Blockchain: The Good, The Bad and The Ugly

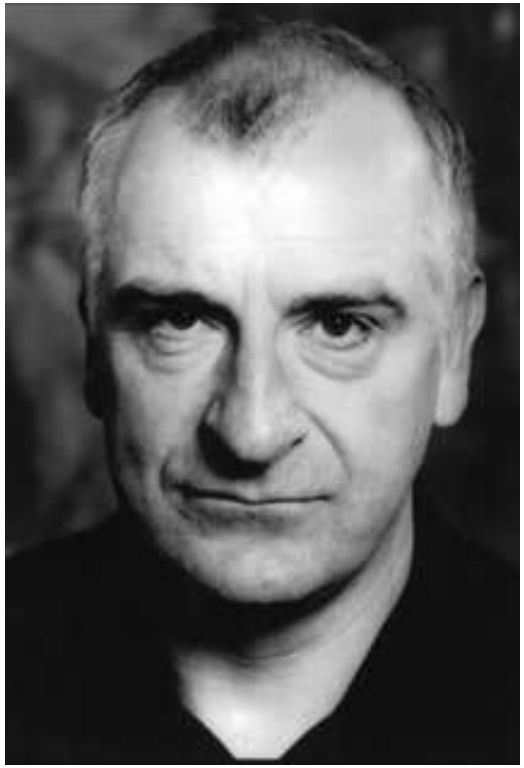
R. R. Brooks – rrb@acm.org
Clemson University, Electrical and Computer Engineering

July, 2019

Blockchain: Good, Bad, Ugly

- Blockchain provides a distributed ledger.
- Rush to exploit the technology, lead to exaggerated claims.
- Exaggerated claims, lead to backlash.
- Let's explore.

A Propos Money



- "This planet has - or rather had - a problem, which was this: most of the people living on it were unhappy for pretty much of the time. Many solutions were suggested for this problem, but most of these were largely concerned with the movement of small green pieces of paper, which was odd because on the whole it wasn't the small green pieces of paper that were unhappy." - Douglas Adams *H2G2*

Yapese currency

- Yap island in Pacific uses limestone blocks as currency.
- No limestone on Yap. Imported from other islands by canoe.
- Rare and valuable. Almost impossible to move.
- Currency ownership established by oral tradition.
- Public ledger of ownership and transactions.

What is Money?

- ☐ 100,000,000,000,000 Zimbabwe Dollars = USD 0.40
- ☐ Money is a widely accepted medium of exchange.
- ☐ Must be a limited supply.
- ☐ Should be hard to counterfeit.
- ☐ Danger of hyper-inflation and deflation.
- ☐ Money supply regulated by a central bank.
- ☐ International exchanges regulated by IMF.

First virtual currencies

- ☐ Online currencies start with trusted intermediary.
- ☐ Credit card companies, eBay, PayPal, E-Gold, etc.
- ☐ Needed for on-line transactions.
- ☐ Risks taken by middle man, in exchange for fees.
- ☐ Some markets use escrow accounts.
- ☐ Lawyers are the real computer and network security mechanism.

Video game currencies

- ☐ Video games create complex worlds with complex societies.
- ☐ Hire economist to avoid hyperinflation and chaos in markets.
- ☐ Some games have hard and soft currencies.
- ☐ Funds go in and out of games.
- ☐ Sometimes used for money laundering.
- ☐ Gold farming and Chinese prison.
- ☐ Wuffie and reputation.

Virtual currency summary

- Banking system and wire transfers changed money from physical tokens to information.
- On-line commerce originates with trusted third parties.
  - Credit cards, PayPal, etc.
  - Escrow accounts.
- Game currencies have actual value.
- Currency moving further from national to market control.
- Virtual worlds hire economists to act as central bankers.

First block chain

NOTICES & LOST AND FOUND
(5100-5102)

Universal Registry Entries:
Zone 2 - FVXiWDLVTk4sIPkIUIUKgHb
T0k0ezPp+x3/X+hWwWSiL1g+r1sL
D9oe5G6xKHxB23UwjIA==
Zone 3 - iFrVod8hv6Ep8W4ACkVZRCD
5ELvhLWXr1uB1PfjR2sxv
1WQpsxv4ci57nTZ38B+O82IRXA==
These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 20160316Z - 20160322Z.
www.surety.com 239-436-2790

