CHALLENGES TO BITCOIN

L Jean Camp
www.ljean.com

I am Not Vint Cerf

Goals: Asking the Right Questions on Blockchain

- Foundational technologies
- Transactional characteristics
- Timing
- Anonymity & Privacy
- Bitcoin negatives

Why? Bitcoin is

- Distributed
- Publically readable
- Publically writable
- Anonymous
- Immutable
  - No recovery or rollback
- Mitigate network latency differences

Bitcoin is Not All Blockchain

- Distributed
- Publically readable
- Publically writable
- Anonymous
- Immutable
- Mitigate network latency differences

Bitcoin is Not Just Blockchain

- Distributed
- Publically readable
- Publically writable
- Anonymous
- Immutable
- Mitigate network latency differences

- Writable or …
  - Subset of stakeholders
  - Revocation
  - Pool of authorizing authorities
  - Only transaction participants
  - One authority

Bitcoin is Not Any Blockchain

- Distributed
- Publically readable
- Publically writable
- Anonymous
- Immutable
- Mitigate delay

- Anonymous or …
  - Identifiable
  - Subject to deanonymization
  - Identifiable by trusted party
  - Identifiable for conflict resolution

Bitcoin is Not Any Blockchain

- Distributed
- Publically readable
- Publically writable
- Anonymous
- Immutable
- Mitigate network delay

- Changeable or …
  - Fraud recovery
  - Revoke transactions with revocation of write
  - Legitimate forks

Bitcoin is Not Your Blockchain

- Distributed
- Publically readable
- Publically writable
- Anonymous
- Immutable
- Mitigate network latency differences

Your Blockchain

- What and who do you trust
  - Who writes, who reads, when and why
  - Who and when are they identified
  - Who can rollback
  - How do you calculate it
- Who does the work
  - Attacker or defender?

Foundations

Understanding components and history to design the appropriate structure

- Hashing this out
- Proof of work
- Cryptocurrencies Past

The Blockchain Core

- Is hashing functions
- Probability of creating a specific outcome from a given input via hashing

Two Things You Already Know

- Pigeonhole principle
  - If you have m pigeons and n containers, if m>n then there will be one more pigeon in one hole

Applies to All Sets

- Also applies to hash values
  - There will be some files that naturally have same hash
  - If you can create a file and change the file often enough then you have two pigeons in one hole
  - This is called a *hash collision*

Birthday Paradox

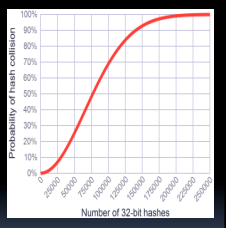
- If you want two people to have the same birthday if you want a 50% chance you need 23 people not 356

Pairs Not Individual People

- 2 people. 1 pair.
  - Possible combinations of birthdays 133225
  - Different 364 of 365 cases, or 99.726% of the time
  - The same 0.0027
- 3 people, 3 pairs
  - How likely is it that all three of there are different?
  - $1 - (364/365)^3 = .0082$
- 57 people. 1596 pairs.
  - Chances of 1596 unique pairs
  - $1 - (364/365)^{1596} = 98.75$

How Rare?

- Hash collisions are rare and unpredictable
  - 2^5 - 2^6 data points for collisions chance >95%
  - The odds of a collision are not the odds of finding the sought after collision
  - Two people with the same birthday is not the same of two people with the birthday of Feb 27



Proof of Work

- Proposed as cost-based anti-spam mechanism
  - Pay money to send each email
  - Have an account of virtual money
  - One way function
  - Collisions are difficult

What is Proof of Work?

- In 1992, the first Proof of Work was invented by Cynthia Dwork and Moni Naor.
- Email sender computes a compute some moderately hard, but not intractable, function thereby proving work.
  - POW using memory constraints means a factor four rather than tens of difference
  - Potential wide application.

C. Dwork and M. Naor, *Pricing via Processing or Combating Junk Mail*, 1992

Penny Black

- The Penny Black project was supported by Microsoft and proposed an explicit ticket server for each email sent
- Recipients contacted the ticker server to stamp the email

Example of Proof of Work

- Hash function
  - H(m) --> n
  - where n is a pre-determined size
  - where small changes in m result in indeterminate changes in n
    - a collision occurs when $H(m_0) = H(m_1)$, $m_0 =! m_1$

Different Types of PoW

- Wide range of processing speeds
- Spam-i-am first proposal for a managed distributed hash table
  - Uses email signatures associated with the quota
  - User creates stamps by signing
  - Each email received decrements quota

