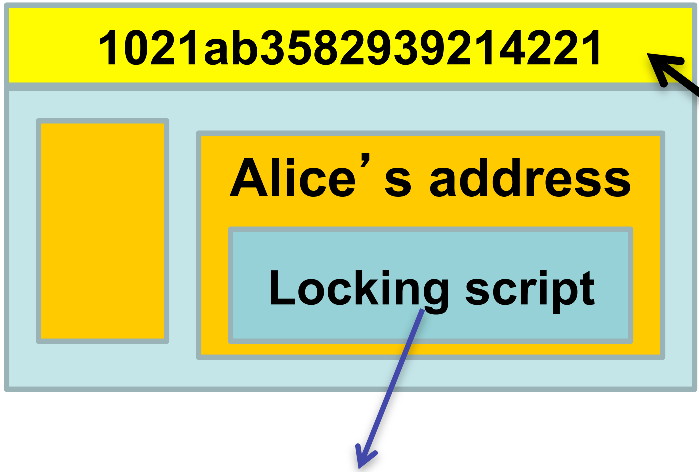
- To send 5 bit coins Alice needs to find transactions worth at least 5 unspent bitcoins in the ledger that were sent to her.

How does Alice claim these transactions as hers?

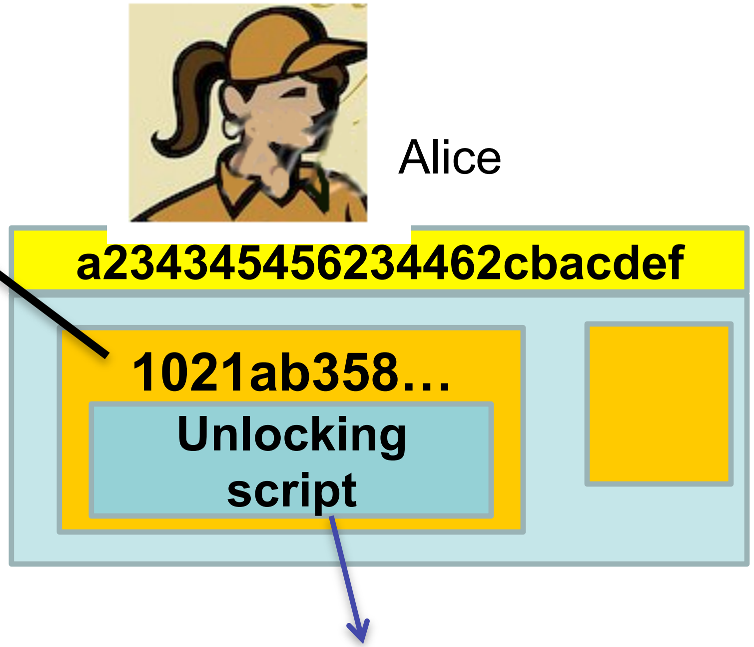


Used as the input
for transaction from Alice to Bob

How to Claim Transactions?



This is a mathematical puzzle.
Anyone who can solve this puzzle
Can claim the bitcoins



This is the answer the mathematical
Puzzle
Since Alice has the solution, she can claim
the previous transaction

Based on digital signatures

CR

Locking and Unlocking Scripts

- Uses a script (a simple programming language)
  - Locking has one half of the script
  - Unlocking has the other half of the script
- Anyone can join the scripts to validate it (thus validating the transactions)
- Since a script is used, the puzzles are flexible.

Locking and Unlocking Scripts

- Example : **Pay-to-Public Key**

Locking Script: <Public key of Alice>

Unlocking Script : <Dig. signature from Alice's private key>

Script:

<Dig. Signature from Alice's private key>
<Public key of Alice>
OP_CHECKSIG

Validation of Scripts

<Dig. Signature from Alice's private key>
<Public key of Alice>
OP_CHECKSIG

Alice

Transaction

Alice's Private Key

Sign function

Signature for M

Everyone else

Transaction

Alice's Public Key

Signature for M

Verify function

Message M was indeed signed by Alice
So Alice can claim the transaction

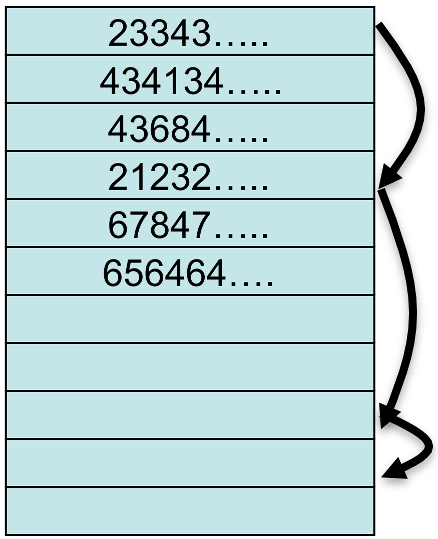
Validation with Signatures

- Signature is dependent on the transaction
  - Therefore changes made to the transaction can be detected

- Since every transaction is different, every signature is different.
  - Therefore signature cannot be reused

Double Spending

How to ensure that Alice is not trying to spend bitcoins twice?



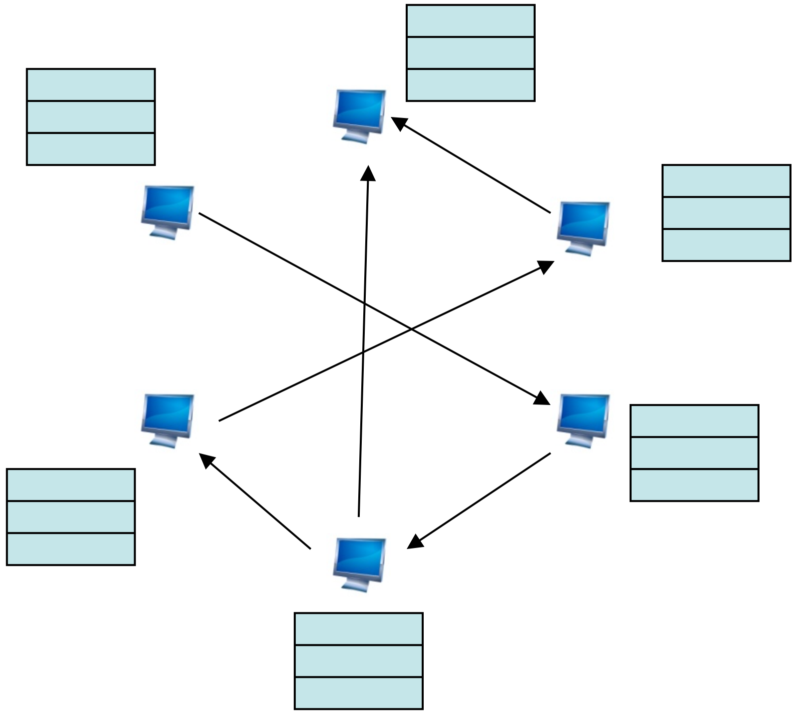
- Check every previous transaction in the blockchain
- Ensure that the inputs used by Alice have not been used again
- Made fast by an index of unused transactions

So far…

1. We have seen how Alice creates a transaction
2. We have seen how the transaction can be validated.
   – For authenticity
   – And for double spending