- ☐ 1991 – "How to timestamp a digital document"
- ☐ Haber and Stornetta
- ☐ Hash a set of documents
- ☐ Publish the hash in the NY Times classifieds each week
- ☐ Proof that the set of documents was gehtered that week
- ☐ Basic concept of blockchain before widespread Internet use

https://www.anf.es/pdf/Haber_Stornetta.pdf

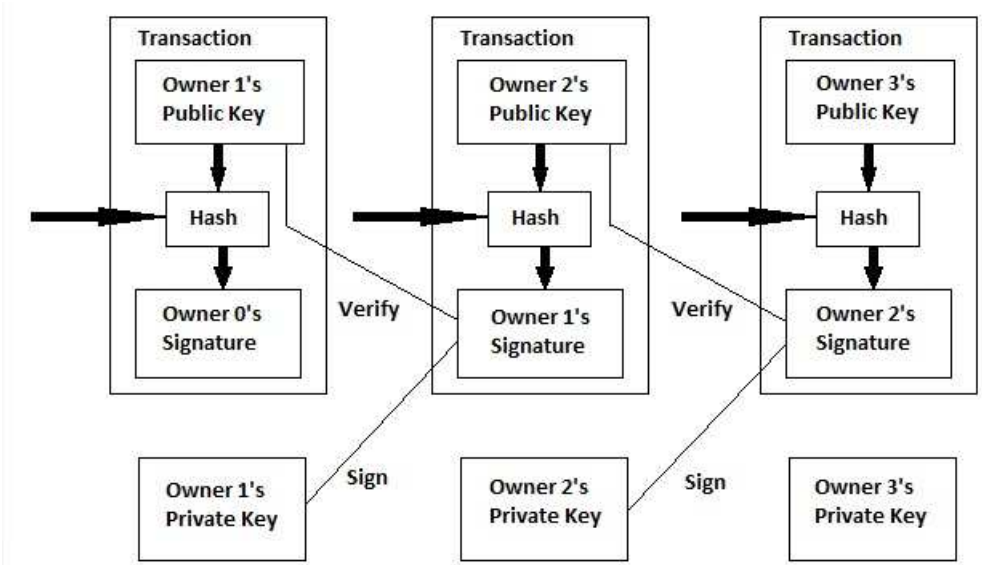
Origin story

- May 2007 – "Satoshi Nakamoto" started coding Bitcoin.
- August 2008 – bitcoin.org registered.
- December 2010 – Satoshi stops talking to people.
- "He" is a billionaire. He is anonymous.
- "He" may be male, female, or a team.
- Built on b-money, Bitgold, HashCash and other proposals.
- Solved many important problems to create first real crypto-currency.
- Only Newsweek believes the person in the picture is Satoshi,

Byzantine Generals Problem

- ☐ Posed by Lamport.
- ☐ Known solutions exist. Including my dissertation.
- ☐ Distributed data base on multiple nodes.
- ☐ Transaction verification by winner of competition.
- ☐ No centralized point of control.
- ☐ Hack has to change multiple nodes in real-time.

Blockchain



- ☐ Each transaction signed by spending party.
- ☐ Transactions put into blocks by 3rd party "miner".
- ☐ Hash of previous block becomes part of next block.
- ☐ Hash is random mapping of inputs to fixed number of bits.
- ☐ Next block signed by another "miner".
- ☐ Public key signing is encryption of hash using (secret) private key.
- ☐ Signature easily verified using (publicly available) public key.
- ☐ Hack has to compromise all nodes to change distributed database in real-time.

Mining

- ☐ Mining verifies transactions and stops inflation.
- ☐ Miners receive and verify transactions.
- ☐ Miners compute hash of block with random value appended.
- ☐ Proof of work – Hash has to start with n zeros.
- ☐ Proof of work requires trying random values for hash.
- ☐ Miner that solves problem gets new BTC and transaction fees.
- ☐ Stop inflation – n varies to create 1 block per 10 minutes.
- ☐ Energy for 1 block could heat house for week.

Why/How it works

- Hash chain (Merkle Tree) patented in 1979.
  - Hashes prove earlier entries not changed.
  - Public key signed hashes certify hash done by person with secret key.
- Interleaved signatures make forgery very difficult.
- Interleaving signatures of competitors makes forgery almost impossible.
- Permissioned/Permissionless controversy.
- Mining approaches: Proof of Work, Proof of Stake, Lightweight mining, proof of burn, proof of elapsed time, proof of authority,proof of capacity, proof of activity, delegated proof of stake, proof of importance, proof of identity, etc.

