BITCOIN FOR HACKERS

JOHN NEWBERY

@jfnewbery

github.com/jnewbery

ABOUT ME

Live in New York

Work at Chaincode Labs

Contribute to Bitcoin Core

github.com/jnewbery

WHAT IS BITCOIN?


$10 000


1000g
999.9
FINE GOLD

ONE HUNDRED 100 | 15 100 C | ONE HUNDRED 100 | THIS NOTE IS A LEGAL TENDER FOR ONE HUNDRED DOLLARS | ONE HUNDRED 100 | 15 100 C | ONE HUNDRED 100 | 15

Z27008X

SERIES OF 1880

THE UNITED STATES

Will Pay to Bearer SEP

ONE HUNDRED DOLLARS

WASHINGTON, D.C.

100

ACT OF MARCH 3, 1863

Z27008X

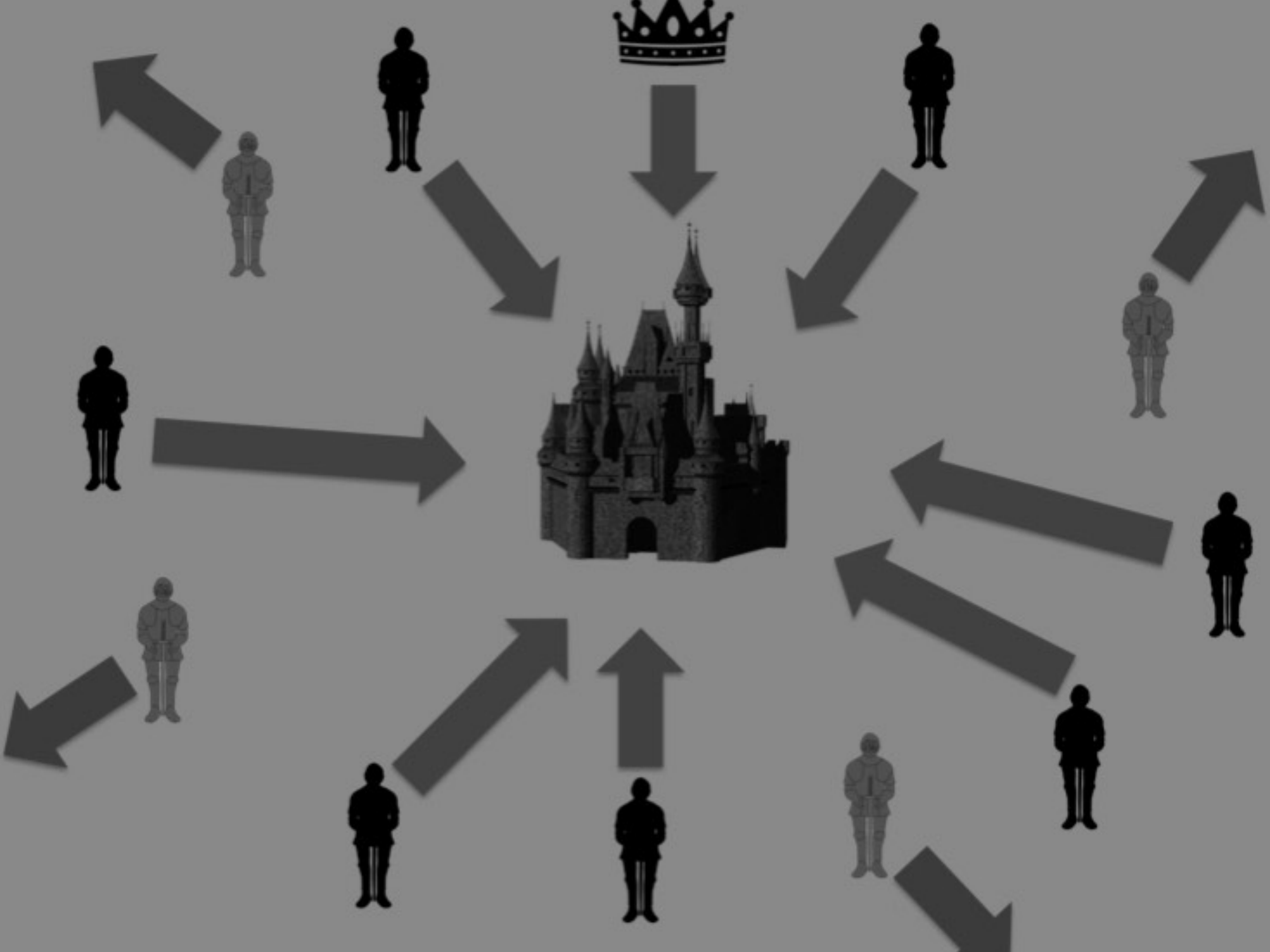
100

B. K. Bruce
Register of the Treasury

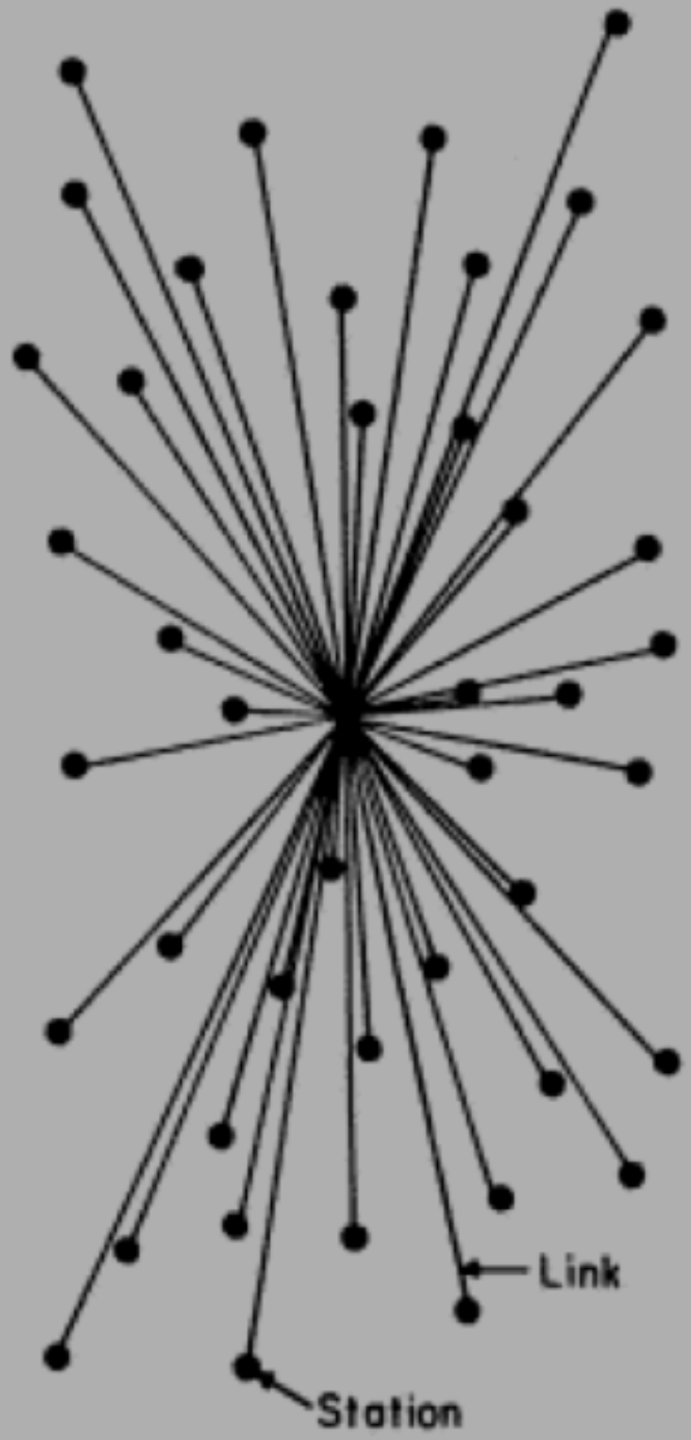
Jas. Gilfillan
Treasurer of the United States

