Blockchain & Bitcoin Overview

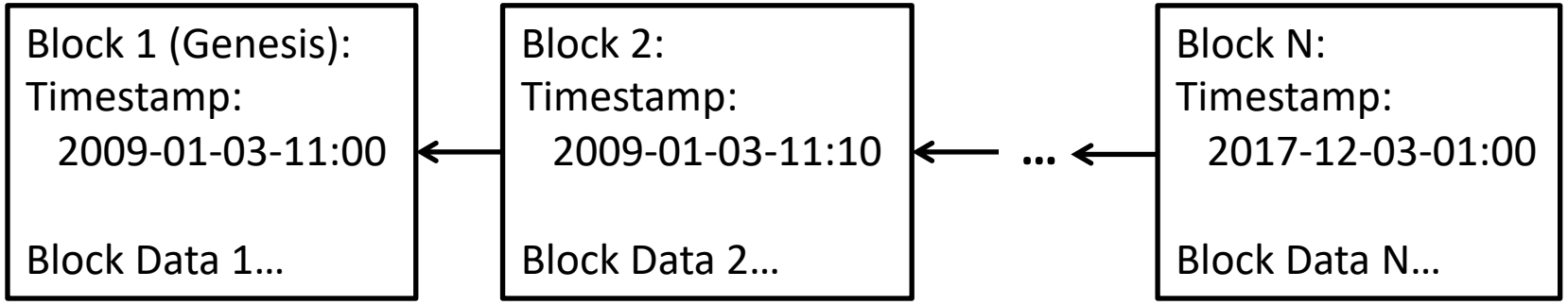
Fan Long

University of Toronto

Acknowledgement: part of the slides are brought from blockchain.berkeley.edu

What is Blockchain?

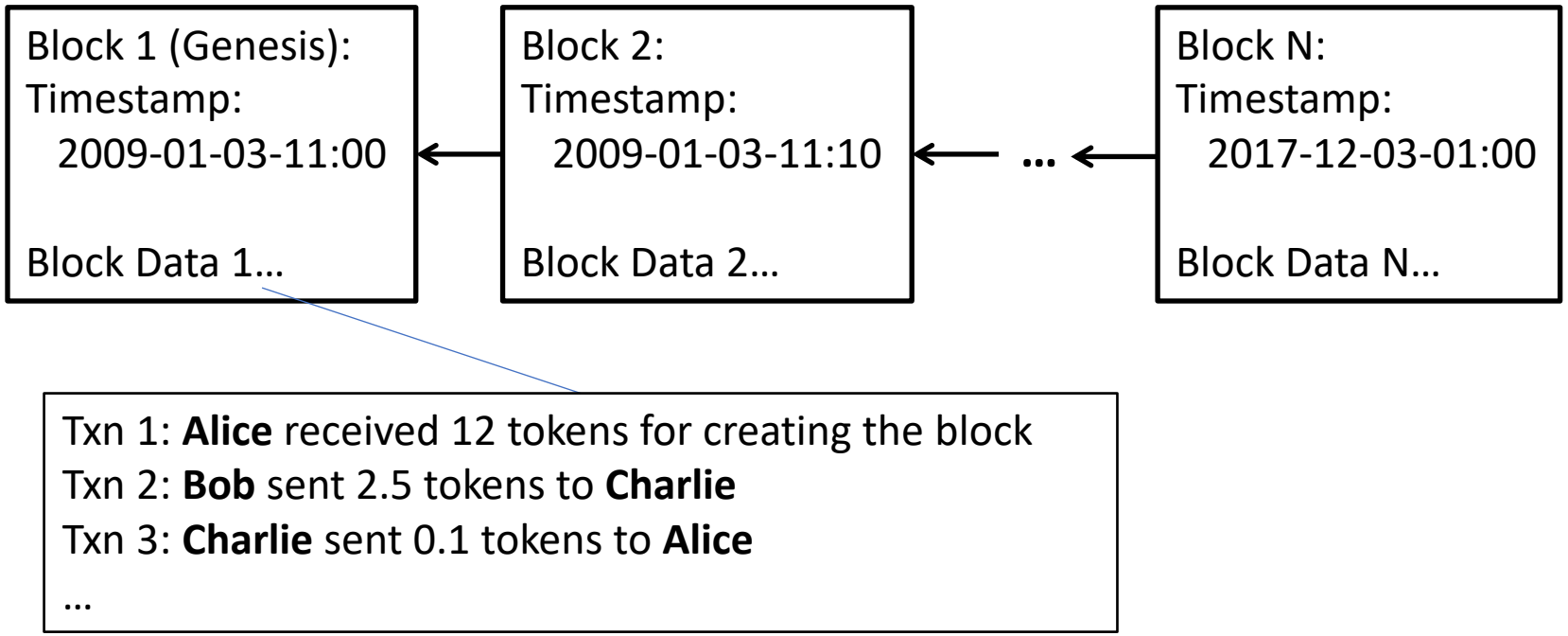
- A list of ordered data blocks maintained by a network:



- Everyone can read
- Everyone can append a *valid* block at the end
- **No one can modify existing blocks**

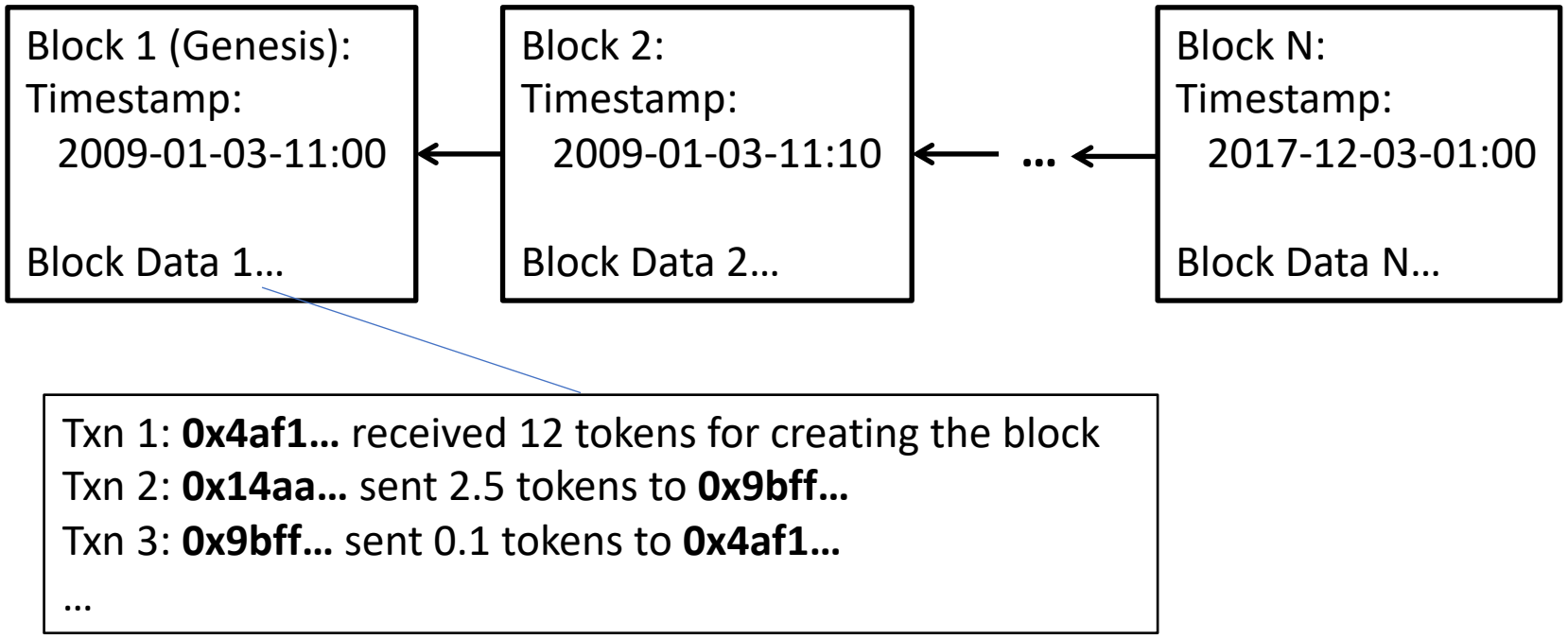
Cryptocurrency: Blockchain Storing Transactions

- The whole transaction history maintained by a network



Cryptocurrency: Blockchain Storing Transactions

- The whole transaction history maintained by a network



The Promise of Blockchain & Cryptocurrency

A system that is:

Decentralized

No central point of failure

Every node in the system works with the agreed protocol

Trustless

No central controls (e.g., government and central banks)

Anonymous

*Difficult to track real-world identifies behind transactions

History: From “Bitcoin” to “Blockchain”

Blockchain Timeline

2009-2010:	Bitcoin creation
2010-2012:	Scandals, hacks, and illegal activity
2013-2014:	Bitcoin attracts attention
2014-Present:	Ethereum
2015-Present:	Scalability struggles
2014-Present:	The buzzword “Blockchain”

2009-2010: Bitcoin Creation


WHO IS?
SATOSHI NAKAMOTO

Bitcoin: The first cryptocurrency

- Satoshi Nakamoto is the anonymous creator of Bitcoin who wrote a nine-page white paper that brilliantly combined all previous efforts to create a self-sustaining digital money.

- **Bitcoin White Paper:**
  - https://bitcoin.org/bitcoin.pdf
  - Must read for this class!

Bankground: Bank Bailouts and QE from Fed

- Lehman brothers bankrupt at 2008
- Many bank bailouts in Year 2009
- Quantitative easing of US Fed
  - Let’s just print money!

THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to launch ground offensive on Gaza

Hundreds of Israeli troops and tanks could enter the Gaza Strip this morning. At least 430 Palestinians have been killed in a week of airstrikes News, page 3

Michael Sheen Frost, Nixon and me

Magazine

Working mums So that's how she does it

Body&Soul

Detox in style The best spas on the planet

Travel

Salman Rushdie I won't marry again

Pages 22, 23

Giant killing? Guide to the FA Cup third round

Sport

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up

day that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would cut the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the hook" but accepted that they need

on state-backed guarantees to encourage private finance, but a wide range of interventions is on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad

debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

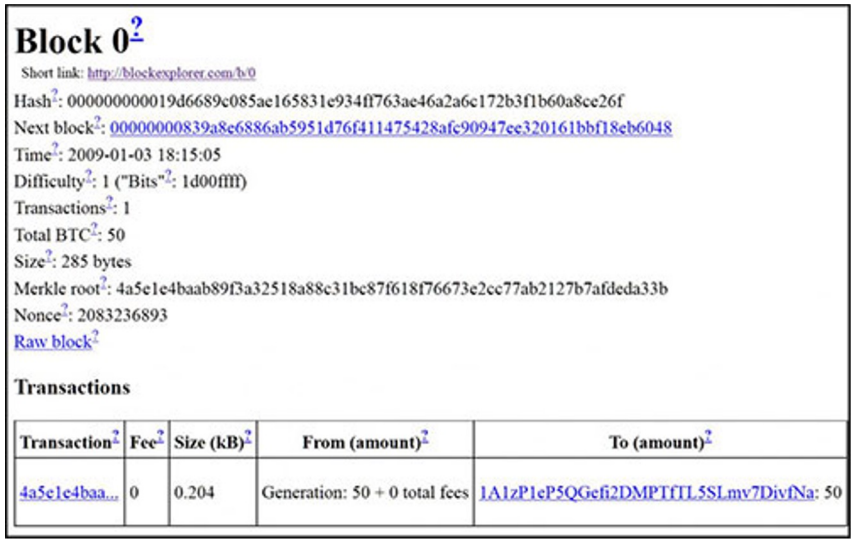
The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

99p

Pub chain cuts the price of a pint from £1.68 to 1980 levels

Genesis Block

- Genesis block mined at Jan 3, 2009
- The coinbase of the genesis block references a story in the Times of London newspaper involving the **Chancellor bailing out banks**
- First bitcoin transaction on Jan 12, 2009 with Hal



Block 0

Short link: http://blockexplorer.com/b/0

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Next block: 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Time: 2009-01-03 18:15:05

Difficulty: 1 ("Bits": 1d00ffff)

Transactions: 1

Total BTC: 50

Size: 285 bytes

Merkle root: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Nonce: 2083236893

Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa: 50

One Hundred Million Dollar Pizza

- On May 21, 2010, Laszlo Hanyecz purchased $25 worth of pizza for 10,000 BTC
- This was the world's first ever Bitcoin transaction for a tangible asset
- 10,000 BTC is now equivalent to $170,000,000

2010-2012:
Scandals, Hacks, Illegal activity

Mt. Gox

- In 2010 Mt. Gox was established and consolidated itself as the biggest bitcoin exchange during the beginning stages of bitcoin.
- On 6/19/11, Mt. Gox suffered a significant breach of security that resulted in fraudulent trading and required the site to be shut down for seven days.
- In 2014, Mt. Gox lost 744,408 bitcoins in a theft that went unnoticed for years
- Eventually, Mt. Gox declared bankruptcy