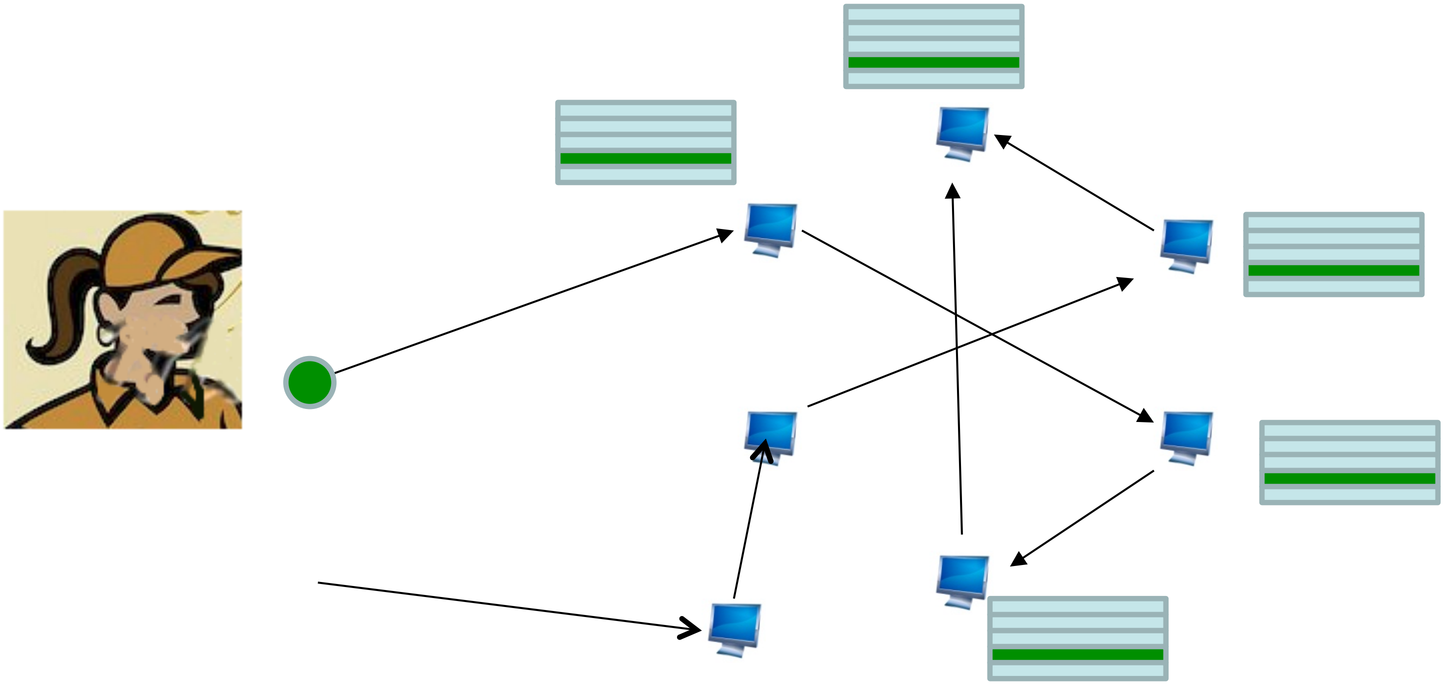
But, who does the validation,

Remember, Bitcoin relies on 1000s of computers and each computer maintains a ledger



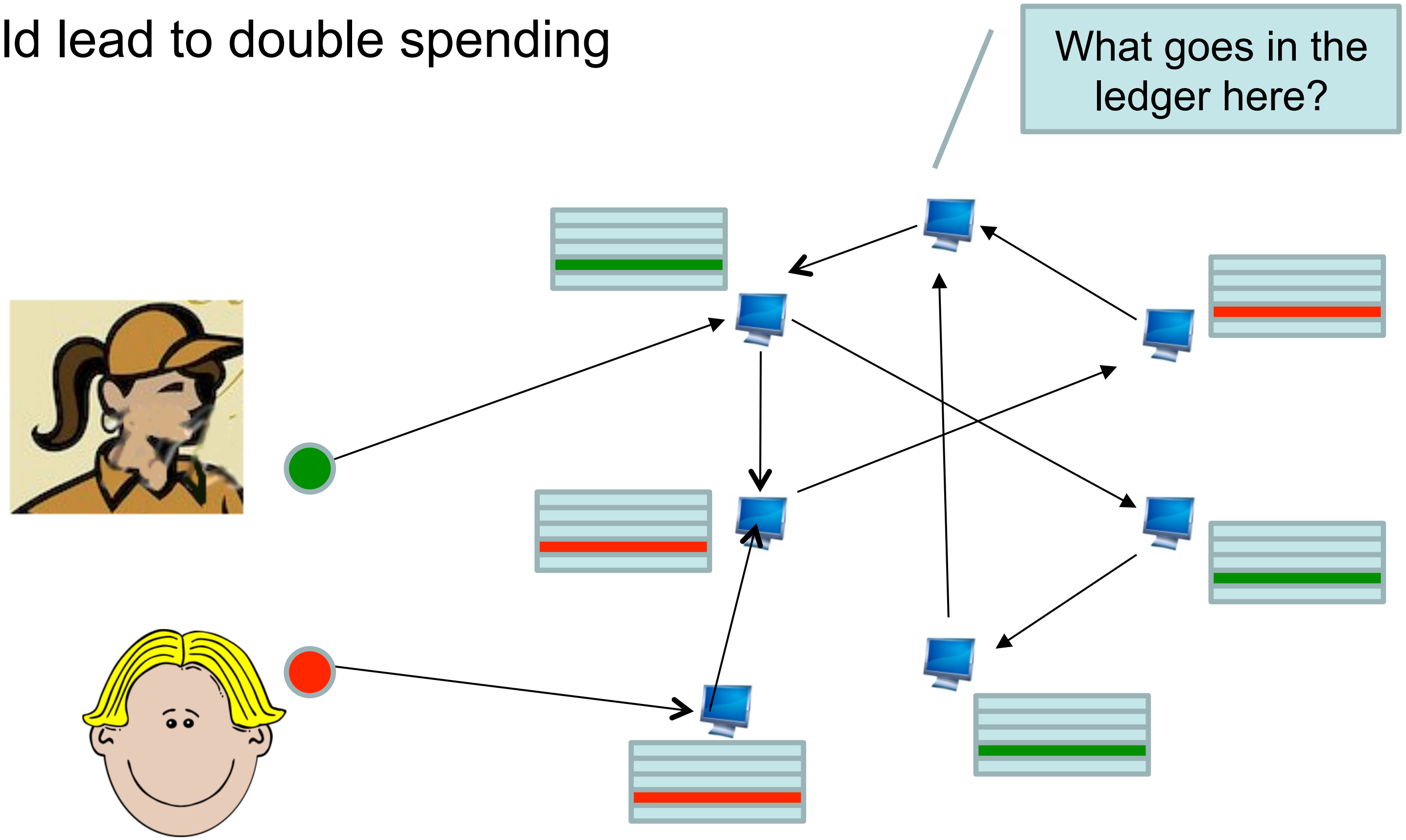
Who validates transactions?