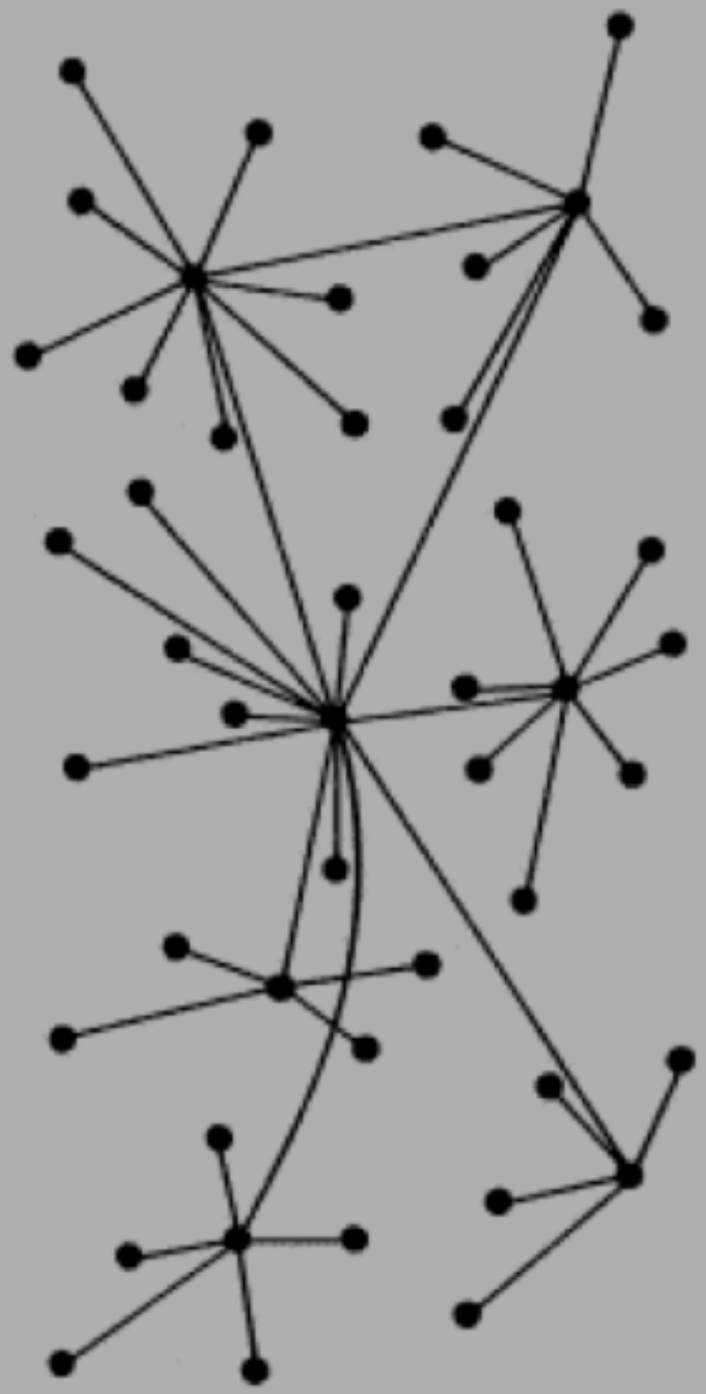
C ONE HUNDRED 100 | 15 100 | UNITED STATES NOTE | ONE HUNDRED 100 | 15 100 C