Silk Road

anonymous market

messages 0 | orders 0 | account B0

Search Go

Shop by Category

- Drugs 4,086
  - Cannabis 983
  - Dissociatives 77
  - Ecstasy 318
  - Opioids 350
  - Other 157
  - Precursors 18
  - Prescription 901
  - Psychedelics 587
  - Stimulants 405
- Apparel 82
- Art 5
- Books 778
- Collectibles 15
- Computer equipment 42
- Custom Orders 27
- Digital goods 369
- Drug paraphernalia 152
- Electronics 36
- Erotica 296
- Fireworks 5
- Food 4

100 x Anadrol 50MG Oxymetholone (sealed)

฿12.41

1 gram MDMA

฿5.89

1/2g Cocaine

฿5.44

10 Pieces White Heart 130-150mg MDMA Content

฿4.49

Red and White Filter (10 packs x 20 cigarettes)

฿1.90

VEGA 100mg Sildenafil citrate 4 tablets

฿1.50

10 gram Santa Maria

฿11.58

1/4 oz G13

฿8.13

Silk Road

- On February 2011, Silk Road opened for business: Silk Road, a Bitcoin marketplace, launched an illicit marketplace for drug deals, called the eBay for drugs.
- On October 2013, the FBI shut down Silk Road, seizing 3.6M dollars worth of bitcoin
- Ross Ulbricht, the founder of Silk Road, is currently serving a life sentence without possibility of parole

2013-2014:
Bitcoin attracts attention

Merchant Acceptance

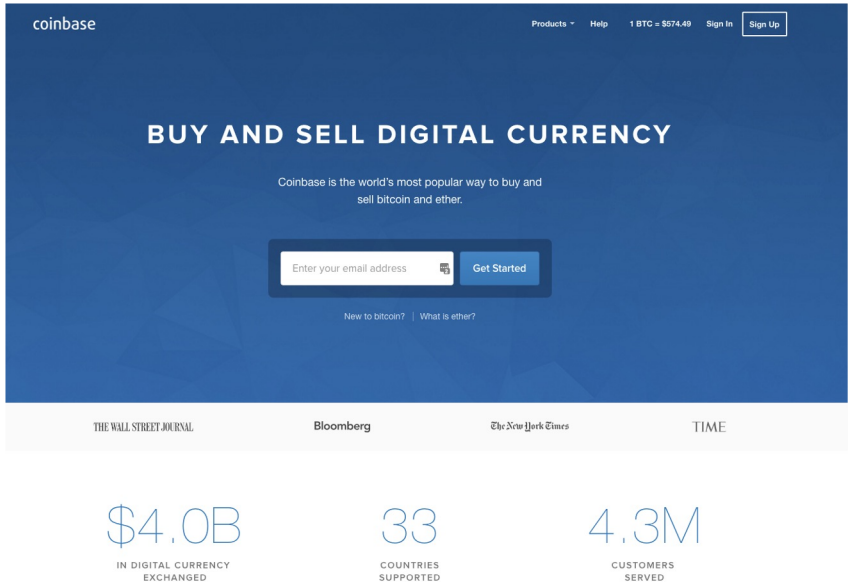
- (From CoinDesk)
  - 2014 Jan. Porn.com accepts Bitcoin
  - 2014 Jan. Overstock.com Becomes First Major Retailer to Accept Bitcoins
  - 2014 Apr. New Colorado Marijuana Vending Machines Will Accept Bitcoin
  - 2014 Sep. PayPal partners with and Coinbase, BitPay
  - 2014 Dec. Microsoft accepts Bitcoin payments
  - (2014 Oct.) "Whoever said that bitcoin couldn't buy you things? ... Shitexpress is a service that mails a tupperware container of horse manure with a personalised message on your behalf." - CoinDesk

Coinbase

Coinbase size representative of investor interest

Online wallet and exchange

- Coinbase founded June 2012, enrolled summer 2012 Y Combinator
- May 2013: $5 mil Series A
- December 2013: $25 million Series B
- July 2015: $75 million Series C



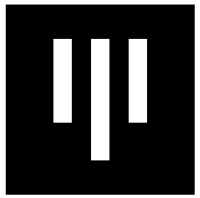
coinbase

Rise of venture funded startups

- Coinbase: Hosted wallet
- BitFinex: Online exchange/ trading platform
- 21 Inc: machine payments & embedded mining
- BitPay: allows merchants to accept Bitcoin for payment, convert to USD
- ChangeTip: social bitcoin micropayments
- Blockstream: Bitcoin Core, Sidechains, Research

BLOCKCHAIN CAPITAL

ANDREESSEN HOROWITZ



PANTERA

2015-2017: Ethereum Blows Up (in multiple ways)

2015-2017: Ethereum blows up (in multiple ways)

- Bitcoin is based off simple scripting language. Ethereum is a Turing-complete version of Bitcoin. Potential for complex decentralized apps
- History
  - Late 2013: Ethereum described in whitepaper by Vitalik Buterin
  - July and August 2014: Ethereum crowdsale
  - July 30th 2015: Ethereum blockchain launched
  - May 2016: Value of Ethereum tokens worth more than $1 billion
- Huge potential for new governance models
  - July 2016 (last month): TheDAO rise and hack

2015-Present: Scalability Struggle

Scalability Problem

Transactions per Second:	~7	~20	~200	~3000

Undesirable user experience, long processing delay, and skyrocketing transaction fees!

Blocksize Debate

- Bitcoin blocks created every 10 minutes
- In 2010, blocksize limit reduced to 1 MB
- In 2015, Bitcoin blocks started to "fill up"
- Huge scalability problem
- Divided the community - Blocksize Debate
- End up in the split of BTC and BCH

- Just increasing blocksize has severe security consequences!
- We will cover this in our course later

New Chains vs. Building Layers on Ethereum

- Improving performance requires completely new consensus algorithms.
- Hard to implement on existing chains with massive amount of assets.
- Many new layer ones emerges like Solana, Avalanche, Algorand, Conflux, etc. >1000 TPS

- Ethereum builds side chains as layer 2s to process excessive transactions
- Side chain transactions then later packed to the main Ethereum chain for verification.

The buzzword "blockchain" created by banks

Jamie Dimon Quotes on Bitcoin/blockchain

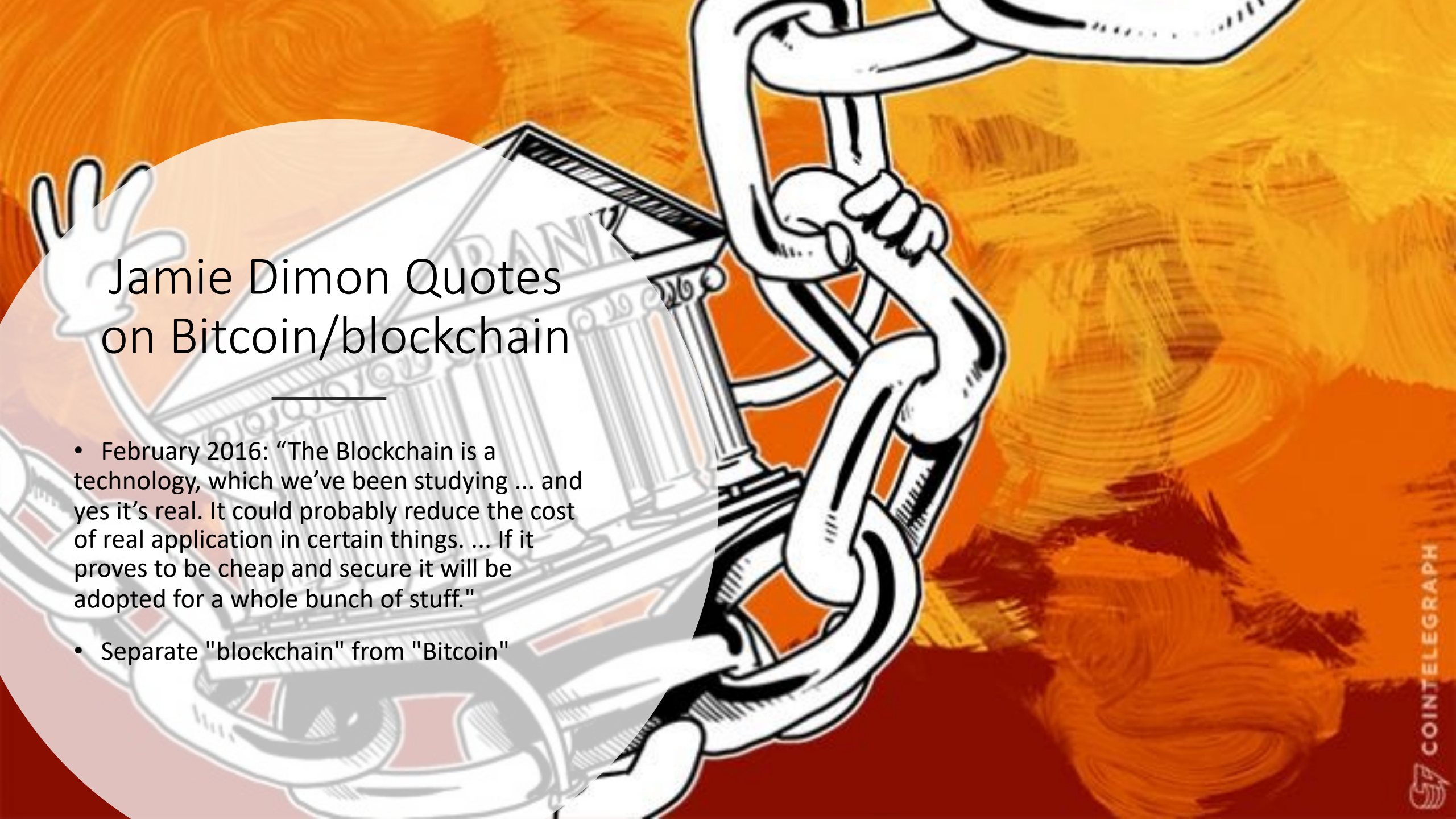
Nov 2015: “Virtual currency, where it’s called a bitcoin vs. a U.S. dollar, that’s going to be stopped. ... No government will ever support a virtual currency that goes around borders and doesn’t have the same controls. It’s not going to happen.”

Bankers hate the lack of control. Perhaps threatened?

http://fortune.com/2015/11/04/jamie-dimon-virtual-currency-bitcoin/

Jamie Dimon Quotes on Bitcoin/blockchain

- February 2016: “The Blockchain is a technology, which we’ve been studying ... and yes it’s real. It could probably reduce the cost of real application in certain things. ... If it proves to be cheap and secure it will be adopted for a whole bunch of stuff."
- Separate "blockchain" from "Bitcoin"



Interest in "blockchain" from banks

- Rise of interest in "private blockchains" or "permissioned ledgers."
  - Not open
  - Not trustless
  - No economic incentives like in Bitcoin
  - Separate "blockchain" from "Bitcoin"
- Con:
  - Often doesn't use consensus
  - Glorified public key cryptography
- Benefit: More compliant

"Private Blockchain" Initiatives

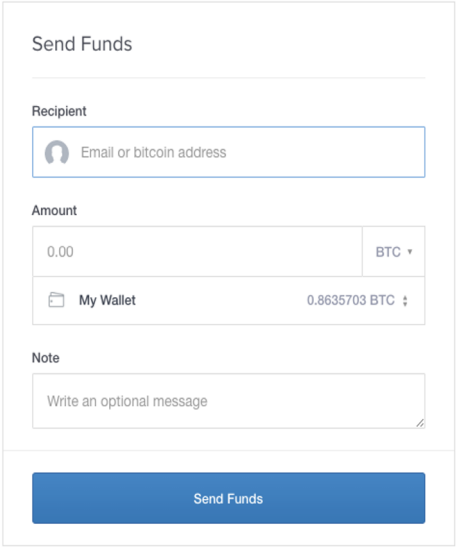
- Digital Asset Holdings
  - Founded by Blythe Masters
- Hyperledger Project: Open source blockchain
  - Run by Digital Asset Holdings and the Linux Foundation
- IBM Open Blockchain
  - Now part of Hyperledger project as "Fabric"
- JP Morgan Juno project
- Facebook Libra

Digital Asset

Bitcoin: Addresses and Transactions

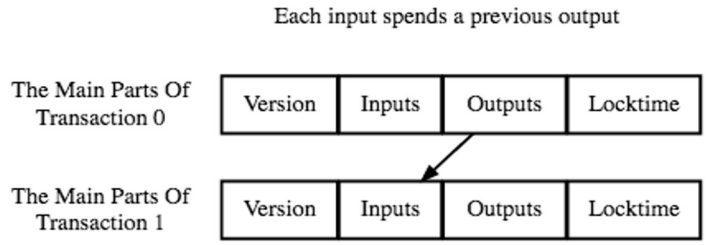
Basic Concepts - Identity in Bitcoin

- Bitcoin exists as software
  - Transactions are conducted through wallet software
  - Wallet creation generates a Bitcoin address
- To receive money, you share your address
  - Sender specifies address and amount
- The transaction is broadcast to the network, where "miners" verify it and add it to the transaction history