- Alice sends transaction to any node in the bitcoin network
- Node validates, adds it to the ledger, and then sends it to other nodes
- In a few seconds several 1000 nodes have validated and broadcasted the transaction



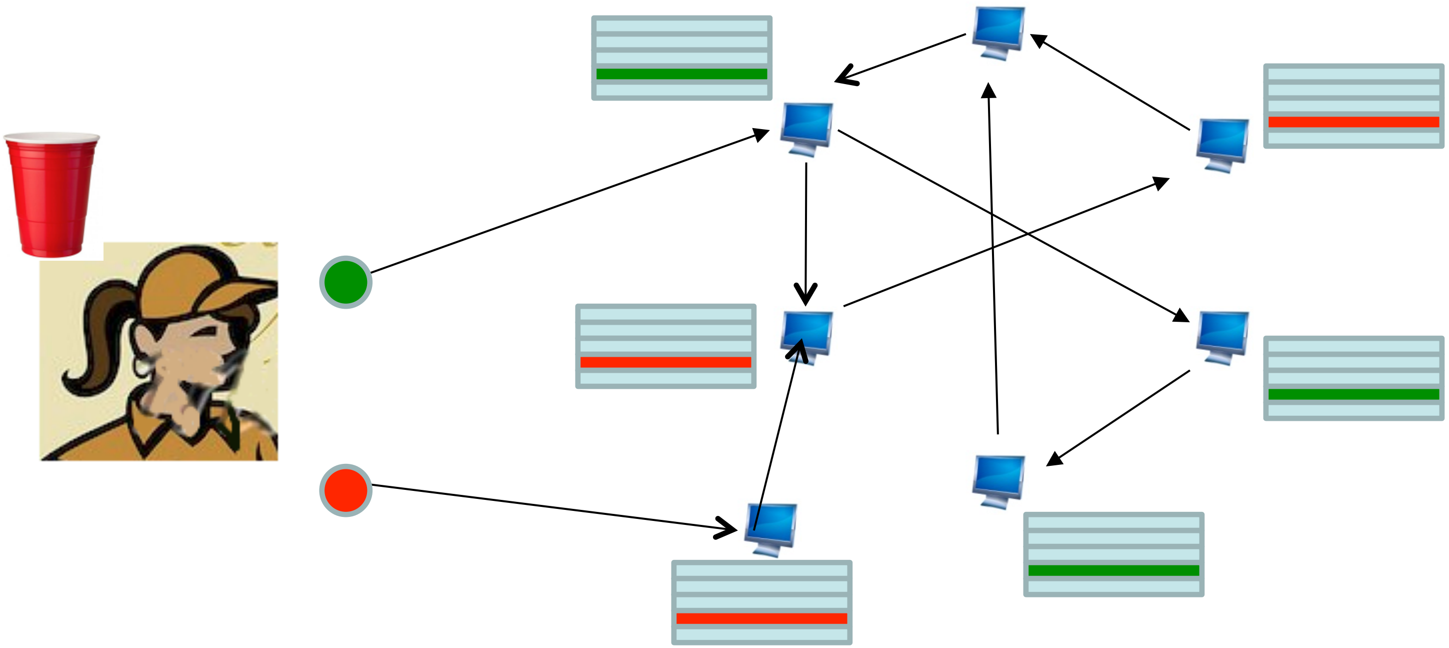
Ordering Transactions

- Transactions hop from one node to another in a random manner
- It is therefore possible for nodes to have different ledgers
- A dishonest node could prioritize one transaction over another
- Could lead to double spending



Double spending (due to transaction order)

- Alice initiates a transaction , waits for Bob to deliver her coffee
- Then immediately initiates another transaction with the same inputs