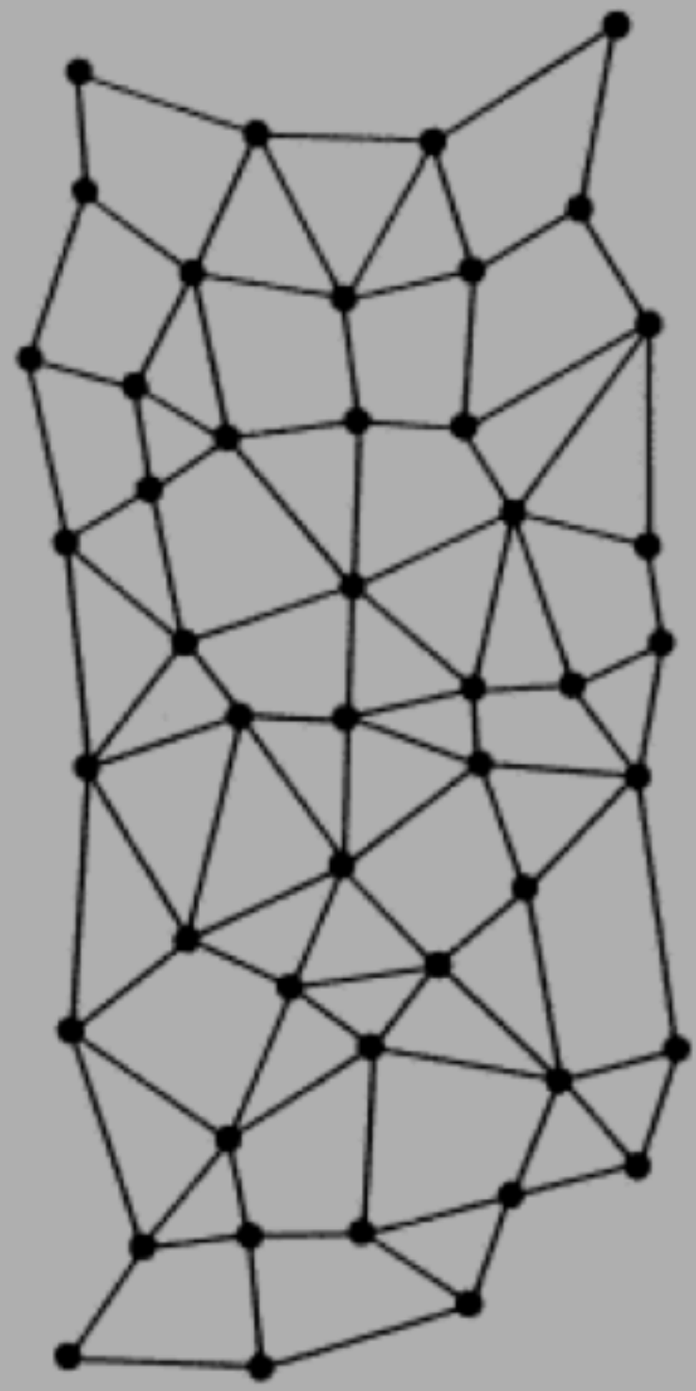

THE UNITED STATES OF AMERICA
50



	No.	Names	Total of Accts	Due to G	Due to M	Due to M & G	Due to M & is paid	M Dr to G	G Dr to M	How paid
	1	Ball Jno D	7.7.9	2.10.8	4.17.1	7.7.9				
X	1	Henderson Hugh	12.1.0	4.0.4	8.0.8	0.0.0	8.0.8			Paid each his part of ...
	3	Minor Joseph	4.7.6	1.9.2	2.15.4		2.18.4			
	5	Shirt Mrs	1.7.0	0.9.0	0.18.0					
	6	Hackley James	6.10.9	2.3.7	4.7.2	6.10.9				paid each his part
	7	Hamilton James	7.6.0	2.8.11	4.17.1		4.07.1			
	8	Thornton Geo	4.15.6	1.12.0	3.3.6			1.12.0		
	9	Barnet Parson	3.0.0	1.0.0	2.0.0				2.0.0	
	10	Willis Lewis	20.17.9	7.1.3	13.16.6					
	11	Throgmorton Thos	5.0.8	1.13.4	3.6.8	3.0.0		3.5.9		
	11	Battaile Lawrence	24.7.9	8.2.7	16.5.2			3.2.7		
	12	Tomlinson Commodore	2.1.3	0.13.9	1.7.6	2.7.3				
	12	Taliaferro Robt	3.11.3	1.5.1	2.10.2			1.5.1		
	13	Ellis Wm	0.5.0	0.2.6	0.2.6	0.5.0				
	15	Dangerfield Belvidere	15.17.9	5.18.11	9.18.10		9.18.10			
	15	Temple Saml Hanover	3.5.9	1.1.11	2.3.10			1.1.11		
	16	Fitzhugh Col Wm London	2.10.3	0.18.7½	1.11.7½		0.10.3	0.18.7½		
	16	Clarke Jno Caroline	0.13.6	0.4.6	0.9.0	0.13.6				
	16	Jones Capt	3.0.0	1.0.0	2.0.0			1.0.0		
	17	Tyrrel Richd	0.10.0	0.3.4	0.6.8			0.3.4		
	18	Gordon Jno	1.1.0	0.7.0	0.14.0				1.11.11	paid on [illegible]
	19	Baylor Col Jno	2.10.6	0.18.7	1.11.11		pr order	6 12.8.3	10.7.3	
	20	Seldon Saml	4.15.9	2.1.0½	2.14.8½			0.6.9		
	20	Bankhead Doctr	0.13.6	0.6.9	0.6.9		pr order	6 5.7.6	0.7.0	
	21	Dunkinson James	13.11.6	4.11.11	8.19.7					
+	22	Wheeler Jacob	10.17.3	3.14.3	7.3.0			0.2.5		
	22	Oliver Thos	1.4.0	0.8.5	0.15.7					
	22	Meriwether Saml	0.7.0	0.2.4	0.4.8	0.7.0	0.7.6			
•	24	Blanton W Capt	0.11.3	0.3.9	0.7.6				0.15.10	