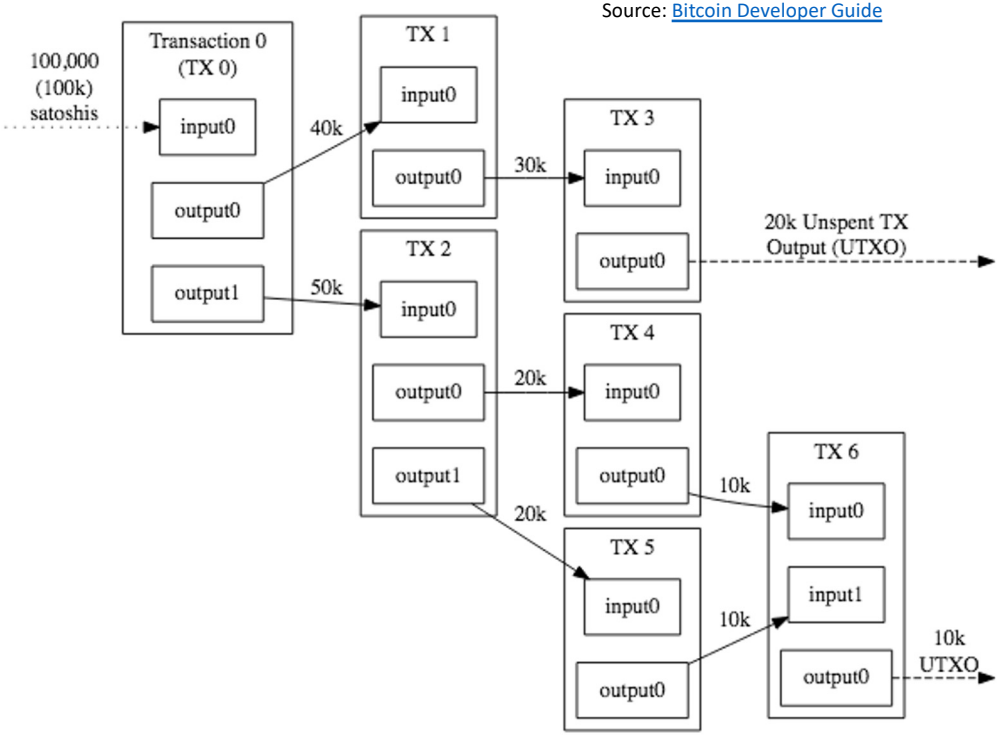
Basic Concepts – Transactions

- Maps inputs addresses to output addresses and amount
  - Outputs can only be spent once
- Typical tx: one input, two outputs
- Fees are implicit



Each output waits as an Unspent TX Output (UTXO) until a later input spends it

Source: Bitcoin Developer Guide

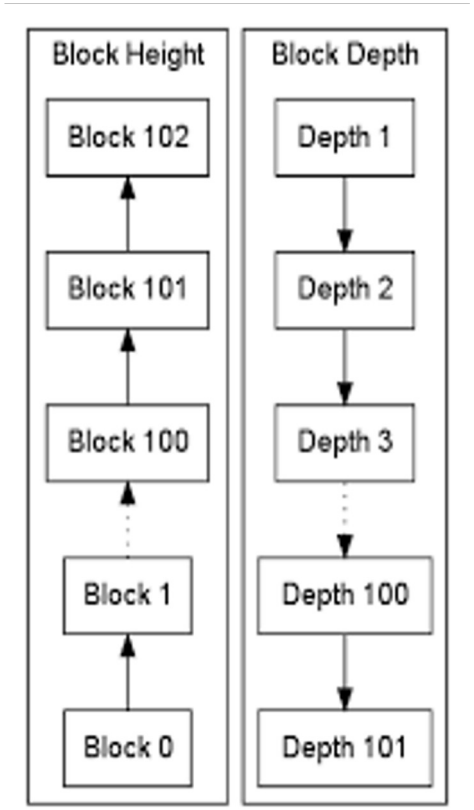


Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Basic Concepts – Blocks + Blockchain

Blocks

- Contains an ordered bunch of transactions
  - Timestamps the transactions, are immutable
- Each block References a previous block
- Each block has height and depth (confirmations)
  - Currently 666k blocks



Block Height Compared To Block Depth

Source: [Bitcoin Developer Guide]

Transaction View information about a bitcoin transaction

447cb6623db32b5f28c94ac10551802075f053208fe995204a145197e2904bb9

3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v (44,000 BTC - Output)	3LrLWTSdd69oZVVQ6dtWaAAaBLn7N3rRjz - (Spent)	333.33328889 BTC
	3QkXtcSWJA9w77eCujnMBKDWFe7F7zwxTg - (Spent)	333.33328889 BTC
	3Qd7hXZoZ1iyXZznrbdUwUQBxHMmujdqhJ - (Spent)	333.33328889 BTC
	3ECJwvx9VgfotcUuEJMVNvmWnTGVMk179L - (Spent)	333.33328889 BTC
	3BuQmbmdce3e31GEovq5SgowLdfMgJzLDE - (Spent)	333.33328889 BTC
	3NwKLjJjzXSnBFQWokXRgBG3JeuF3bsnfE - (Spent)	333.33328889 BTC
	3GEaT8ZRXELcjMSFvGro6eZcC5S1LSLZuN - (Spent)	333.33328889 BTC
	35DVAzDtZDKAU94kFT9sxoscnuLCTxgwYc - (Spent)	333.33328889 BTC
	3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v - (Unspent)	38,000 BTC
	35mwqShnStDro6uEB4bmsgbyBo8en6Byfm - (Spent)	333.33328889 BTC
	39pvSqfNcUosc8RGVWxyzKM3ny96a3uSkW - (Spent)	333.33328889 BTC
	39QNJSgQg5JnBXAtbF8ezkDn72VqWdPZPJ - (Spent)	333.33328889 BTC
	3L9qAGBQLbXkFAB2GpijnJXPScSVjuiJio - (Spent)	333.33328889 BTC
	37WSkANPVUQ8uuktf8hv671CejRtBtQ4tJ - (Spent)	333.33328887 BTC
	3EEwPZZ6pYRJSotCz9RBoVYPRnoWyGWEka - (Spent)	333.33328889 BTC
	3C4ABC7iPcAAKBh6SJXfvUSDBew3abCtw3 - (Spent)	333.33328889 BTC
	3HpQozfTzoXAsHf87m2mwJXUQ14LVtLgK4 - (Spent)	333.33328889 BTC
	337RfngTLRTpU7RT9sKWQWDdmfcdmWnugi - (Spent)	333.33328889 BTC
	3P2eoKr3vAeZhJcTzon3VFkv5r7DqSXW9G - (Spent)	333.33328889 BTC
		43,999.9992 BTC

Summary	
Size	1055 (bytes)
Received Time	2016-08-30 11:45:03
Included In Blocks	427512 (2016-08-30 11:51:09 + 6 minutes)
Confirmations	854 Confirmations
Relayed by IP	5.39.93.85 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	44,000 BTC
Total Output	43,999.9992 BTC
Fees	0.0008 BTC
Estimated BTC Transacted	333.33328887 BTC
Scripts	Hide scripts & coinbase

BLOCKCHAIN info | Home | Charts | Stats | Markets | API | Wallet | Search | English

Transaction View information about a bitcoin transaction

447cb6623db32b5f28c94ac10551802075f053208fe995204a145197e2904bb9

One-way crypto-hash functions!

How bitcoin gets the transaction id?

3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v (44,000 BTC - Output)

3LrLWTSdd69oZVVQ6dtWaAAaBLn7N3rRjz - (Spent)	333.33328889 BTC
3QkXtcSWJA9w77eCujnMBKDWFe7F7zwxTg - (Spent)	333.33328889 BTC
3Qd7hXZoZ1iyXZznrbdUwUQBxHMmujdqhJ - (Spent)	333.33328889 BTC
3ECJwvx9VgfotcUuEJMVNvmWnTGVMk179L - (Spent)	333.33328889 BTC
3BuQmbmdce3e31GEovq5SgowLdfMgJzLDE - (Spent)	333.33328889 BTC
3NwKLjJjzXSnBFQWokXRgBG3JeuF3bsnfE - (Spent)	333.33328889 BTC
3GEaT8ZRXELcjMSFvGro6eZcC5S1LSLZuN - (Spent)	333.33328889 BTC
35DVAzDtZDKAU94kFT9sxoscnuLCTxgwYc - (Spent)	333.33328889 BTC
3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v - (Unspent)	38,000 BTC
35mwqShnStDro6uEB4bmsgbyBo8en6Byfm - (Spent)	333.33328889 BTC
39pvSqfNcUosc8RGVWxyzKM3ny96a3uSkW - (Spent)	333.33328889 BTC
39QNJSgQg5JnBXAtbF8ezkDn72VqWdPZPJ - (Spent)	333.33328889 BTC
3L9qAGBQLbXkFAB2GpijnJXPScSVjuiJio - (Spent)	333.33328889 BTC
37WSkANPVUQ8uuktf8hv671CejRtBtQ4tJ - (Spent)	333.33328887 BTC
3EEwPZZ6pYRJSotCz9RBoVYPRnoWyGWEka - (Spent)	333.33328889 BTC
3C4ABC7iPcAAKBh6SJXfvUSDBew3abCtw3 - (Spent)	333.33328889 BTC
3HpQozfTzoXAsHf87m2mwJXUQ14LVtLgK4 - (Spent)	333.33328889 BTC
337RfngTLRTpU7RT9sKWQWDdmfcdmWnugi - (Spent)	333.33328889 BTC
3P2eoKr3vAeZhJcTzon3VFkv5r7DqSXW9G - (Spent)	333.33328889 BTC

43,999.9992 BTC

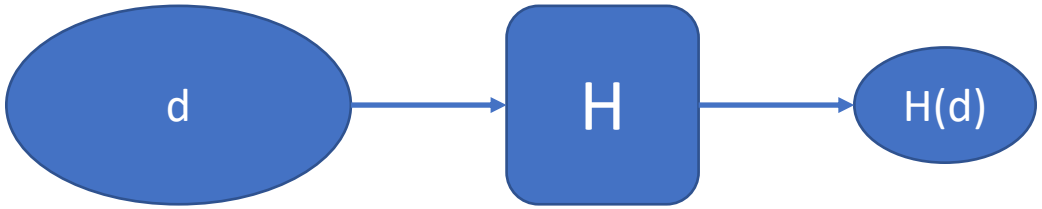
Summary	
Size	1055 (bytes)
Received Time	2016-08-30 11:45:03
Included In Blocks	427512 (2016-08-30 11:51:09 + 6 minutes)
Confirmations	854 Confirmations
Relayed by IP	5.39.93.85 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	44,000 BTC
Total Output	43,999.9992 BTC
Fees	0.0008 BTC
Estimated BTC Transacted	333.33328887 BTC
Scripts	Hide scripts & coinbase

Crypto Basic Constructs for Blockchains

One-way Crypto Hash Function

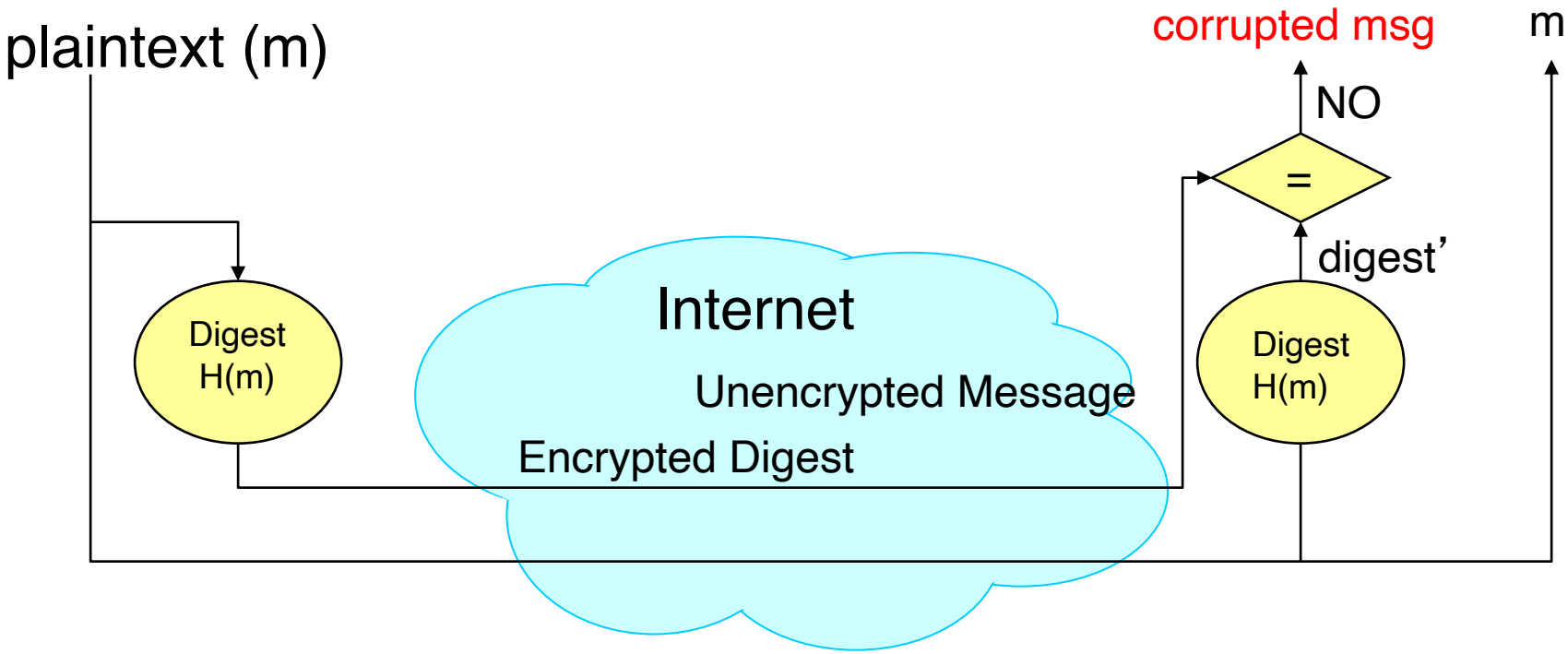
- For data d, H(d) generates a fixed-size hash for d