Bitcoins solution for ordering transactions

Block Chains

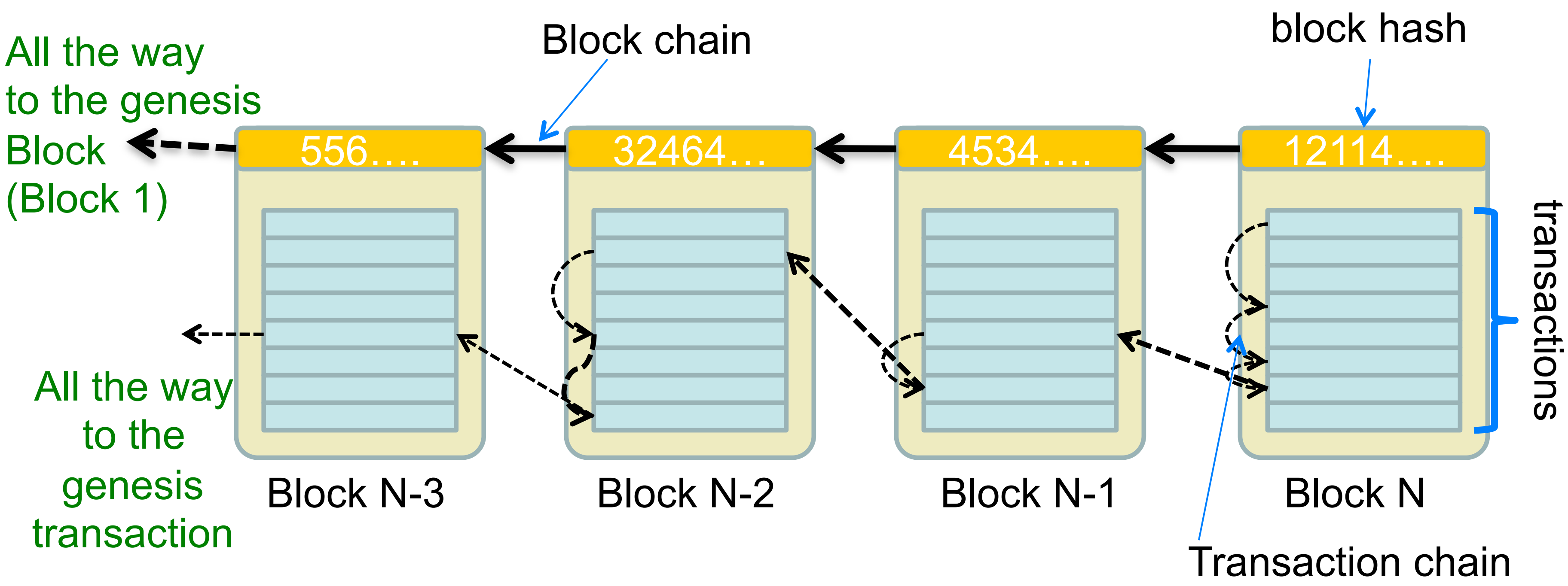
Blocks

Miners

More Puzzles

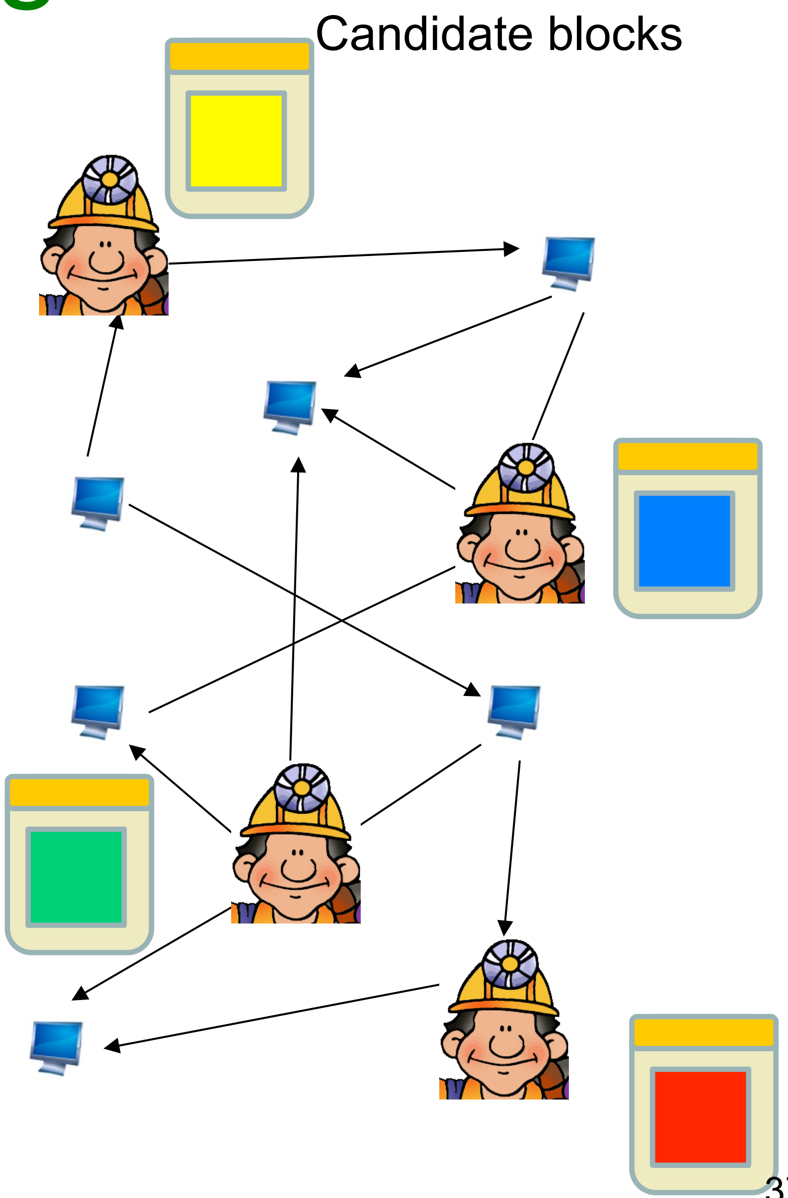
Blocks & Blockchains

- Ledgers are now stored as blockchains
- Each blockchain now has blocks instead of transactions
- Blocks contain multiple transactions



Miners

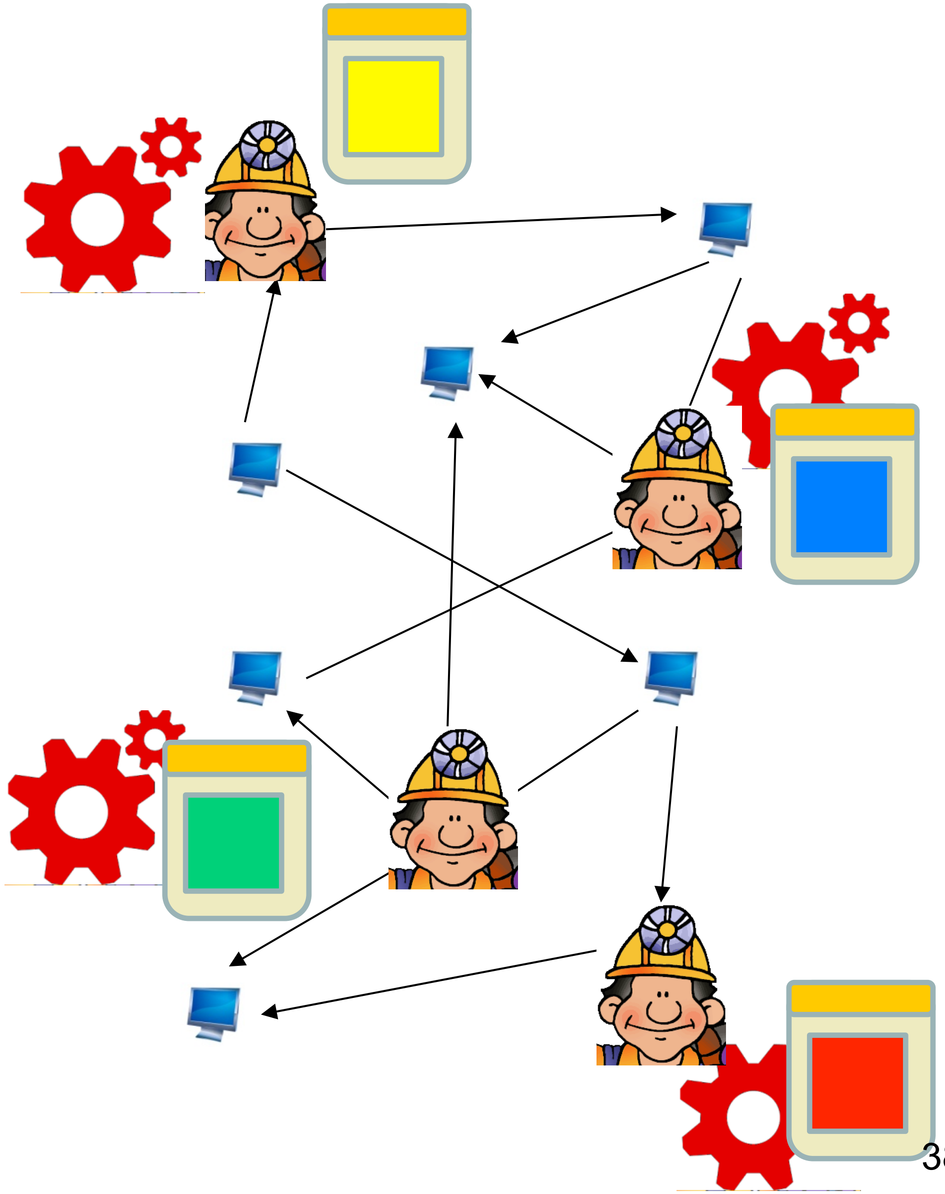
- Special nodes in the network called miners
- Miners track bitcoin transactions and add them to 'candidate blocks'
- Due to transaction ordering issues, candidate blocks in each miner may be different



How do the miners reach a consensus?