	25	Farrel Austin	1.3.9	0.7.11	0.15.10					
	25	Buckner Elliot	2.11.0	0.17.6	1.13.6	2.11.0			3.3.10	
	26	Hunter James Junr	4.19.0	1.15.8	3.3.10					
	27	Farris - drawer at P Johnston	0.13.0	0.4.4	0.8.8	0.13.0				
	27	Walker apt. J Dunlop	0.12.6	0.4.2	0.8.4			0.4.2		
	28	Newton Capt Wm	0.15.0	0.5.0	0.10.0			0.5.0	0.3.4	
	28	Mullatto George	0.5.0	0.1.8	0.3.4		2.0.11			
	29	Allan James	3.1.4½	1.0.5½	2.0.11	3.0.9	paid by Mr James		Uncles Vol 179	
	29	Hunter Wm Early	3.4.9	1.1.7	2.3.2				2.6.2	
	30	Ball Burgess	3.9.3	1.3.1	2.6.2			0.11.8		
	31	Hennon Peter	1.15.0	0.11.8	1.3.4			0.19.6		
	31	Campbell Lancelot	2.18.6	0.19.6	1.19.0				0.13.4	
	31	Hewel in Galw.	1.0.0	0.6.8	0.13.4		2.0.0			
	33	Brooke Robt	8.16.9	2.19.8	5.16.1	0.8.0		2.1.2½		
	33	Gale at Mrs Thorntons	0.8.0	0.2.8	0.5.4					[illegible] 1/2
	34	Page Mann Esq Mannsfd	39.18.9	13.11.2½	26.7.6½		0.19.9		2.11.8	
	35	Jn. Hawkins	1.11.6	0.11.9	0.19.9					
	36	Allason Wm	9.13.9	3.4.7	6.9.2			0.6.9	1.13.0	
	37	Taylor James Orange	0.13.6	0.6.9	0.6.9		1.13.4		0.17.11½	
	37	Spotswood John	3.3.0	1.4.0	1.19.0		2.8.0	1.4.7	9.3.8	pd cash
	38	Taliaferro Francis Junr	3.19.4	1.8.0½	2.11.3½					
	38	Mannis James	2.14.9	1.4.7	1.10.2				4.0.4	
	40	Morton Mrs	23.9.0	7.16.4	15.12.8					
	41	Thornton Cuthbert Junr	20.14.6	7.6.8	13.7.10			0.3.8		
	42	Hill the Shipwright	6.3.3	2.2.11	4.0.4					
	42	Waller at Acquia	0.11.0	0.3.8	0.7.4	3.15.9	Dr Clements took his Bd		3.15.3½	
	43	Batley Mrs	3.15.9	1.9.2½	2.6.6½			0.4.3		
•	43	Hammond Doctr	7.10.7	3.15.3½	3.15.3½		0.5.0			
	45	Tyler Francis	0.12.9	0.2.3	0.7.6					
	45	Wilson	0.7.6	0.2.6	0.5.0			0.12.1½		
	46	Taylor George	1.2.3	0.12½	0.12.1½					
	46	Lewis Wm overs. Mr Page	2.5.0	0.15.0	1.10.0		2.5.0	0.10.[illegible]	[illegible]	2.6