Select a Public Hash Value

- Hashcash produces a series of dated values, then publishes collisions
  - each email sender calculates a collision
  - sender tries multiple calculations $O(2^{n/c})$
  - recipient implements two calculations
    - Places in list, marking those received as expired
- Hash values were designed as per email, with a common public seed
  - recipient accepts one email per collision

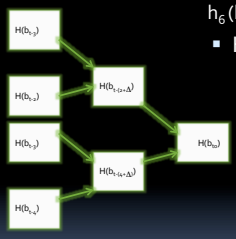
PayWord

- Essentially an aggregator
- User has an account with a key pair, payment, and email account
- Using that, the user commits to a vendor-specific hash chain

Merchant-Specific Hash Chains

- Create a chain
  - $h_6(h_5(h_4(h_3(h_2(h_1(h_0(\text{word})))))))$
  - Give vendor the end of the chain h_6
  - Keep going down the chain to pay more

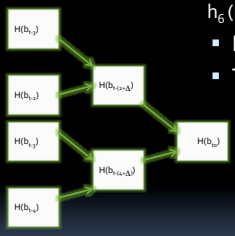
Hash Trees



$h_6(h_5(h_4(h_3(h_2(h_1(h_0(\text{block})))))))$

- Hash tree

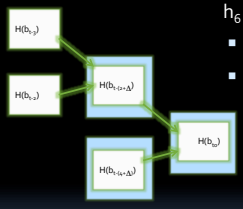
Hash Chains



$h_6(h_5(h_4(h_3(h_2(h_1(h_0(\text{block})))))))$

- Hash tree
- Time flows towards the root

Hash Chains



$h_6(h_5(h_4(h_3(h_2(h_1(h_0(\text{block})))))))$

- Hash tree
- Allows combinations and verifications where the existence of 0 proves it was calculated after the two previous inputs

Micro Mint

- Uses collisions as currency
- Centralized issuers
- Clear format of coin

So every string that include 000111 and such that $h(s_4)=h(s_3)=h(s_2)=h(s_1)=h(s_0)=\text{coin}$

Expansion & Magnitudes

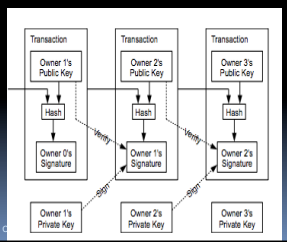
- Micro Mint handled expansion and magnitudes by *forms of the coins*
  - 000111 is worth a fraction of 0000111
  - Fraction could be determined by work factor
  - There is centralized agreement in MicroMint

Construction a Bit of Coin

- Bitcoin is built upon well known foundations
- What is the protocol
- What are the resulting challenges

Bitcoin

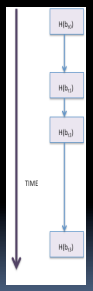
- A bitcoin wallet is ideally a functional, useable public key signing mechanism
- In practice a simple interaction to a stored account with no signatures



Solve Double Spending

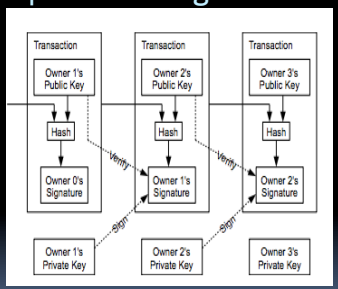
- Announce first spend
- Use a hash chain for time stamping

Series of Transactions

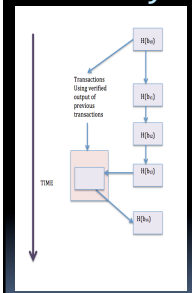


- Announce your transaction
- Input is the same as output value
- Then the miners race to add to the distributed hash chain

A Simple Exchange

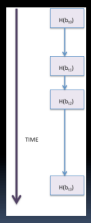


Verify to Create Money



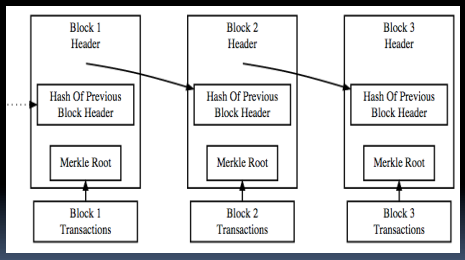
- When the miner creates the hash
- Which includes the miners own key
- Then that miner augments the hash chain

This Is a Blockchain, Not Bitcoin



- It is a *linked list* with hashed values
- It is also tamper evident
- If you sign it with a public key it becomes what is commonly called blockchain because PKI and inclusion of hashed previous result

Use the Nonce, for Freshness!