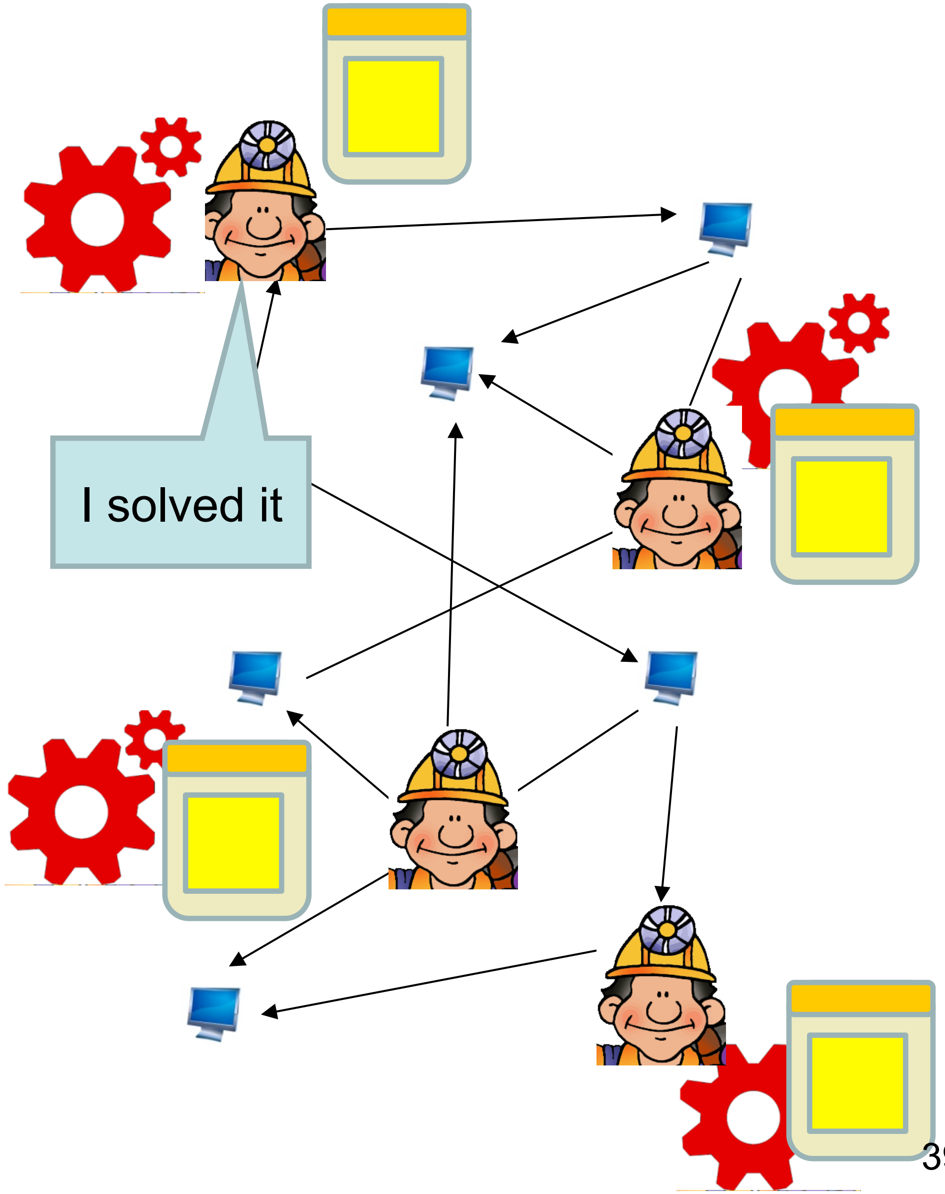
Mathematical Puzzle

- All miners simultaneously try to solve a mathematical puzzle
- The puzzle takes around 10 minutes to solve



Solving the Puzzle

- When a miner solves the puzzle, he announces the result to all others
- His candidate block is adopted by all others and added to the block chain
- Incentives for the winning miners

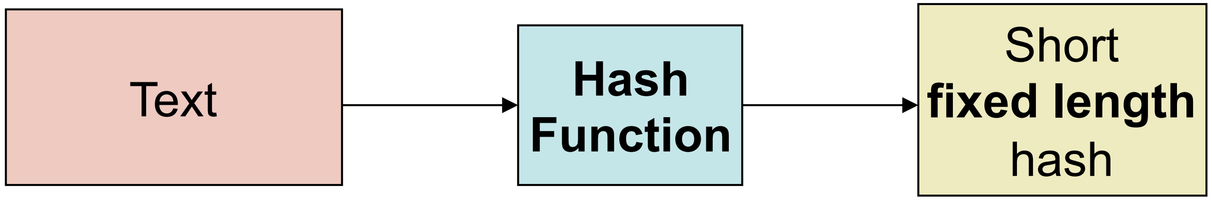


CR

Mathematical Puzzle

- **Three Requirements**
  - Should be difficult to solve
  - But still solvable in 10 minutes
    - Independent of the computing power of the miners
  - Once solved, the solution should be easily verified
- The only way to solve the puzzle must be by randomly trying different inputs

Hash function randomness



The hash is completely random.
The only way to find an output is to make random guesses of the input.

SHA256(“short sentence”)
0x 0acdf28f4e8b00b399d89ca51f07fef34708e729ae15e85429c5b0f403295cc9
SHA256("The quick brown fox jumps over the lazy **dog**")
0x d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592
SHA256("The quick brown fox jumps over the lazy **dog."**)
(extra period added)
0x ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c

A Puzzle

Concatenate a number to the message ‘M’ so that the hash begins with a 0.

M = “I am Satoshi Nakamoto”

```
I am Satoshi Nakamoto0 => a80a81401765c8eddee25df36728d732...
I am Satoshi Nakamoto1 => f7bc9a6304a4647bb41241a677b5345f...
I am Satoshi Nakamoto2 => ea758a8134b115298a1583ffb80ae629...
I am Satoshi Nakamoto3 => bfa9779618ff072c903d773de30c99bd...
I am Satoshi Nakamoto4 => bce8564de9a83c18c31944a66bde992f...
I am Satoshi Nakamoto5 => eb362c3cf3479be0a97a20163589038e...
I am Satoshi Nakamoto6 => 4a2fd48e3be420d0d28e202360cfbaba...
I am Satoshi Nakamoto7 => 790b5a1349a5f2b909bf74d0d166b17a...
I am Satoshi Nakamoto8 => 702c45e5b15aa54b625d68dd947f1597...
I am Satoshi Nakamoto9 => 7007cf7dd40f5e933cd89fff5b791ff0...
I am Satoshi Nakamoto10 => c2f38c81992f4614206a21537bd634a...
I am Satoshi Nakamoto11 => 7045da6ed8a914690f087690e1e8d66...
I am Satoshi Nakamoto12 => 60f01db30c1a0d4cbce2b4b22e88b9b...
I am Satoshi Nakamoto13 => 0ebc56d59a34f5082aaef3d66b37a66...
I am Satoshi Nakamoto14 => 27ead1ca85da66981fd9da01a8c6816...
I am Satoshi Nakamoto15 => 394809fb809c5f83ce97ab554a2812c...
I am Satoshi Nakamoto16 => 8fa4992219df33f50834465d3047429...
I am Satoshi Nakamoto17 => dca9b8b4f8d8e1521fa4eaa46f4f0cd...
I am Satoshi Nakamoto18 => 9989a401b2a3a318b01e9ca9a22b0f3...
I am Satoshi Nakamoto19 => cda56022ecb5b67b2bc93a2d764e75f...
```

Satisfying the requirements

- Should be difficult to solve
  - The only way to solve the puzzle is by randomly varying the inputs
- Once solved, the solution should be easily verified
  - Easily checked!!!
- Solvable in 10 minutes. Independent of the computing power of the miners.
  - Scalable difficulty (next!!!)

Scalable Difficulty

- **Why?**
  - Computing power of miners increases with technology
  - More miners in the network over time
  - Problem difficulty should be adjusted so that solution (on average) obtained in 10 minutes
- **How?**

Concatenate a number to the message 'M' so that the hash begins with N zeros.