Link
Station





. . . AND MORE!

WHAT I'M NOT GOING TO TALK ABOUT

- Money
- History
- Philosophy and culture
- Satoshi Nakamoto

WHAT I WILL TALK ABOUT – TECHNOLOGY

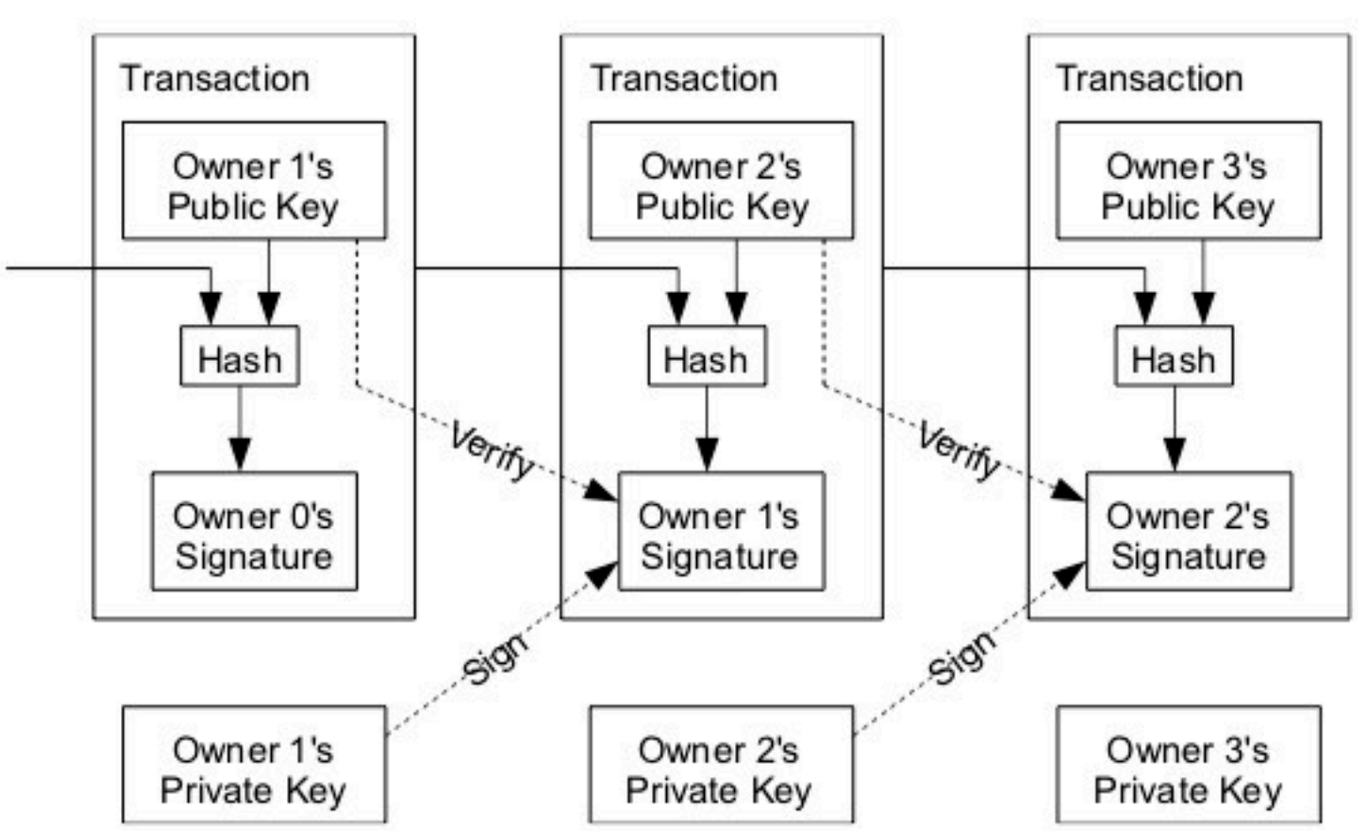
- Electronic coins
- The double spend problem
- Proof-of-work