Contents of a Block

Field	Function
Version	Defines acceptable format of the coin, the rest of the message, and the protocol used when creating the transaction
In counter	A counter
Inputs	Amount and source of money
List of inputs	The first input is the money created by mining the hash to create the block. It is the nonce. So there are multiple transactions.
Outputs	The amount is the same as the input. This usually means multiple outputs.
Out counter	A counter
List of output	The transaction fee which is created by the miner who calculated the PoW to validate the block
Time stamp	When the block is approved, not the transaction

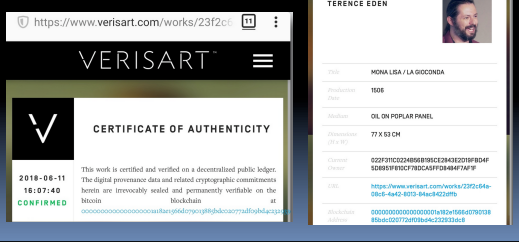
Scope

- Each bitcoin is associated with a public key
- Each public key is associated with a wallet
- Wallets may be associated with devices, addresses, or unique identifiers

The Limits and Risks

Encryption is not Validation

- Encrypting data does not make it correct
- Does not solve trust issues



Some Transactions Basics

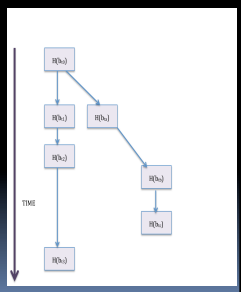
- Ideally transactions are ACID
  - Atomic
  - Consistent
  - Isolated
  - Durable

Atomic

- Transactions succeed completely
- Fail completely
- Each block has multiple components
- One may become an orphan block

Orphan Blocks

- There is essentially a raffle or lottery where it is not possible to determine the validity or underlying block
- Alice pays Bob
- Alice pays Alice
- Alice adds $H(b_{ta})$
- Bob tries to add $H(b_{t1})$

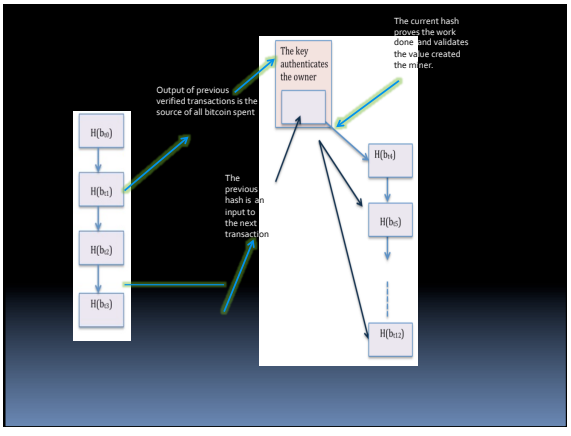


Consistent

- Publicly consistency is the strength of a blockchain approach
- Allows for dating, ordering, and consistent agreement; for example, for tracking
- Underlying requirements
  - trustworthy public key distribution
  - trustworthy data sources
  - if you have these is blockchain the right approach
    - Lacks write controls, so private blockchains

Isolated

- Lack of isolation is a fundamental design characteristic
- Being unable to disentagle components was a design goal
- Participation requires agreement with previous transaction



Lack of Isolation

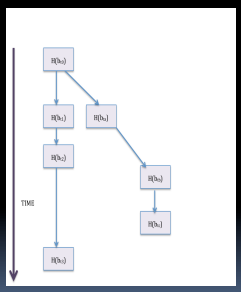
- Stolen assets used to generate wealth
- Conflating legitimate and illegal transactions
- Extreme lack of clarity about legal ownership

Anderson, Ross, Ilia Shumailov, and Mansoor Ahmed. "Making Bitcoin Legal." In Security Protocols Workshop. 2018.
Reed, C., Sathyanarayan, U.M., Ruan, S. and Collins, J., 2018. Beyond BitCoin: legal impurities and off-chain assets. *International Journal of Law and Information Technology*, 26(2), pp.160-182.