  - If N is less (easily solved)
  - If N is large (more difficult to solve)
  - Every 2016 blocks, difficulty adjsted depending on average time taken for the last 2016 blocks

CR

Summarizing Miners

- Miners do three tasks simultaneously

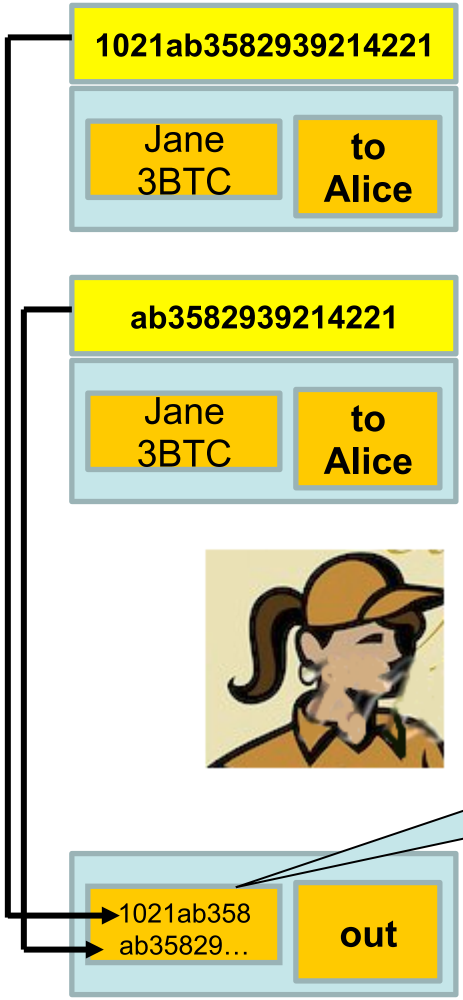
Add incoming transactions to candidate block

Try to solve the puzzle → If solved → B roadcast solution → Add candidate block to blockchain

Lookout if any one has solved the puzzle → If solved → B roadcast solution → Add winner's candidate block to blockchain

Summary of Bitcoins

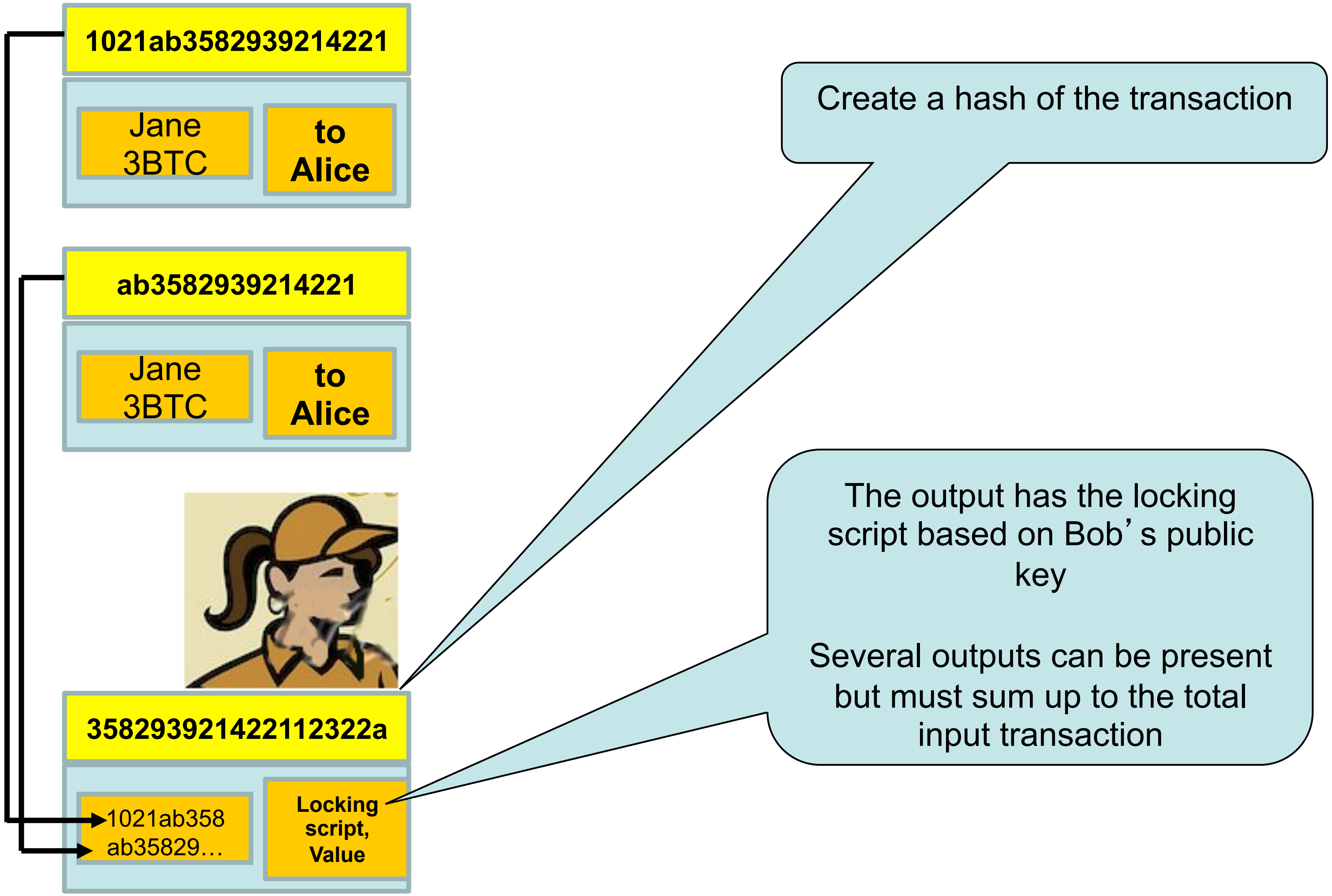
1. Build a transaction from previous unused bitcoins



Each input in the transaction also has the unlocking script, which will allow Alice to claim the transactions