- **Collision Resistance**: Difficult to find x and y, such that H(x) == H(y)
- **Hard to Reverse**: Given a, it is hard to find d such that H(d) = a

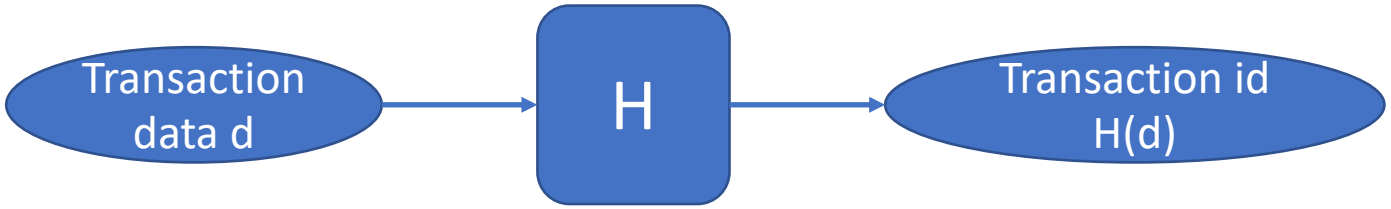
One-way Crypto Hash Function

- Commonly used to detect message corruption

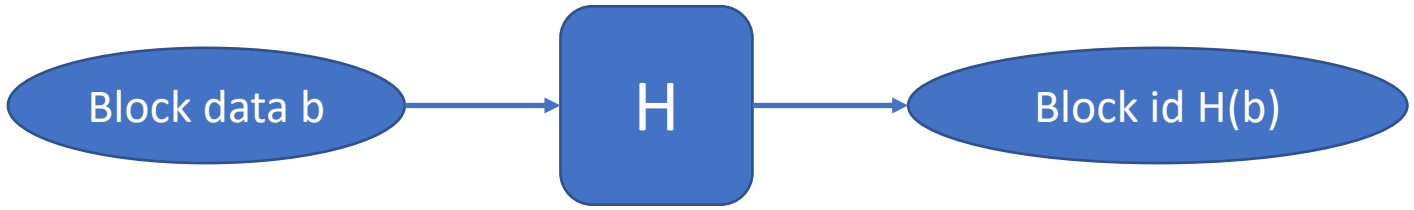


One-way Hash Usage in Blockchain

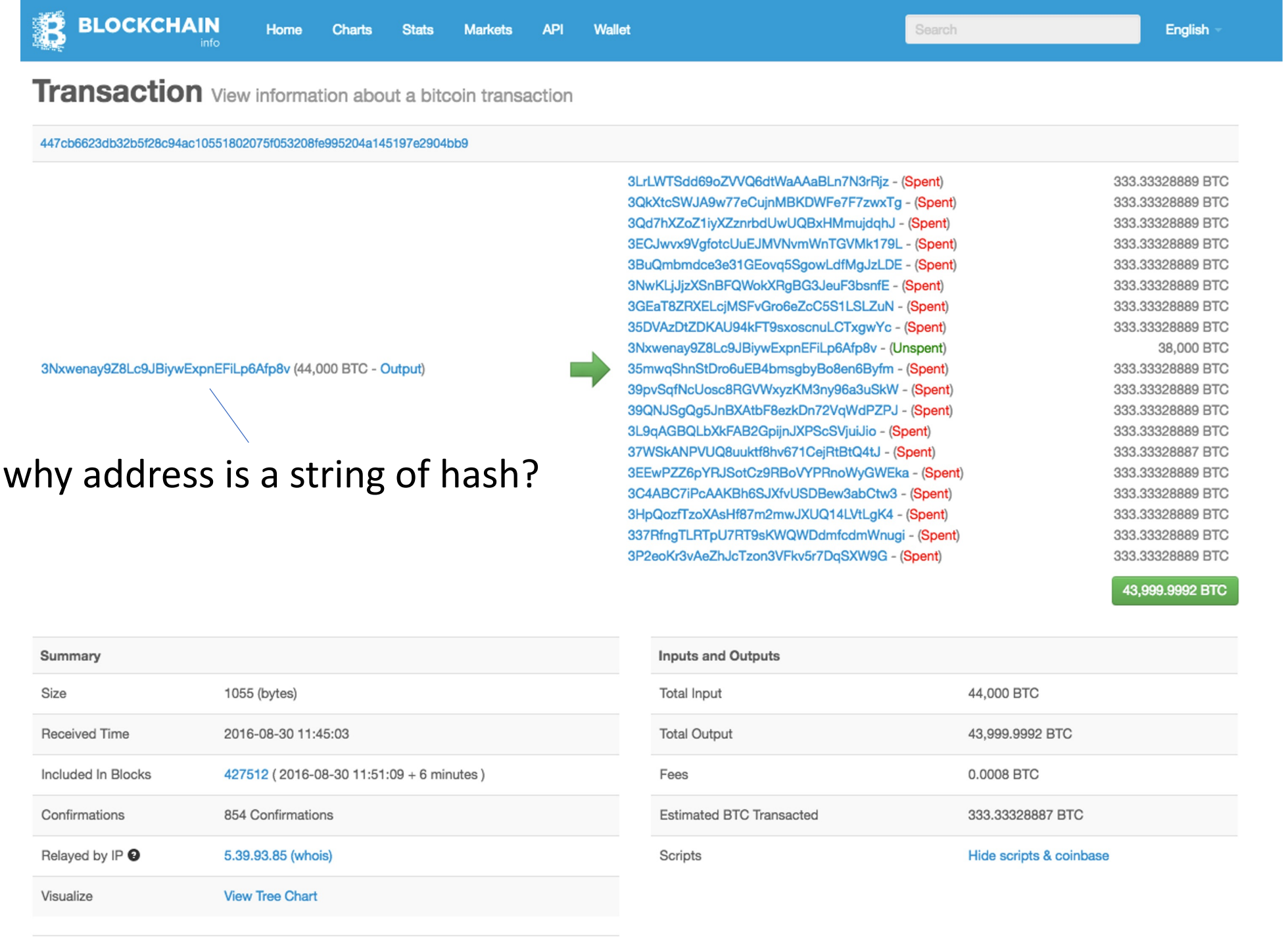
- Generate Unique Transaction Identifier



- Generate Unique Block Identifier



- Conveniently detect duplicate transactions and blocks
  - Bitcoin uses SHA256/SHA3 (Kaccak)



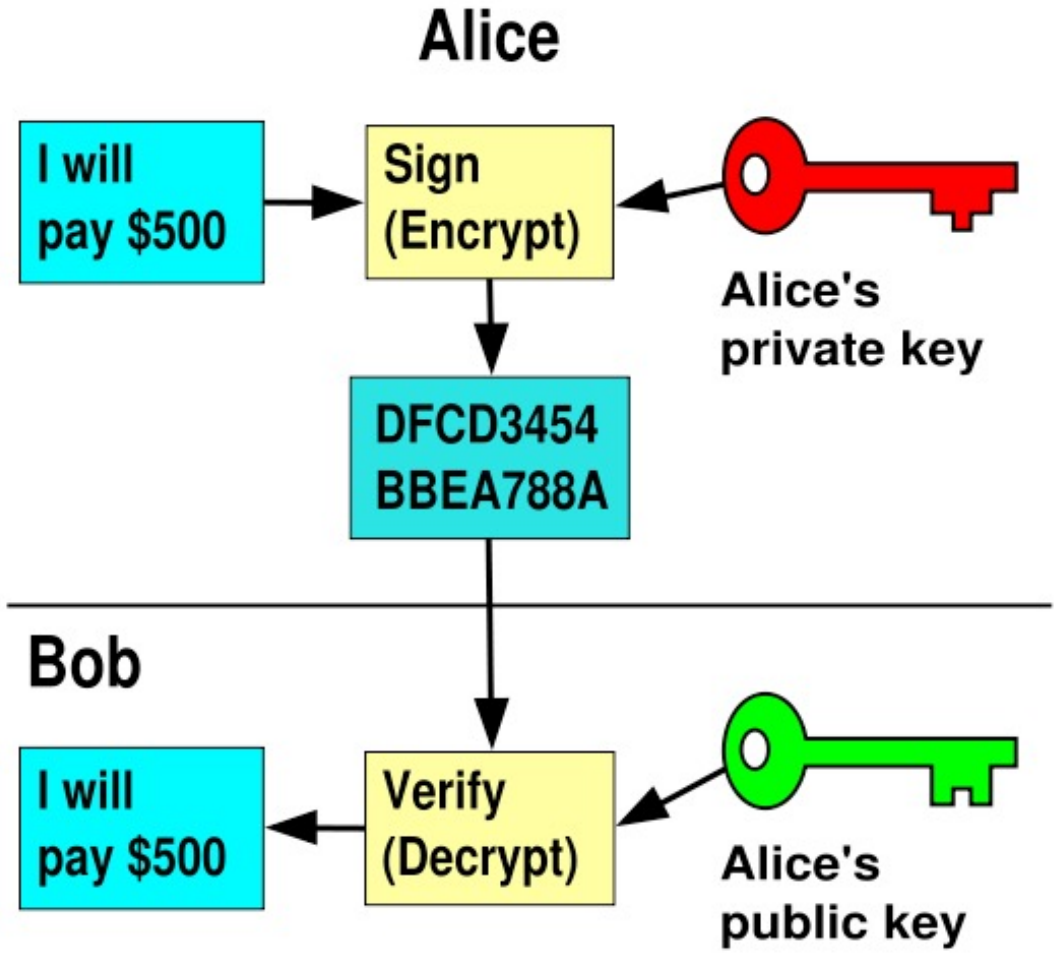
So why address is a string of hash?