Durable After a Given Time

- Transaction blocks are created
  - Added to the hash tree
  - Then only after a number of blocks is the transaction reliable
- The design goal is every ten minutes
- Eventual agreement
- Probab(ilistical)ly

Conflict Can Emerge



- When two miners are very close and have different solutions
- Hash chains can diverge
- Usually the longest wins

A Mess of Race Conditions

- Transaction blocks are created
- Added to the hash tree
- Then only after a number of blocks is the transaction reliable
- The design goal is every ten minutes

Transactions Basic

- Ideally transactions are ACID
- Atomic X
- Consistent √
- Isolated X
- Durable X√

Anonymous

- Pseudonymous
  With due care
- 95% of transaction generators can be uniquely identified

Bitcoin Anonymity IP

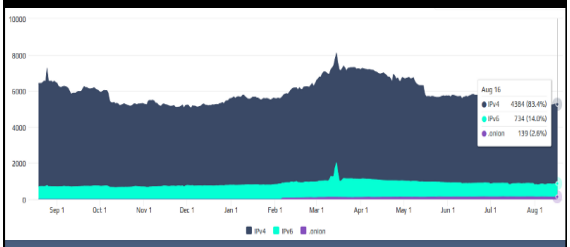
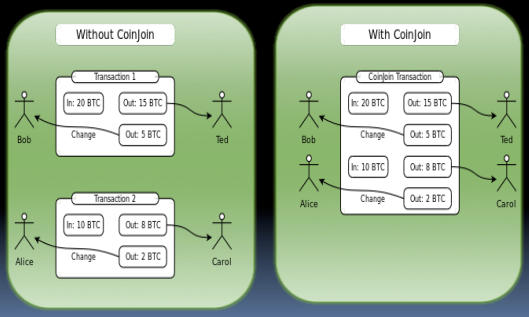


Image from https://medium.com/@lopp/how-to-run-bitcoin-as-a-tor-hidden-service-on-ubuntu-cff52d543756

Bitcoin Anonymity CoinJoin



Data Are Not Private

- Blockchain is a broadcast of hashed content
- Hashes do not provide eternal secrecy
- Each block contains additional transaction information
- Assume it will be made public
- Private content should not be placed on the blockchain
  - votes
  - medical records
  - confidential exchanged

Distributed?

- The party with the most processing power wins
- The party who included the previous block losses all their investment in the computational power
- Once that party wins they obtain the funds
  - Strong positive feedback
- In economics the result for this is, in the long term, is high levels of concentration

Speculation

- Volatility is normally a bug
  - Unless you can control it and make money
- The prices can be manipulated by strategic transactions
- Possible because most transactions are in private exchanges not on the blockchain

Price Manipulation

Markus & Wiley on Mt Gox
Vastly increased market value
Then stole all the bitcoins

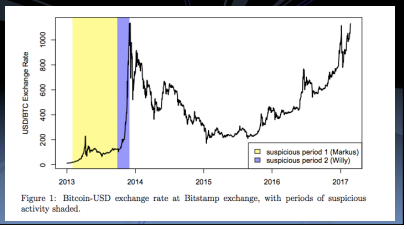


Figure 1: Bitcoin-USD exchange rate at Bitstamp exchange, with periods of suspicious activity shaded.

It Is Public

- Voting is announcing votes
- Announce internal transactions
- Place public health records on block chain because it is encrypted…
  - One Bad Prime

It is Not Agile

- The data are public
- Historical agreement is critical
- Integrity depends on past transactions

- A mathematical breakthrough could easily result in immediate diffusion of inconsistent historical records.

Crypto Isn't Diamonds

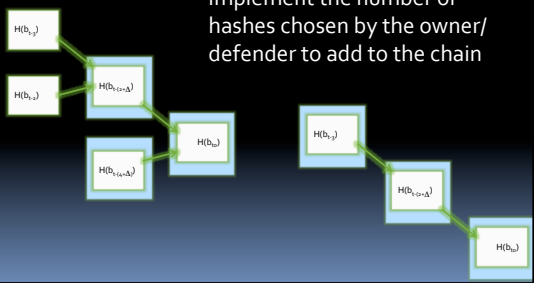
- 2018
- 2017 GnPGP RSA 1024
  - Code failure
- 2016 Factoring as a service, up to RSA 512
- 2012 Heniger broke 0.5% of RSA TLS/SSL private keys on internet from bad prng

This is Not Unreasonable

- Updating hash functions and public key signatures is sometimes needed
  - MD5 -> SHA1
  - SHA1 -> SHA128
  - RSA512 -> RSA 2048
  - DH -> DHEC
- Centralized ownership means it is possible to have an authoritative update

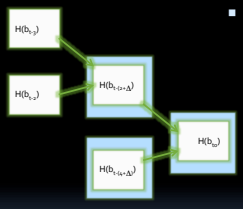
With A Hashed Chain or Tree

- The attacker has to implement the number of hashes chosen by the owner/ defender to add to the chain