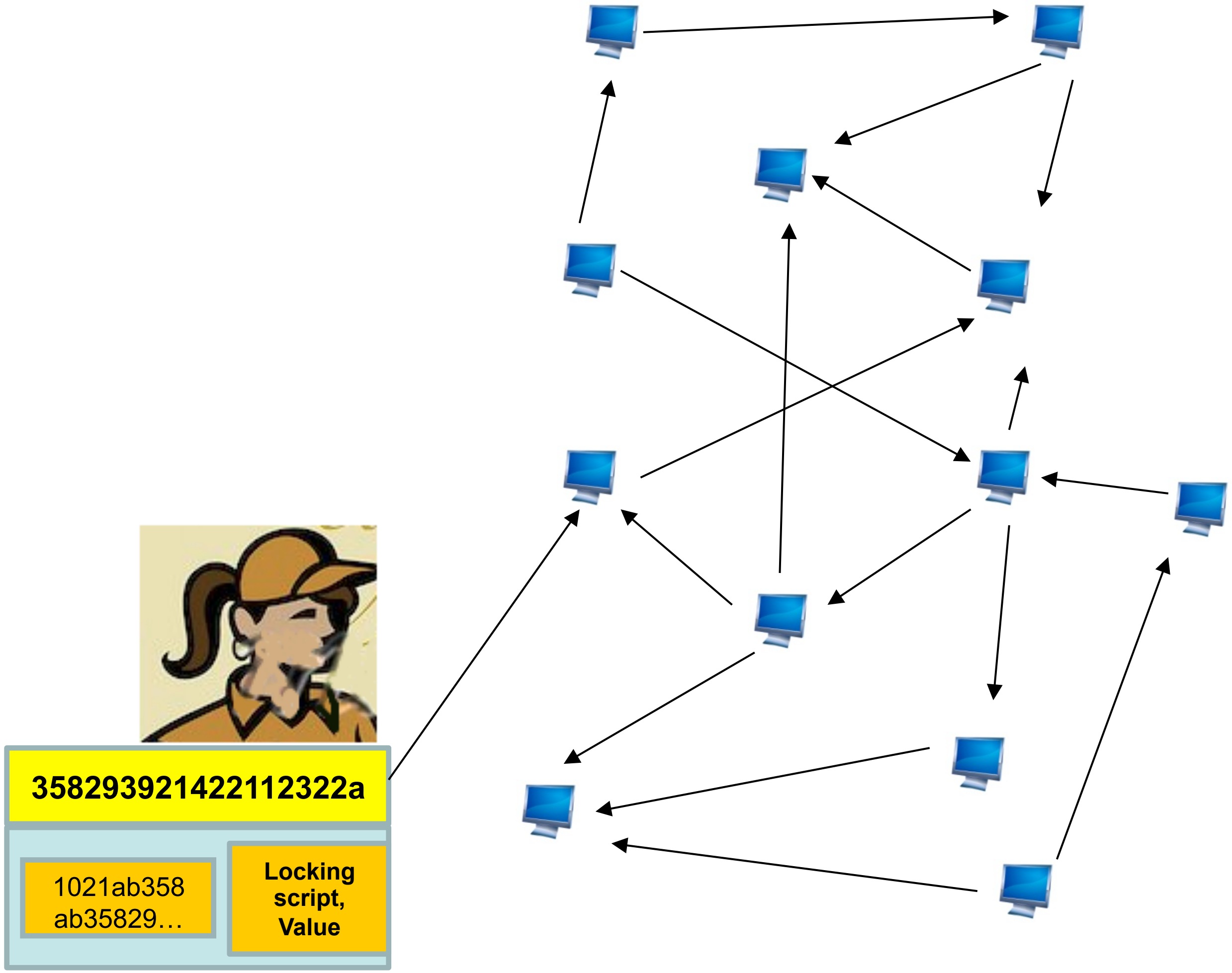
Summary of Bitcoins

1. Build a transaction from previous unused bitcoins



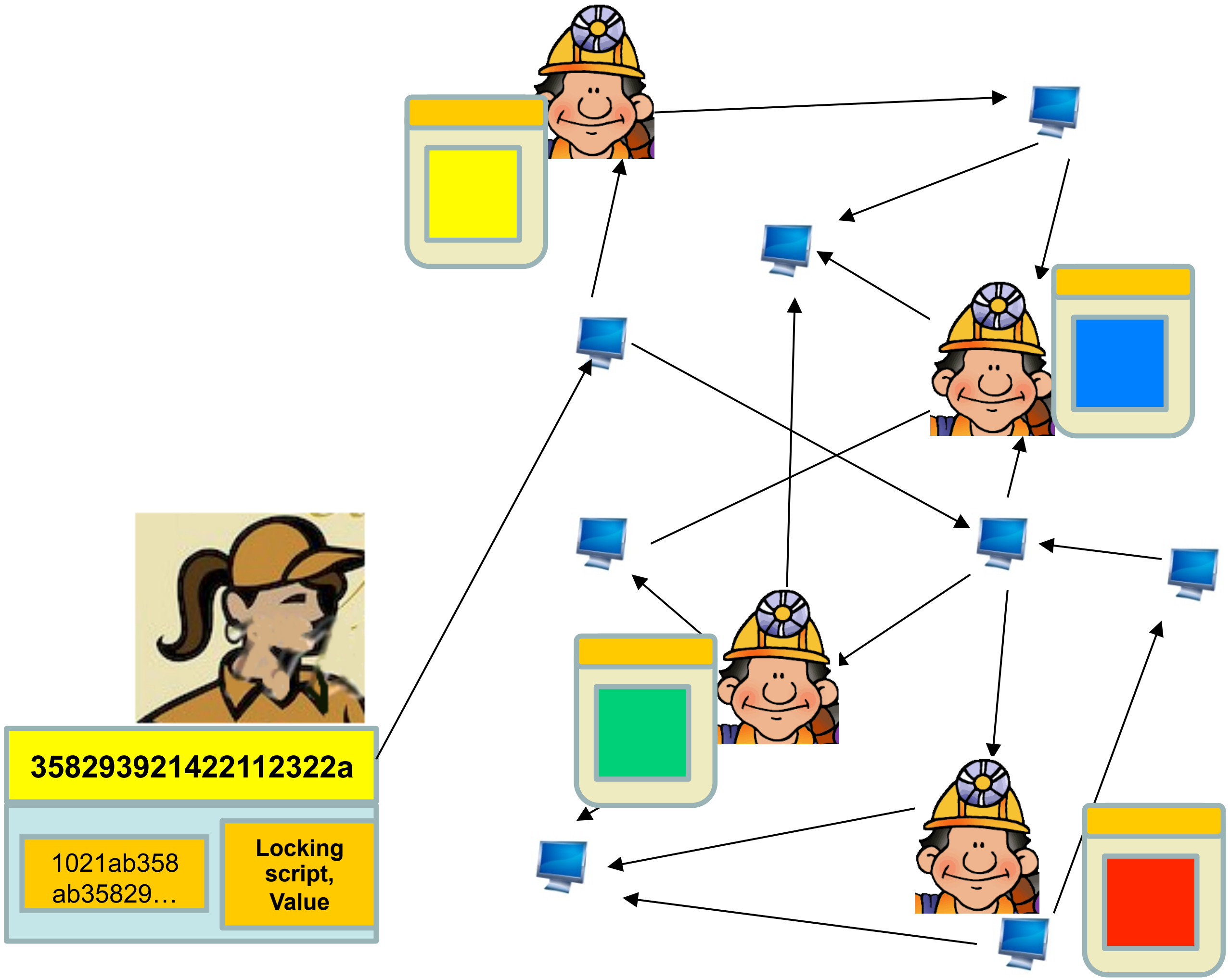
Summary of Bitcoins

2. Push transaction to network, where it is broadcasted



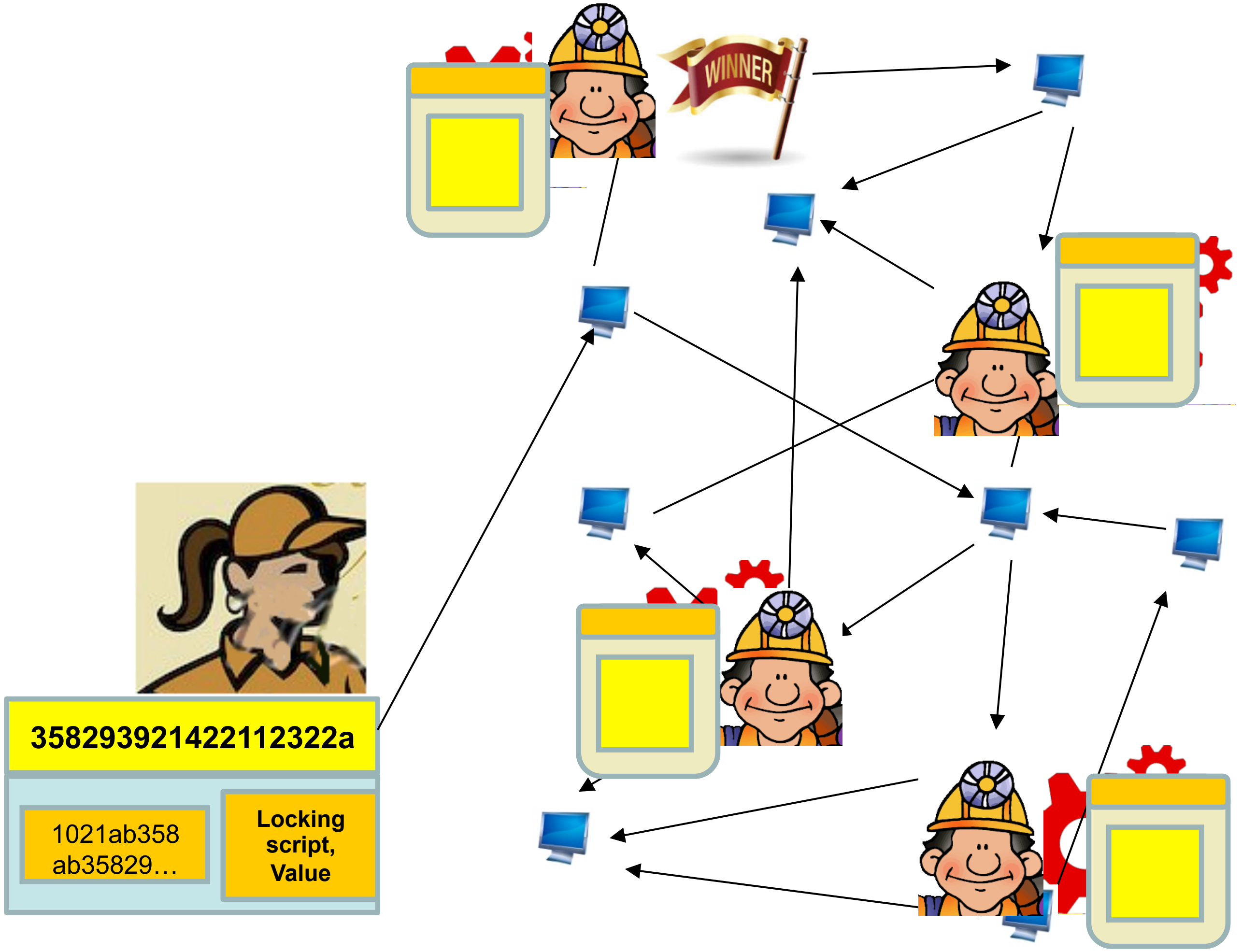
Summary of Bitcoins

2. Miners on network validate Alice's transaction. If found valid, add to a candidate block



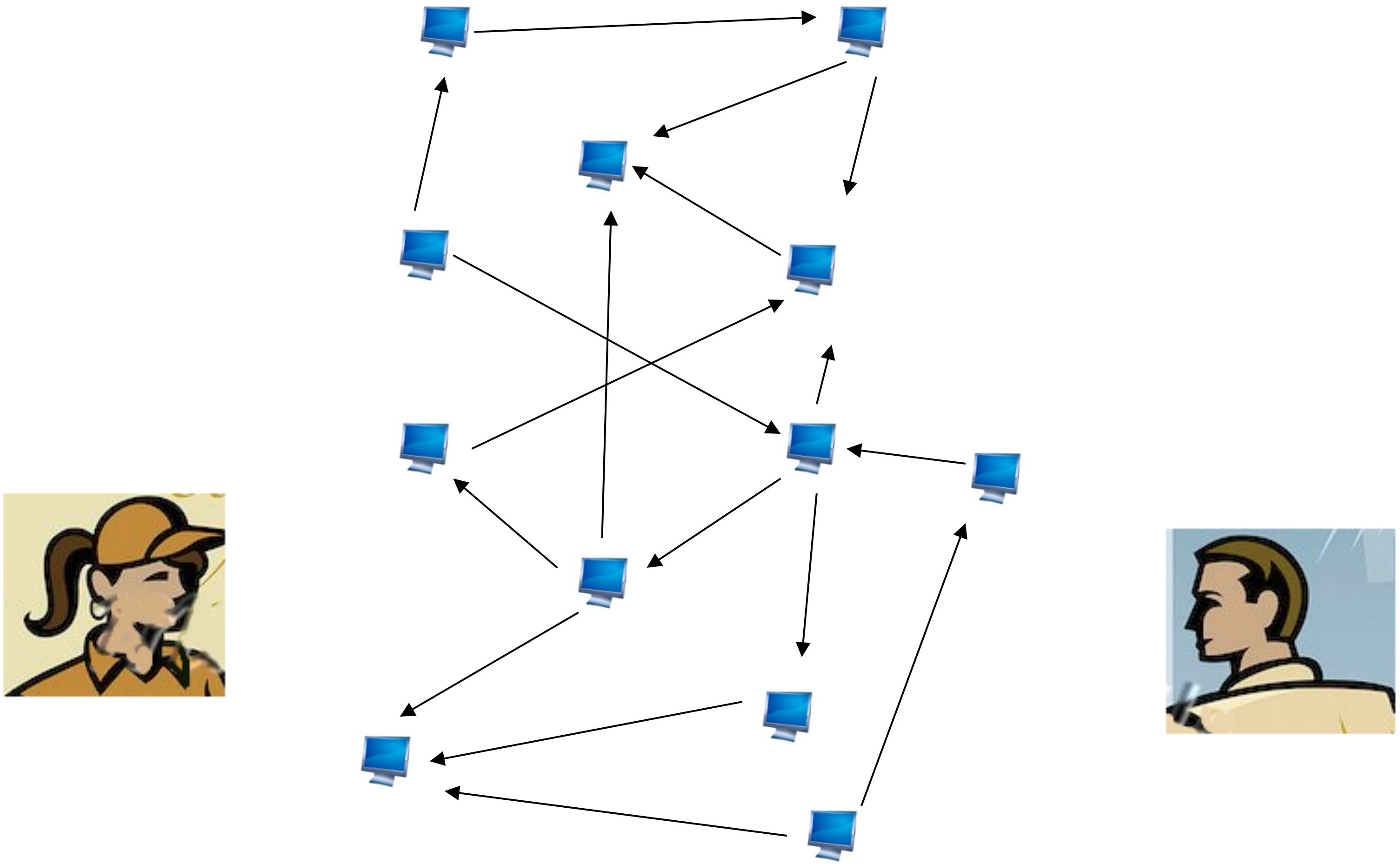
Summary of Bitcoins

3. Miners simultaneously try to solve a mathematical puzzle. If a miner succeeds, the result is broadcasted. The winning miner's candidate block is adopted by all others



Summary of Bitcoins

4. The transaction shows up in Bob's wallet and can be claimed in any transaction Bob makes



Conclusions

- Bitcoins are an alternative to physical currency
- Trust is achieved by using cryptography and by large number of users
- Still not fool proof (attacks stell exist)
  - Tokyo based bitcoin exchange Mt. Gox hacked

Potential Problems

- Theft of private keys
- Tracing coin’s history
- Sybil attack : Attacker controllers large number of nodes in the network
- Side channel analysis
- Denial of Service Attakcs
- Malware in systems
- Energy requirements for mining