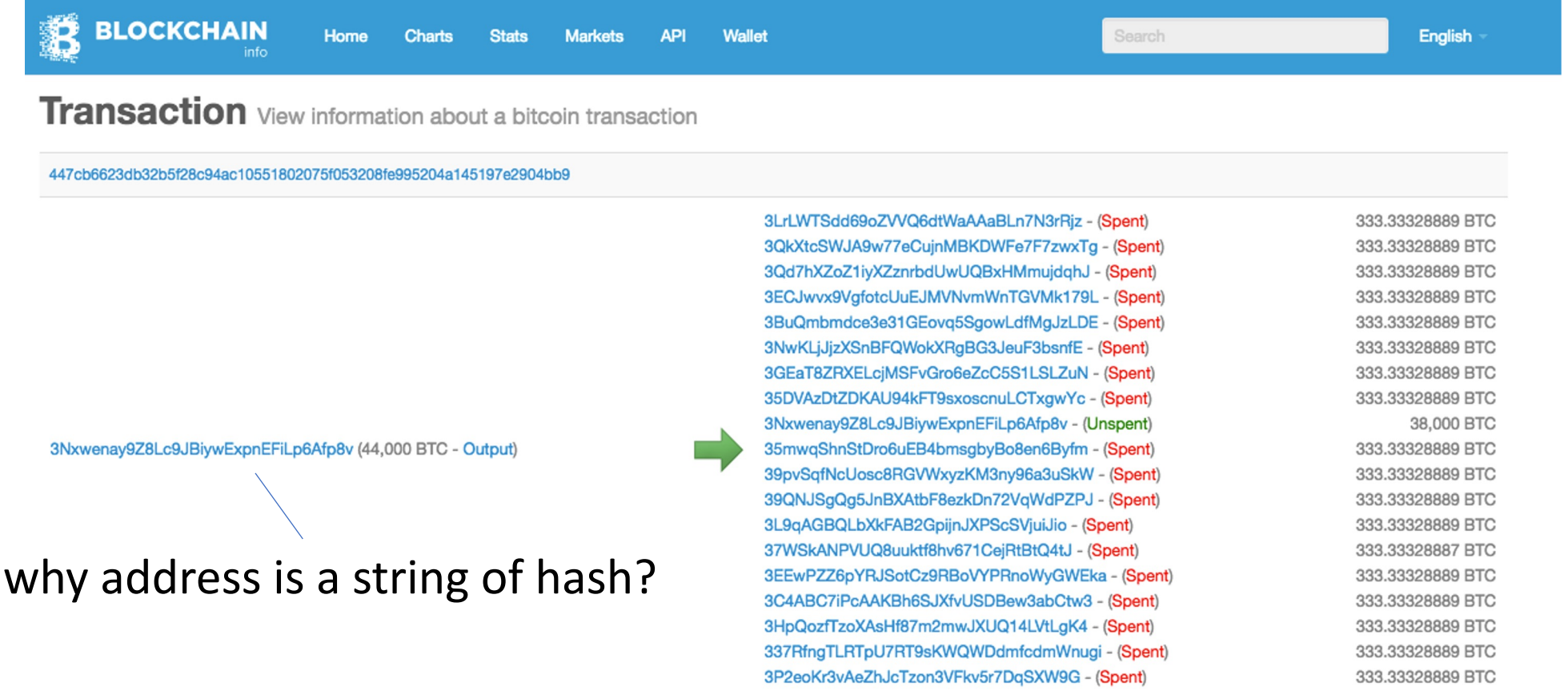
Asymmetric Encryption & Signatures

- Alice has a private key K_E and a public key K_D
- Alice can use private key to sign a message m:
  - Alice sends an encrypted message $E(m, K_E)$ of **m** based on K_E
  - Everyone can use K_D to verify that the owner of K_E sent m
- **Non Repudiation**: Alice cannot deny he sent the message!

- Bitcoin uses Elliptic Curve Digital Signature Algorithm:
  - Addresses in Bitcoin correspond to public keys
  - Smaller signature size than RSA

Asymmetric Encryption & Signatures



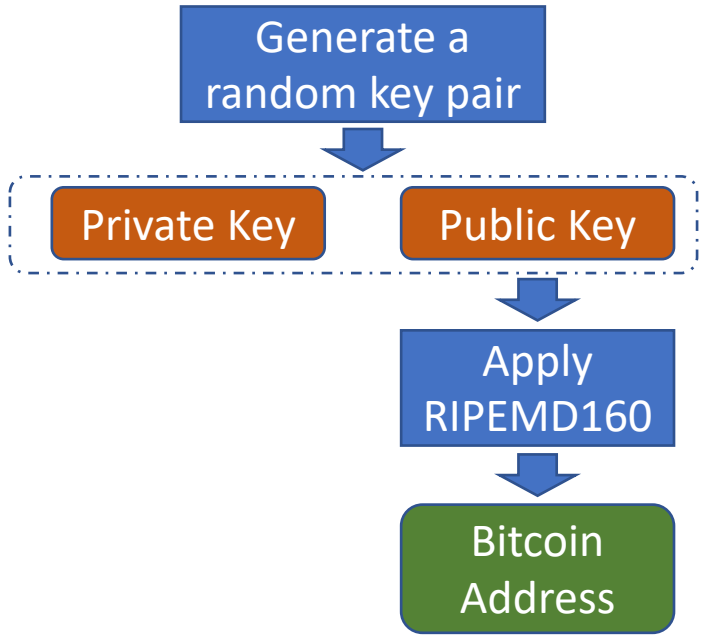


So why address is a string of hash?

In Bitcoin, this address corresponds to the public key!

Address v.s. Public Key

- In Bitcoin implementation, an address is an one-way hash result of the public key
  - Shorter and normalized addresses
- To send a transaction, sender provides:
  - Public key
  - Signature generated with the private key
- To verify a transaction:
  - Check the public key matches the sender's address
  - Check the signature is correct



Nakamoto Consensus in Bitcoin

Bitcoin – Key Properties

- Valid transactions eventually go through with high probability
  - Alice send Bob 1 BTC
  - Eventually, this transaction will be included into the blockchain

- **No double spending**
  - Alice cannot later send Charlie 1 BTC that she already sent to Bob
  - No one can modify existing blocks in the blockchain

How to achieve decentralized consensus on transactions?

Slide by
Viget

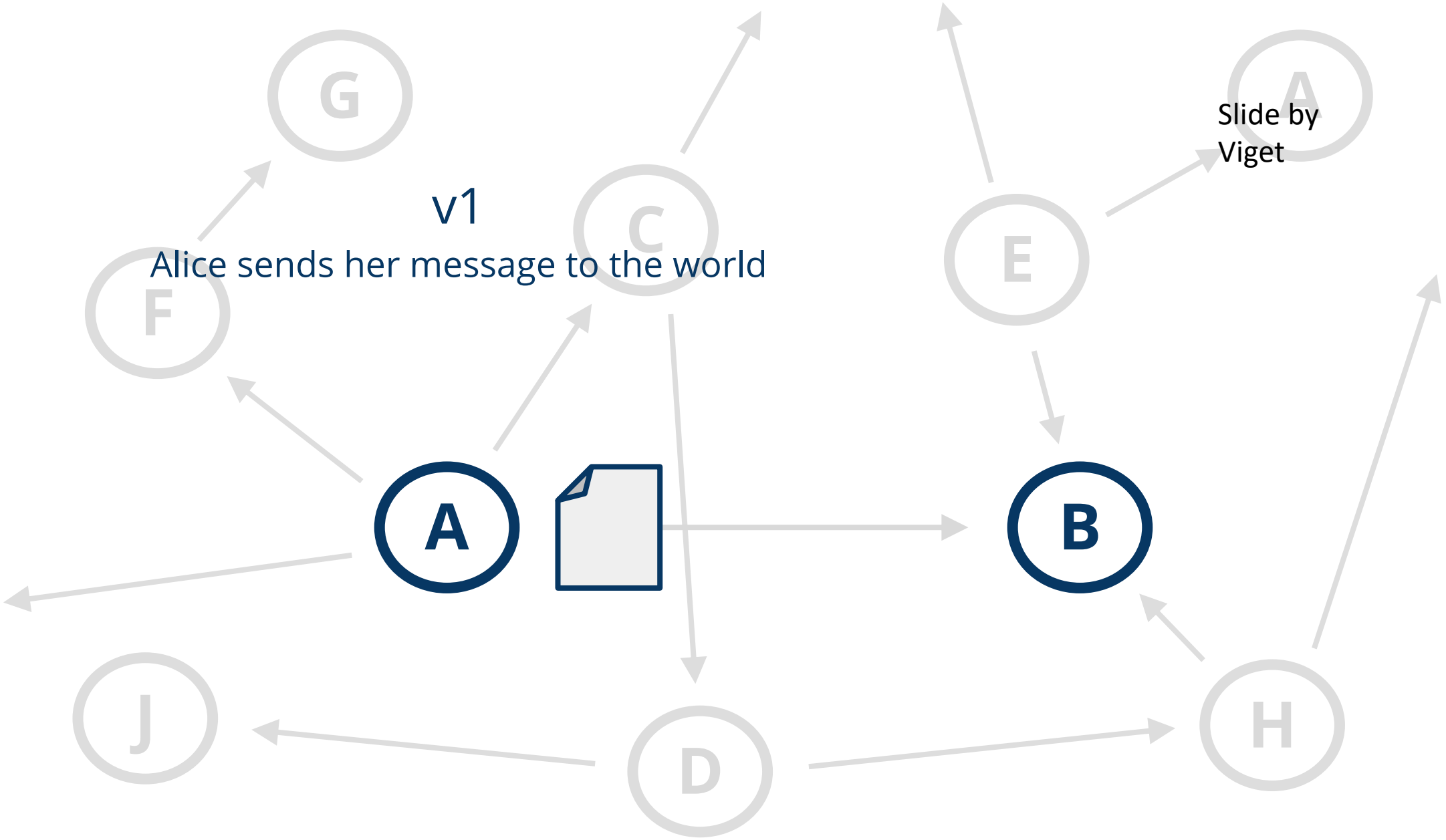
v1

Alice writes and signs a message describing her transaction

“I, Alice, am giving Bob one bitcoin.”

v1

Alice sends her message to the world



Slide by Viget

v1

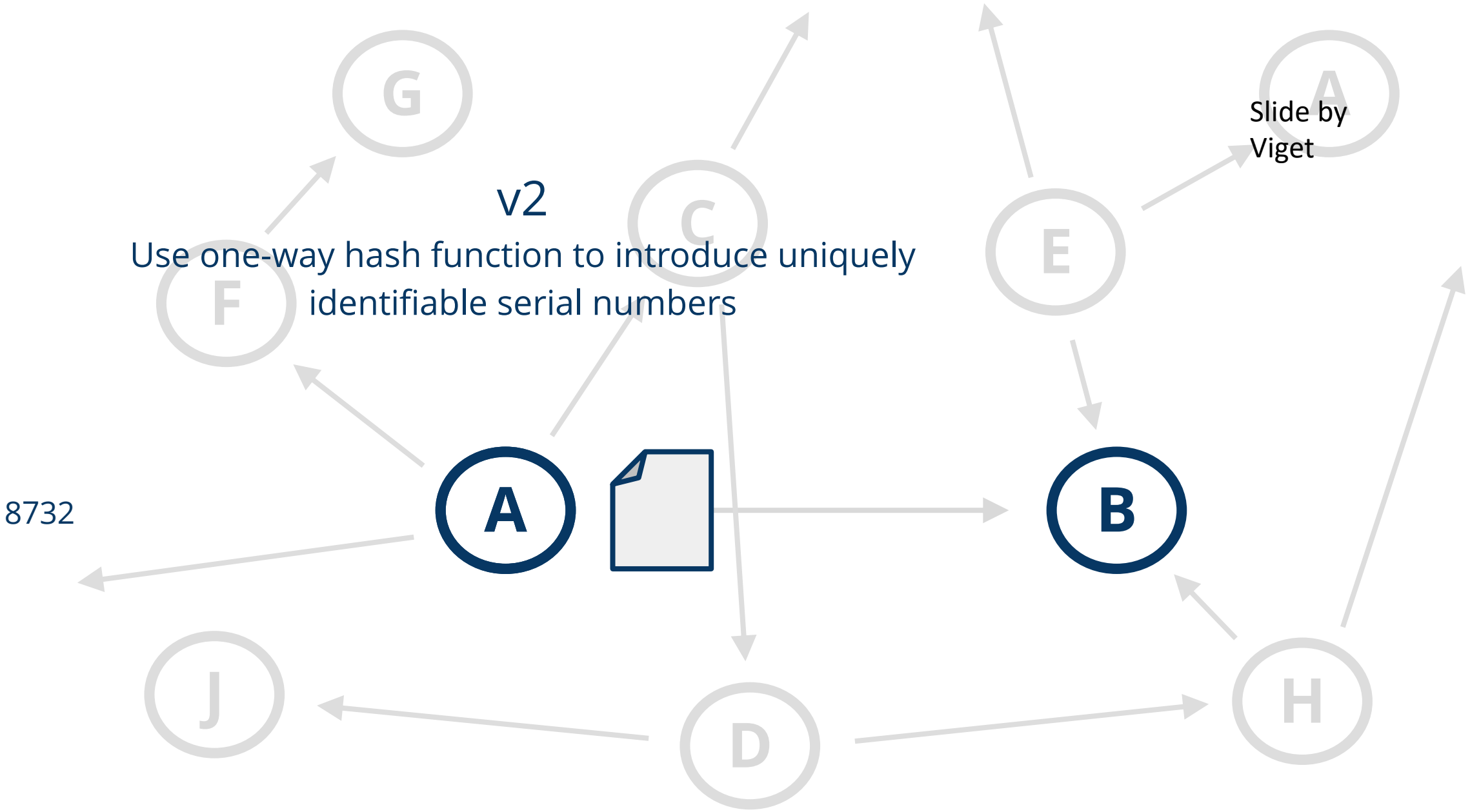
Alice sends five identical messages

?

Slide by Viget

v2

Use one-way hash function to introduce uniquely identifiable serial numbers



Slide by Viget

v2

Who manages the transactions?