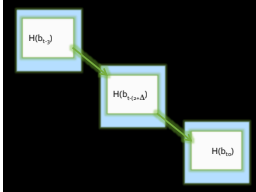


With A Predetermined Output

- The defender has to implement the number of hashes chosen by the design to add to the chain



With Public Blockchain



- The work required and if a block is acceptable are beyond your control
- There is motivation to increase the work and to speculate

Other Bitcoin Observations

- Carbon
- Crime
- Corruption

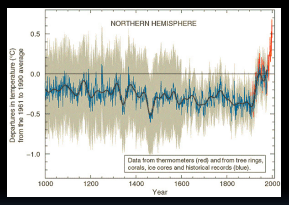
Tobin Tax?

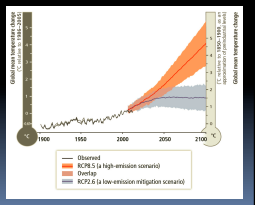
- Proof that Tobin Tax works

  Stockholm Prize in Economic Sciences Laureate economist James Tobin a tax on all spot conversions of one currency into another. It was originally intended to reduce speculation and increase the cost of short-term financial investments across currencies.

- Unfortunately it goes to the person who generates the most carbon in an speculative currency in a moment of global climate change

Carbon

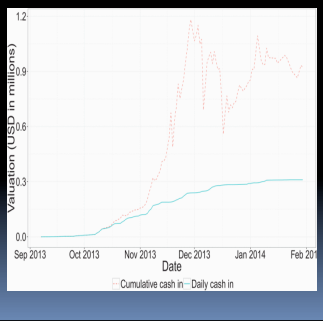




Role in the eCrime Ecosystem

- Beyond theft of bitcoin
  - Ransomware
  - Stealth bitcoin miners

Ransomware Early Innovator



Origins of Ransomware

- Launch malware
  - Free downloads
  - Purchase black market
  - DIY

STONE-GROSS, B., ABMAN, R., KEMMERER, R. A., KRUEGEL, C., STEIGERWALD, D. G., ANDVIGNA, G. The Underground Economy of Fake Antivirus Software. In Proceedings of the Workshop on the Economics of Information Security and Privacy(2013)

COVA, M., LEITA, C., THONNARD, O., KEROMYTIS, A. D.,ANDDACIER, M.An Analysis of Rogue AV Campaigns. In Proceedings of the International Conference on Recent Advances in Intrusion Detection(2010), pp. 442–463

Ransomware Contributor

- Shifts the production or cost curve for obtaining payment for ransomware
  - Cost of production
  - Difficulty of removal for home users
  - More targets capable of payment

Quality Measures

- Encryption strength
  - Weaker roll your own
    - Some reverse engineering
    - No cryptographic library calls
  - Size of target space
    - Harder to detect by observing processes

Functionality

- Scope
  - 61.2% only target the desktop
  - 5.4% encrypt all the files
  - 35.6% delete the files without encryption
- Encryption style
  - Windows API calls
  - Weaker version

Key Management

- Key on device
  - Similar to early DRM
- Then remote server key generation

Early Adopters in Malware

Table 5: Summary of types of charges in 15 ransomware families.

Families	Type of Charge			
	Premium Number	Untraceable Payments	Online Shopping	Bitcoin Transactions
Reveton		✓	✓	
Cryptolocker		✓		✓
CryptoWall				✓
Tobfy		✓		
Sefnit	✓			
Winlock				
Lektrom	✓			
Calelk	✓			
Urausy		✓	✓	
Krotten		✓		
BlueScreen		✓		
kovter		✓	✓	
Filecoder		✓		
GPcode		✓		
Weelsof		✓		
Number of Samples	132 (9.71%)	1,199 (88.22%)	14(1.03%)	28 (2.86%)
Number of Variants	18 (19.35%)	75 (80.64%)	4 (4.30%)	4 (4.3%)

Currency Types

- Direct payment
  - Bitcoin
- Purchase that requires a PSP
  - Software purchase
- Purchases that require resale or use
  - Gift cards

Future of Malware

- A wider range of products
  - IoT
    - Automobiles a major target
  - Mobile devices not likely targeted
    - Difficult to pay with no phone
    - Payment platform

Goals

- Foundations
- A transaction
- Risks

Blockchain Provides

- A public commitment that a key holder has committed to a give statement
- In a cryptographically immutable fashion
  - At a window in time
  - After some time
  - And for some duration
  - At a variable processing cost

Know your threat model

Know your trust model