ELECTRONIC COINS

ELECTRONIC COINS

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



“We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership…”

ELECTRONIC COINS

- Uses public key cryptography
- The spender signs a transaction with their *private key*
- **Anyone** can verify the transaction using the spender's *public key*
- The 'coin' changes ownership in a chain of transactions, extending back to when the coin was first created

THE DOUBLE SPEND PROBLEM

THE DOUBLE SPEND PROBLEM

- Bitcoin transactions are self-validating
- Everyone can verify that a Bitcoin transaction is valid
- Alice can send her coin to Bob by signing with her private key
- Alice can sign a second transaction paying Carol with *the same* unspent coin. That's also a valid transaction!
- This is called the 'double spend' problem

THE DOUBLE SPEND PROBLEM (PART 2)

- Alice can sign as many transactions as she wants
- If we don't agree on which coins have already been spent, there's no way to prevent double spends
- We need a way for everyone to agree which coins have already been spent
- We need to agree on the *ordering* of transactions

PROOF-OF-WORK

SOLVING THE DOUBLE SPEND PROBLEM

- Ordering transactions is easy in a centralized system: trust a third party to do it!
- Banks, credit card companies, PayPal, etc are third parties
- Nobody knew how to create a shared ledger without a trusted third party until…

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as

"...the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work..."

PROOF-OF-WORK

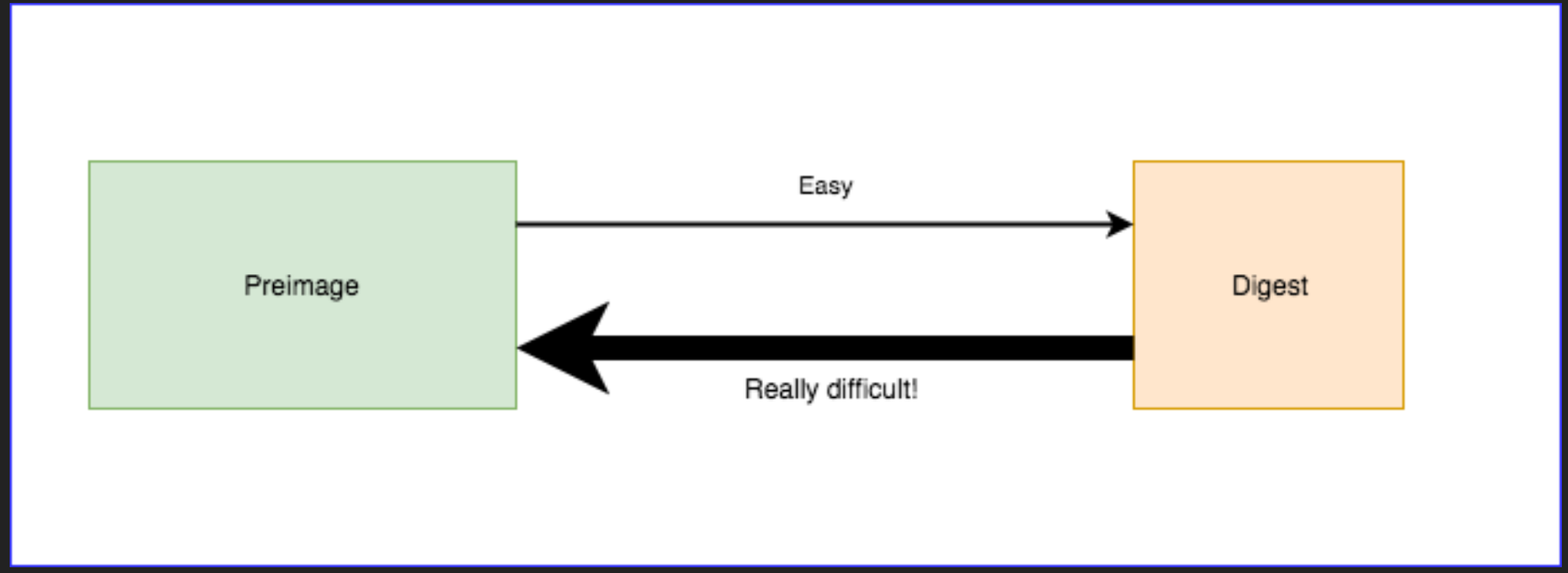
- Satoshi's solution to the double spend problem
- Based on Adam Back's *hashcash* and other earlier proof-of-work schemes
- Requires the miner to do computational work in order to *discover* a new block