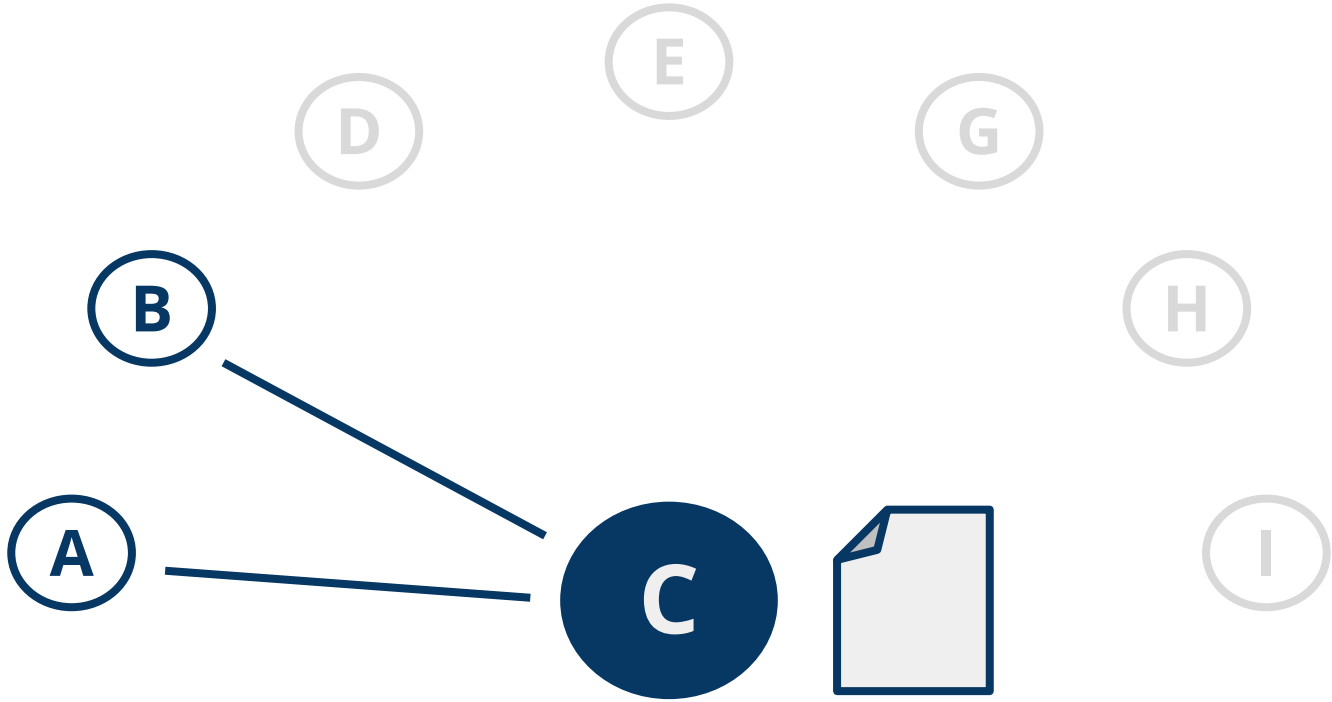
8732

?

Slide by
Viget

v2

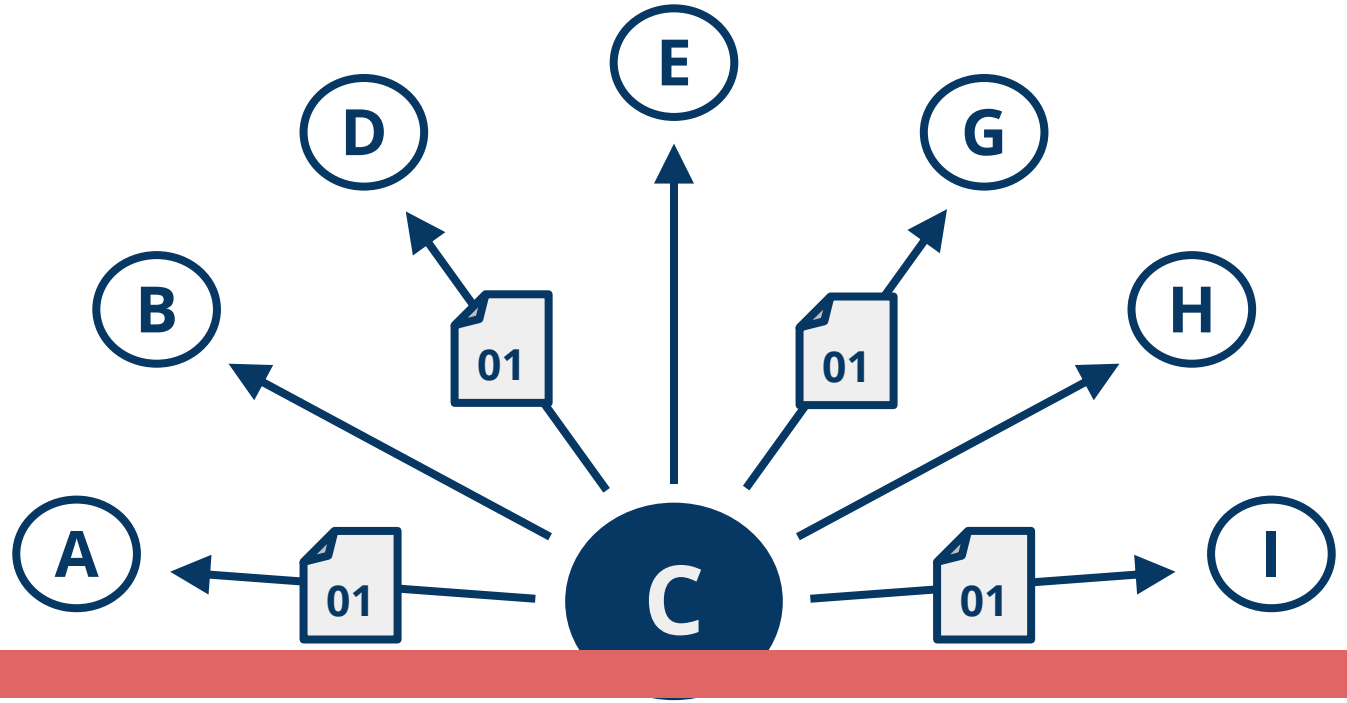
A central bank manages transactions and balances



Slide by
Viget

v2

Centralization



Slide by
Viget

v3

Making everyone the bank

Slide by
Viget

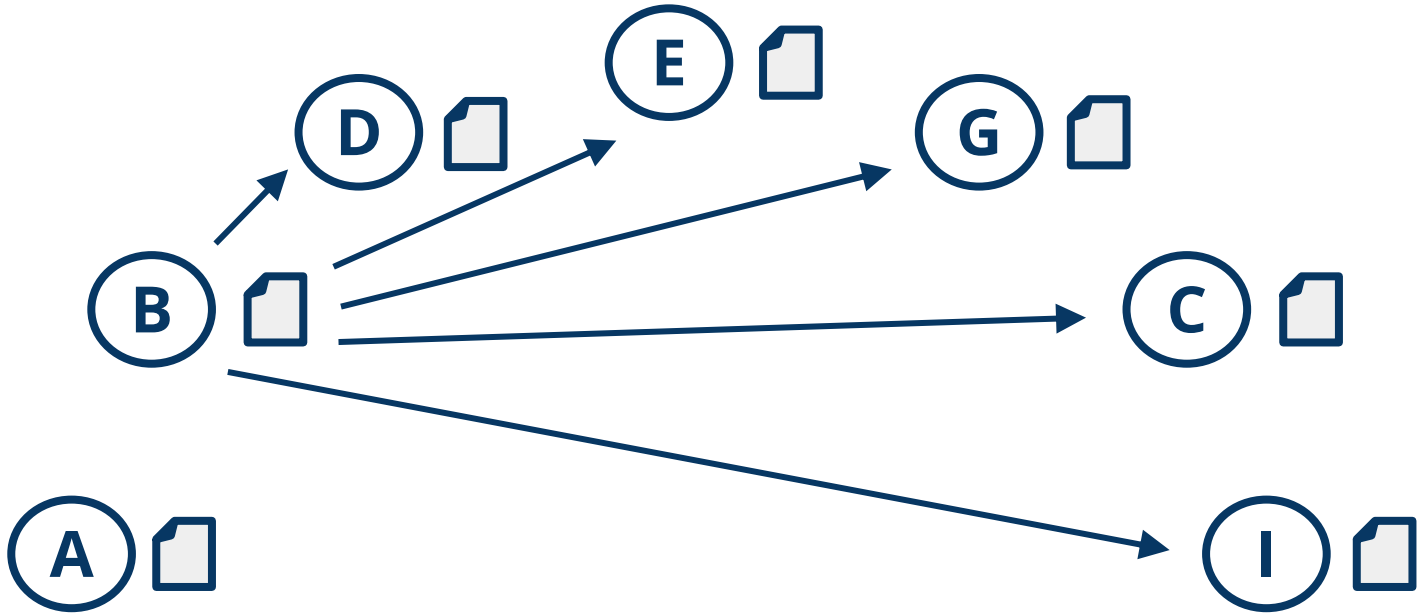
v3

Alice sends her transaction to Bob

Slide by Viget

v3

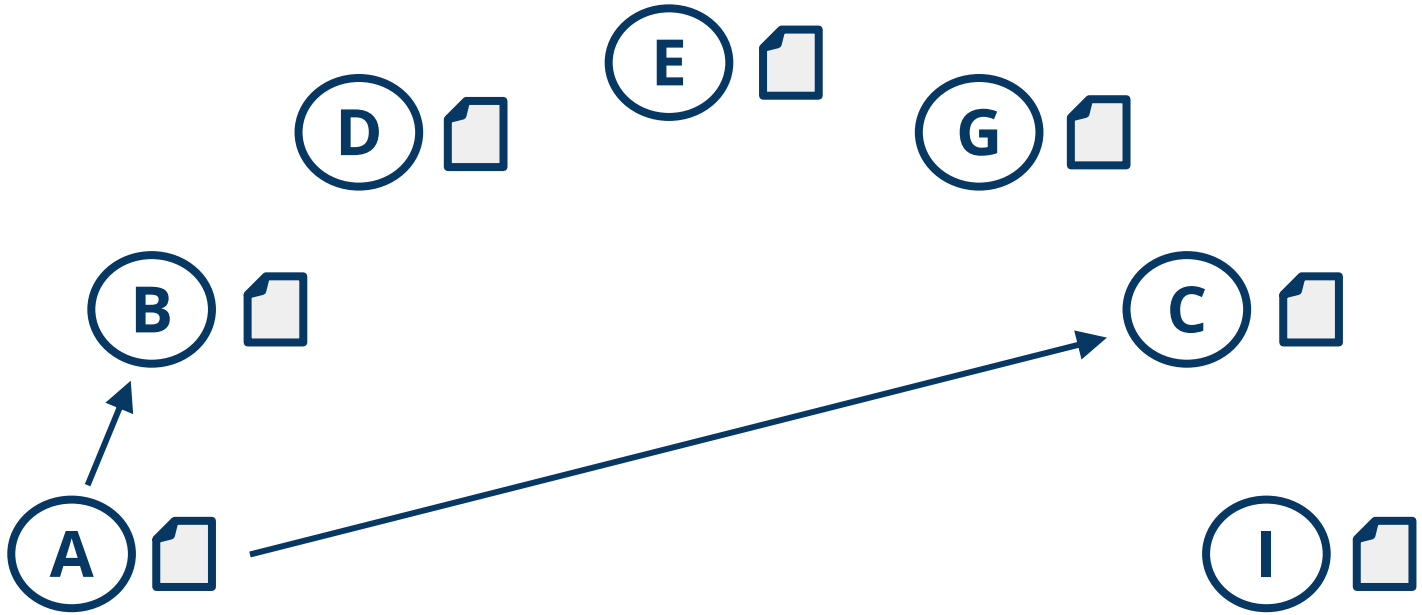
Bob announces the transaction to the world