CRYPTOGRAPHIC HASH FUNCTIONS

- A hash function is a function that takes an arbitrary-length input message and outputs a fixed-length *digest*
- A cryptographic hash function has additional properties:
  - it is infeasible to generate a message from its hash value (preimage resistance)
  - a small change to a message results in a completely different digest (avalanche effect)
  - it is infeasible to find two different messages with the same hash value (collision resistance)
- A cryptographic hash function is a one-way function. To an observer, the outputs of the hash function look like random numbers

CRYPTOGRAPHIC HASH FUNCTIONS

- A cryptographic hash function is a one-way function. To an observer, the outputs of the hash function look like random numbers



SHA 256

- SHA256 is a cryptographic hash function that maps inputs to 256 bit outputs
- Those outputs are essentially randomly distributed:
  - Half of all possible messages will hash to 0b0... and half of all possible messages will hash to 0b1...
  - One fourth of all messages will hash to 0b00...
  - One eighth of all messages will hash to 0b000...
  - ...
- In general, 1 out of 2^x messages will hash to a digest with x leading zeroes

PROOF-OF-WORK OVER A MESSAGE (1)

- To do proof-of-work *over* a message:

    1. Append some random bits to the end of the message. We call those bits a *nonce* (a **n**umber used **once**). For now, let's call <message|nonce> a *block*
    2. Hash the block using SHA256
    3. If the digest starts with the *target* number of zeroes, the block is valid. If not, the block is invalid - go to (1) and try with a different nonce

PROOF-OF-WORK OVER A MESSAGE (2)

- If the difficulty target is 4 zeroes, then *on average* we'll need to try 16 different nonces to find a valid block
- An observer only needs to do one hash to verify that the block is valid

BITCOIN MINING

- Bitcoin mining uses the exact same mechanism. Miners try lots of different nonces until they discover a valid block
- Miners do work over the Bitcoin block header
- The miner who discovers a valid block is allowed to update the global ledger with new transactions
- The current difficulty on the bitcoin network requires ~70 leading zeroes

MINING AND THE BLOCKCHAIN

- The block header includes the hash of the previous block
- The miner is doing work *over the entire chain*
- Mining is a race to extend the chain. When a miner discovers a block, he/she transmits it to the network and other miners start trying to build a block on top of it

QUESTIONS?

WHAT NEXT?

- Look at Jameson Lopp's Bitcoin resources page: http://lopp.net/bitcoin.html
- Read Jimmy Song's *A Gentle Introduction to Bitcoin Core Development*: https://bitcointechtalk.com/a-gentle-introduction-to-bitcoin-core-development-fdc95eaee6b8
- Contact me on IRC, twitter or github

THANK YOU!

@jfnewbery

github.com/jnewbery