Slide by Viget

v3

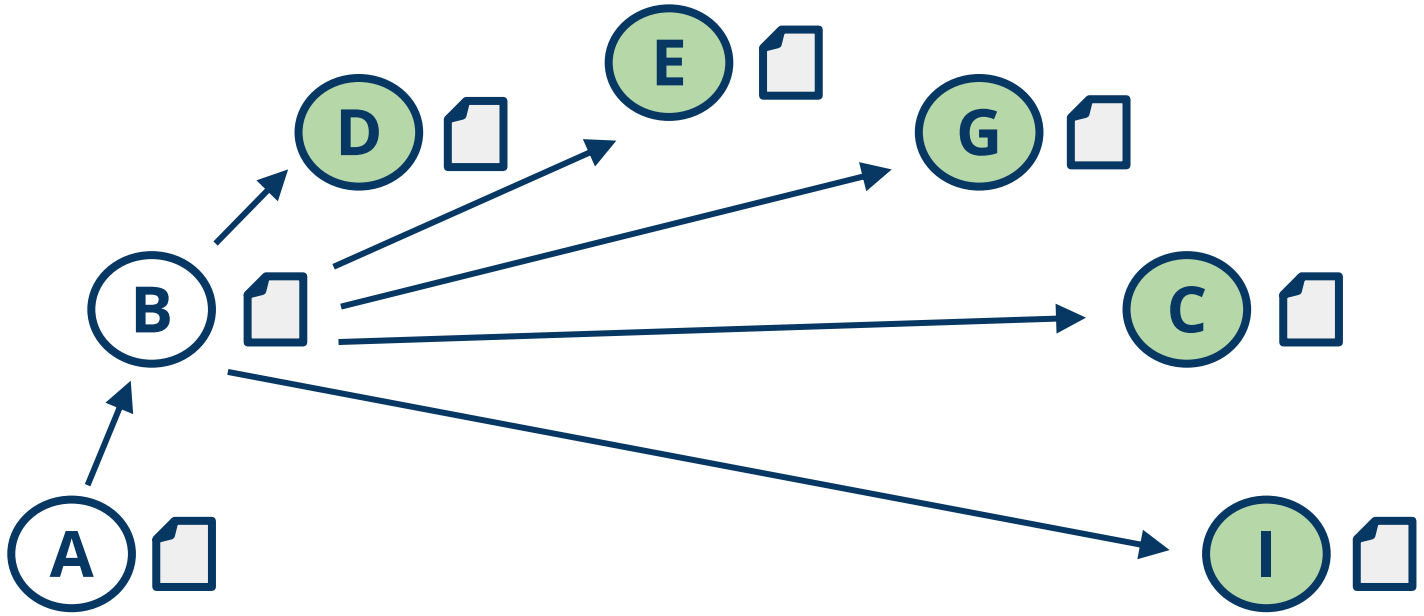
Alice double spends on Bob and Charlie



Slide by
Viget

v4

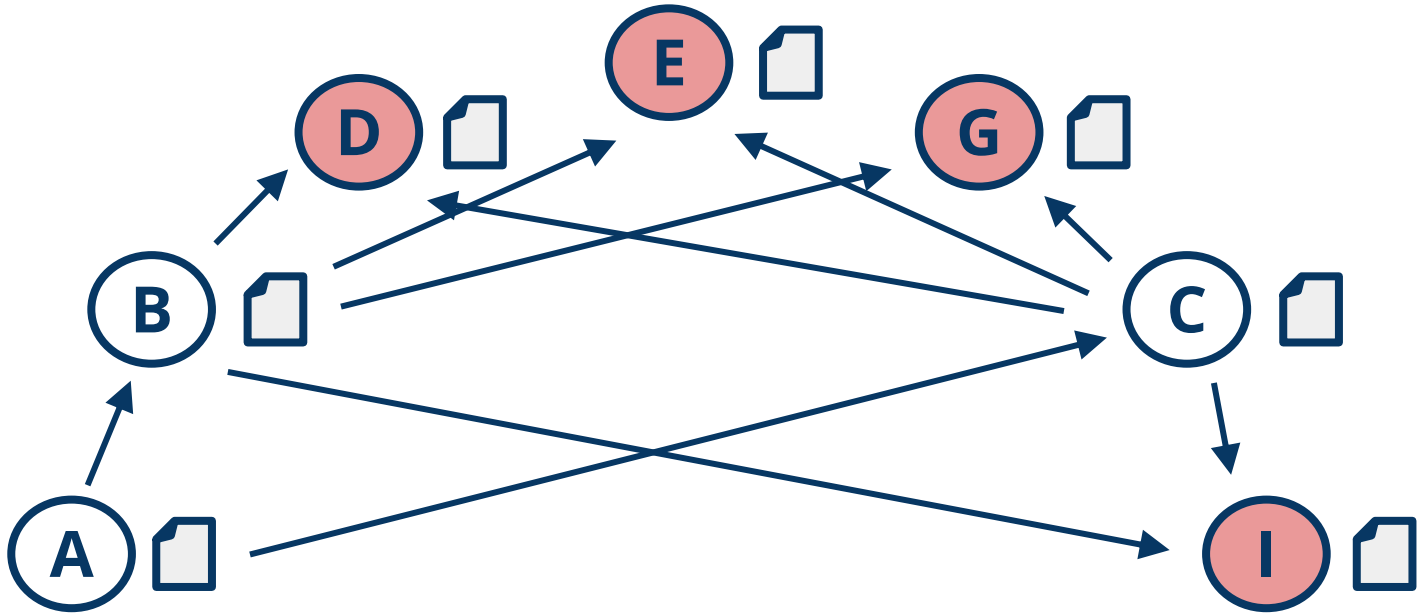
Everyone verifies transactions



Slide by
Viget

v4

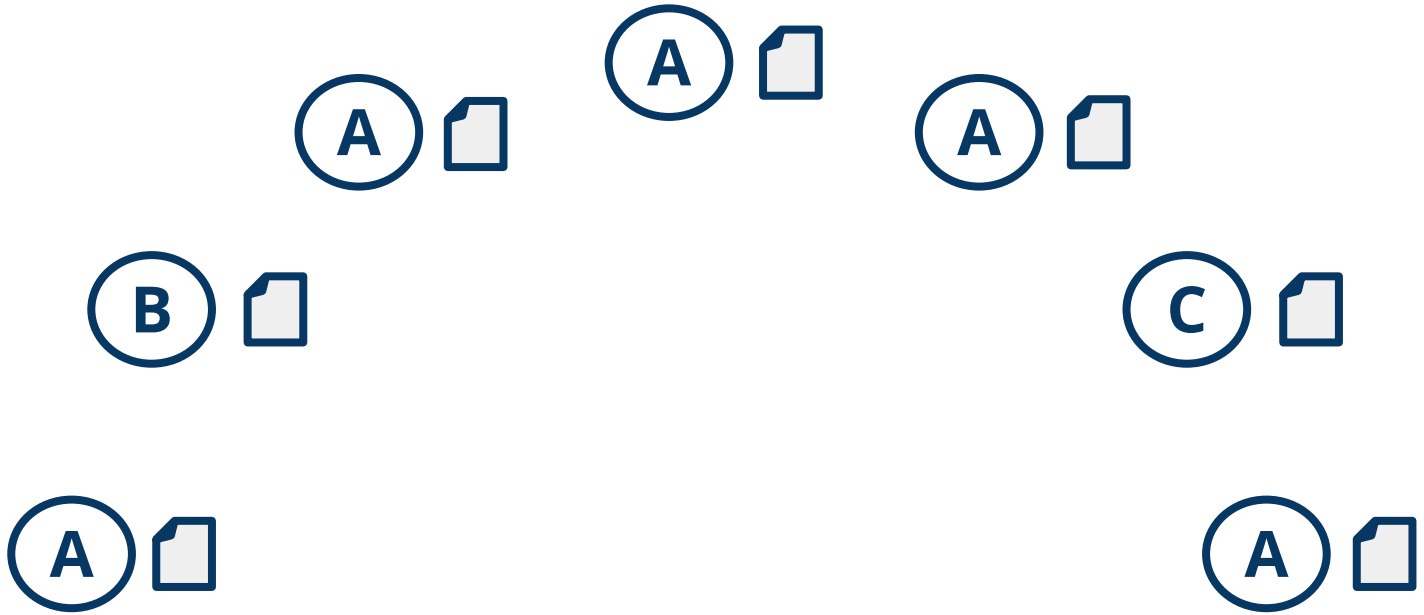
Alice is prevented from double spending



Slide by Viget

v4

Alice sets up multiple identities

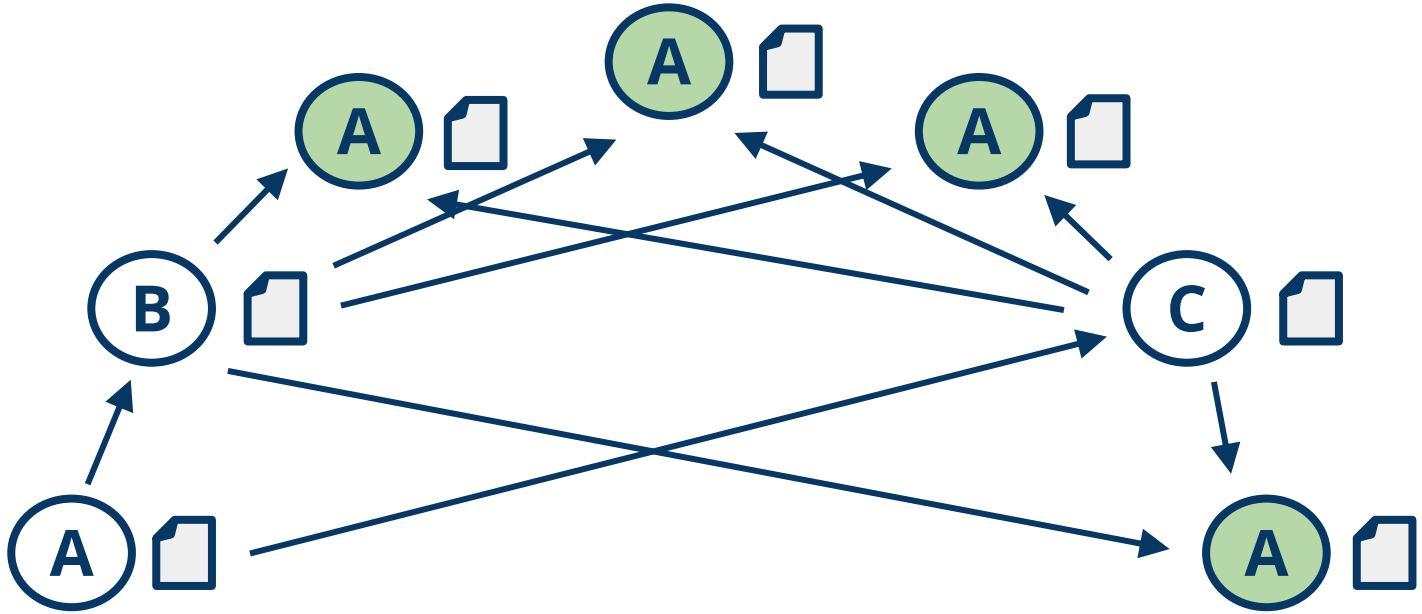


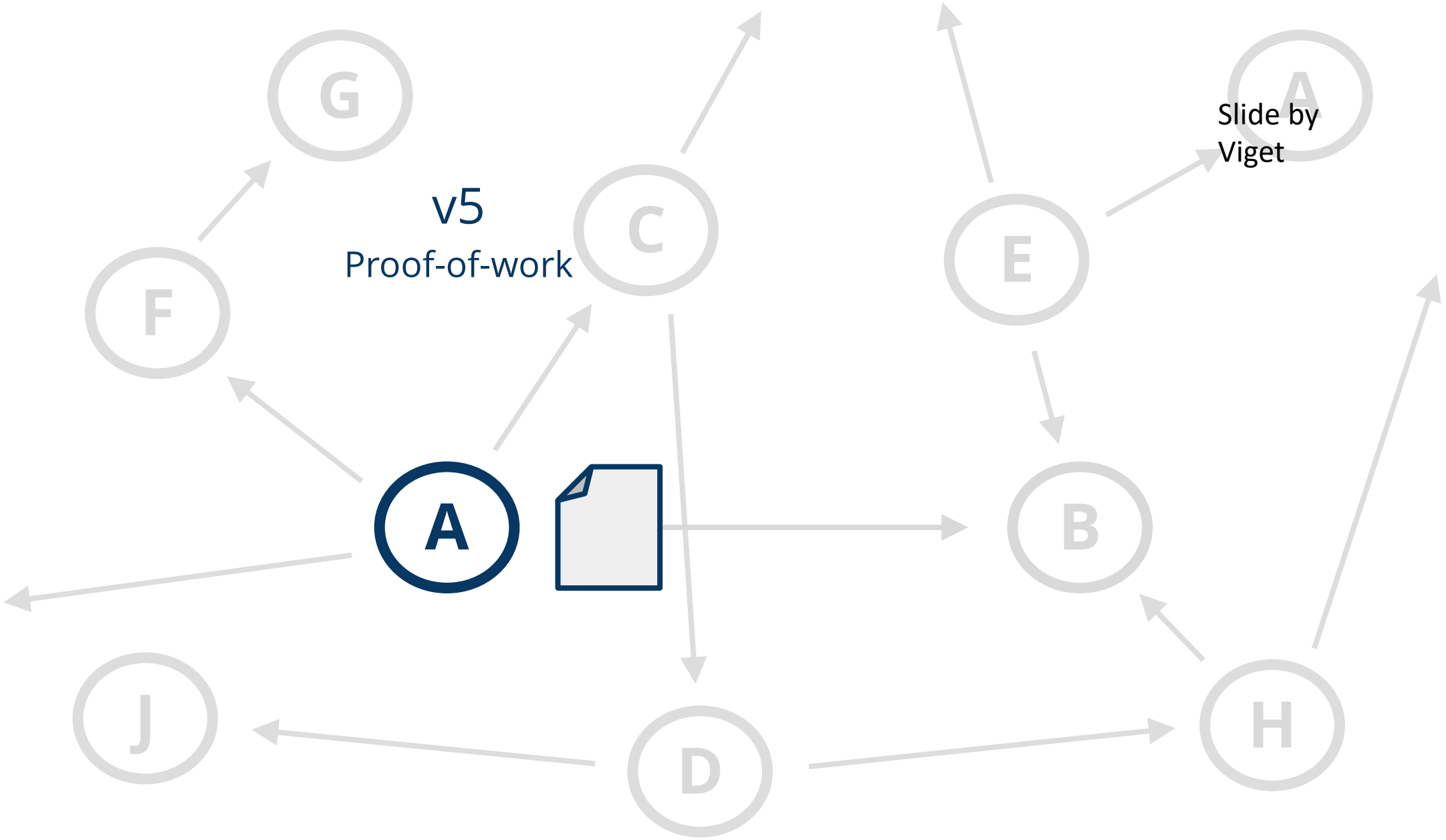
Slide by Viget

v4

Alice double spends with her multiple identities

Sybil Attack: Done by creating many fake identities




v5
Proof-of-work
Slide by
Viget
G
C
A
F
E
A
B
J
D
H

Slide by Viget

v5

Pending transactions

1. I, Tom, am giving Sue one bitcoin, with serial number 3920.
2. I, Sydney, am giving Cynthia one bitcoin, with serial number 1325.
3. I, Alice, am giving Bob one bitcoin, with serial number 1234.

Slide by Viget

v5

Verifying transactions

1 2 3

Slide by
Viget

v5

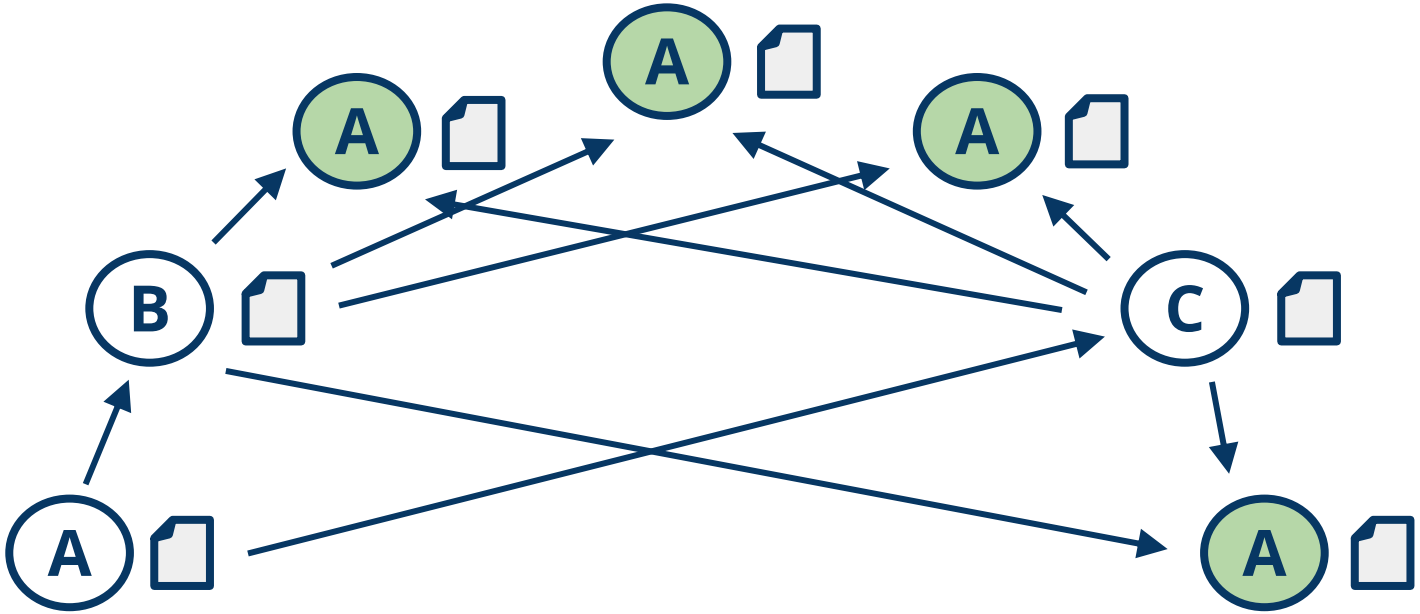
Why the math?

Slide by Viget

v5

Alice **cannot** create multiple identities anymore because it is costly to do so

One CPU one vote!



Slide by
Viget

v5

Proof-of-work as a competition

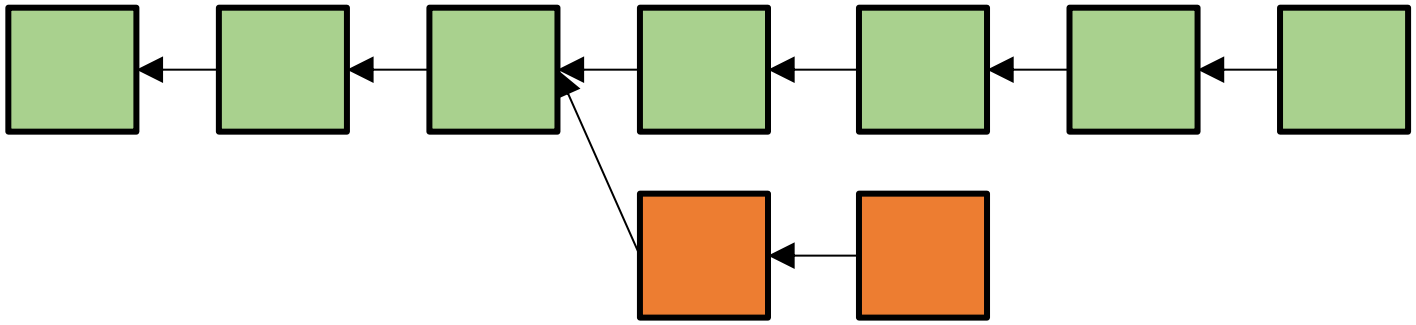
Slide by Viget

Summary

Version	Major feature	Value added
1	Signed messages announced to the network	Basis of entire system
2	Serial numbers	Uniquely identifiable transactions
3	The block chain	Shared record of transactions
4	Everyone verifies transactions	Increased security
5	Proof-of-work	Prevents double spending

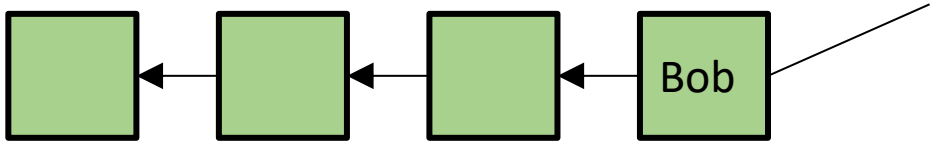
Nakamoto Consensus : The Longest Chain is the Valid Chain

- Honest nodes only work on the longest chain:



- Only transactions in the green nodes are validated by the network.
- Why longest?

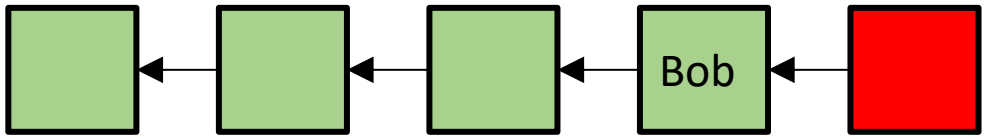
Prevent Double Spend Attack



Suppose Alice sent 1 BTC to Bob and the transaction is included in this block.

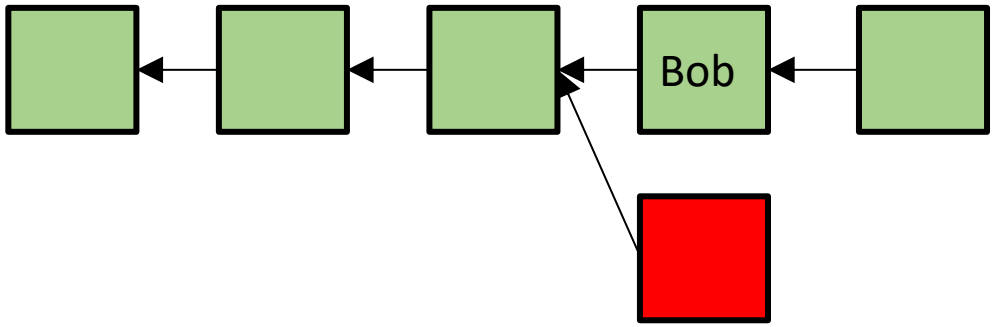
Now Alice wants to maliciously double-spend her the BTC.

Prevent Double Spend Attack



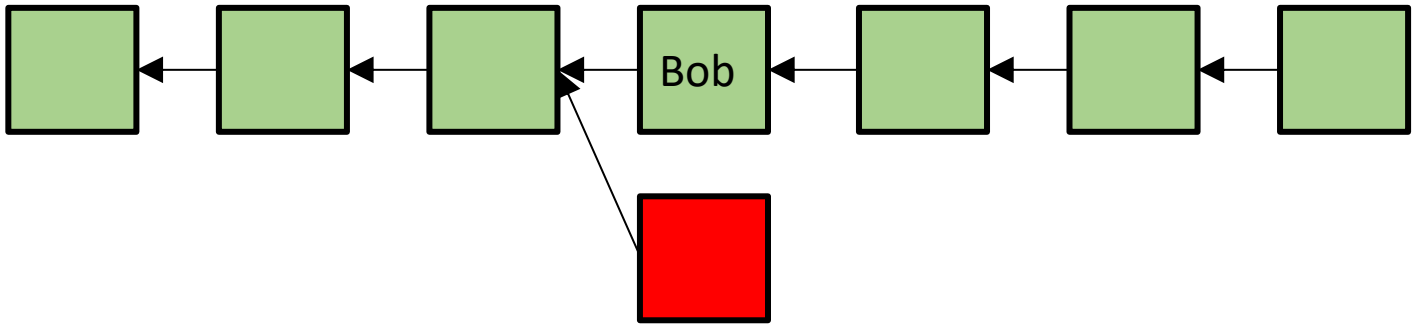
Because every node in the network validates transactions, Alice cannot simply append a conflict transaction.

Prevent Double Spend Attack



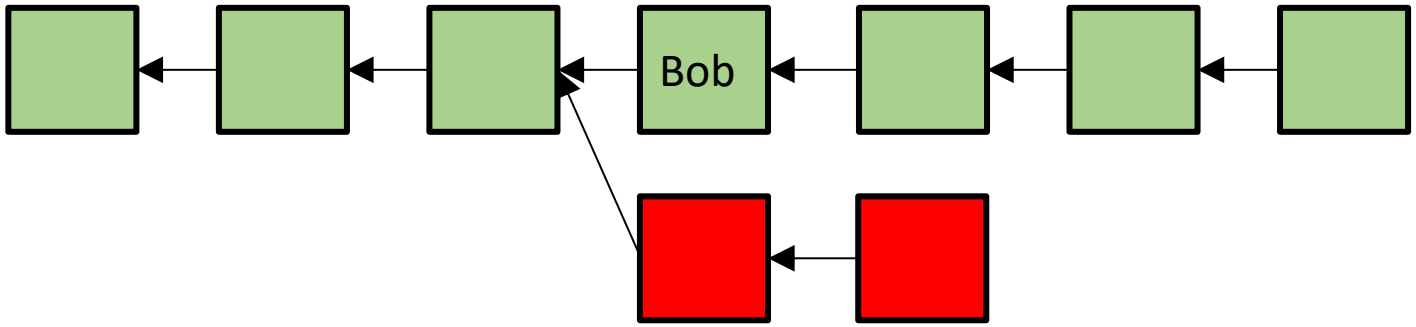
Alice has to fork the chain to revoke her previous transaction.

Prevent Double Spend Attack



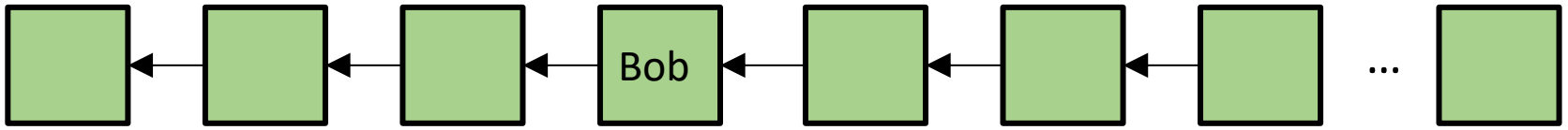
But in the mean time, honest nodes ignores this fork and working on the longest chain.

Prevent Double Spend Attack



Alice has **very low** probability to revoke the transaction to do double-spend unless she can beat the whole network on proof-of-work.

Prevent Double Spend Attack



Bob can wait for more blocks to appear on top of the block containing the transaction to make double-spending even harder!

Major Assumption

- More than 50% of computation power belongs to honest nodes
  - *One CPU one vote
- A malicious attacker who controls 51% of the computation power can perform arbitrary changes to the blockchain!
- Is this assumption practical?
- How to define “honest”?

Other Assumptions

- Block transmission between honest nodes are reasonably fast
  - Bitcoin limits each block to 1MB
- Block generation should be comparably slow
  - Bitcoin generates a block every 10 minutes
- What if those assumptions do not hold?

Forks in Nakamoto Consensus