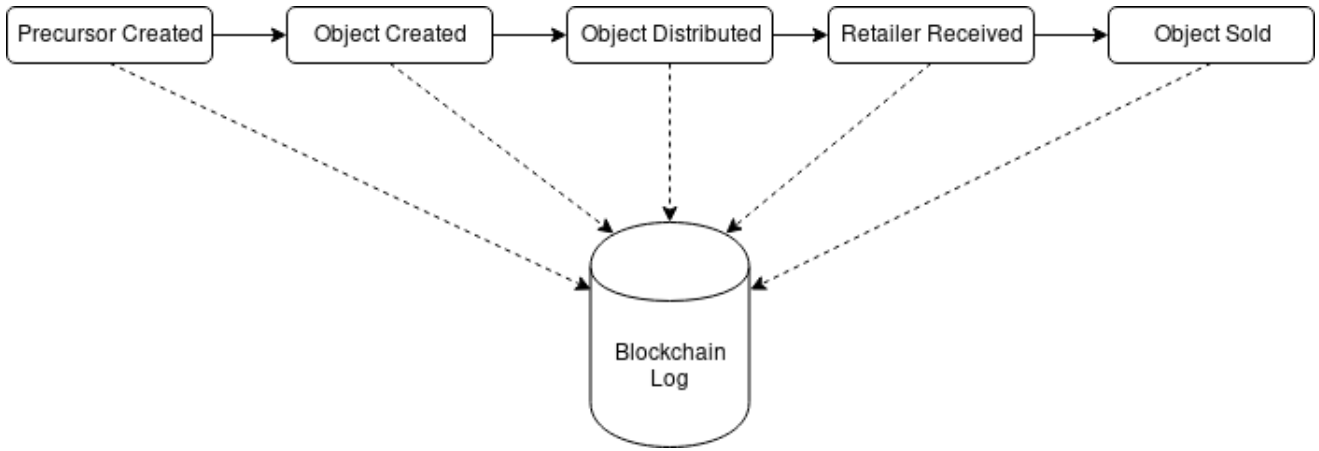
BTC summary

- ☐ Working system.
- ☐ Public ledger does not allow double spending.
- ☐ Transactions independently verified by miners.
- ☐ Blockchain universally stored in cloud.
- ☐ Malicious modification effectively impossible.
- ☐ Value maintained by limited number of BTC.

Application: Domain Name Service

- Namecoin
  - DNS system on its own independent blockchain, similar to Bitcoin
  - Has its own currency.
  - Allows key-value associations between a .bit address and machine-readable data.
  - Merged mining - shares mining power with Bitcoin
- Ethereum Name Service (ENS)
  - DNS system built in Ethereum smart contracts
  - Has no associated currency.
  - Automatic auctioning of names to register a .eth address.

Application: Supply Chains



- Hyperledger Fabric - Used for supply chain management
  - Each step in the supply chain records their data.
  - The mining process is only subverted if different steps in the chain cooperate.
  - Since the blockchain is practically immutable, the data's integrity is assured.
  - Walmart has begun using Hyperledger for its food supply chains.

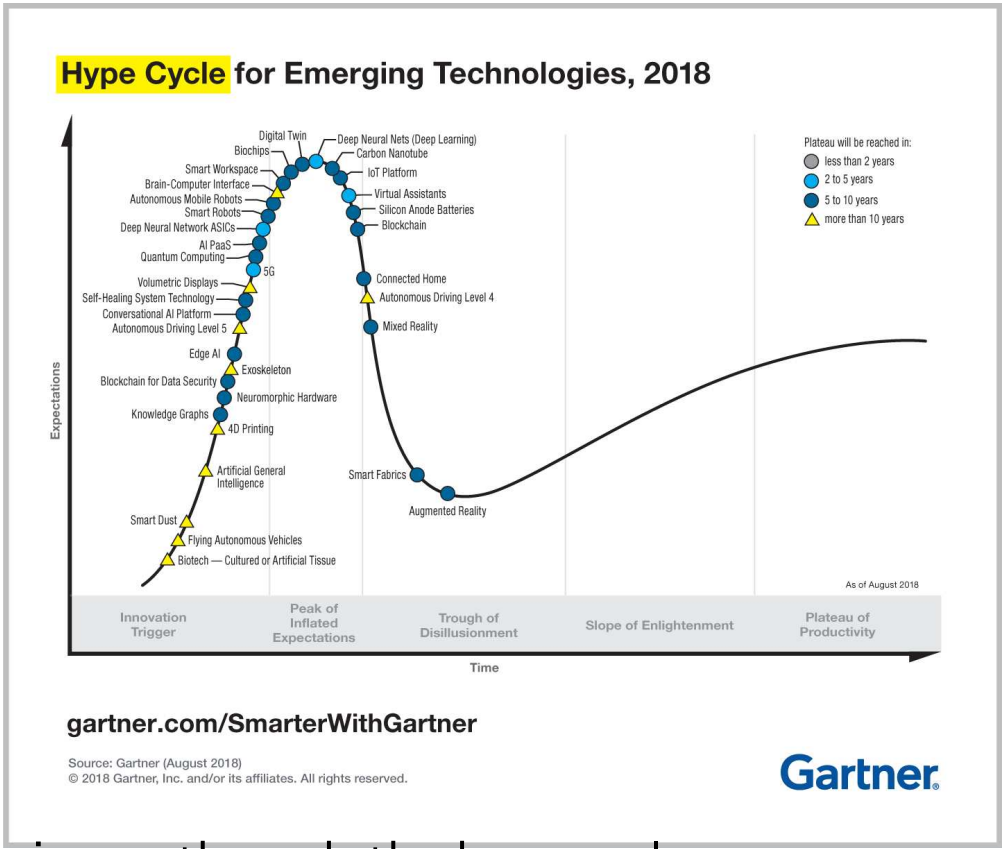
Application: Fun!

- CryptoKitties
  - Game built in Ethereum smart contracts
  - Trade and breed cute animals
  - In 2017 a CryptoKitty sold for $100,000
- Blockchains allow for more persistent game economies where assets have value beyond the creator's control.

Blockchain

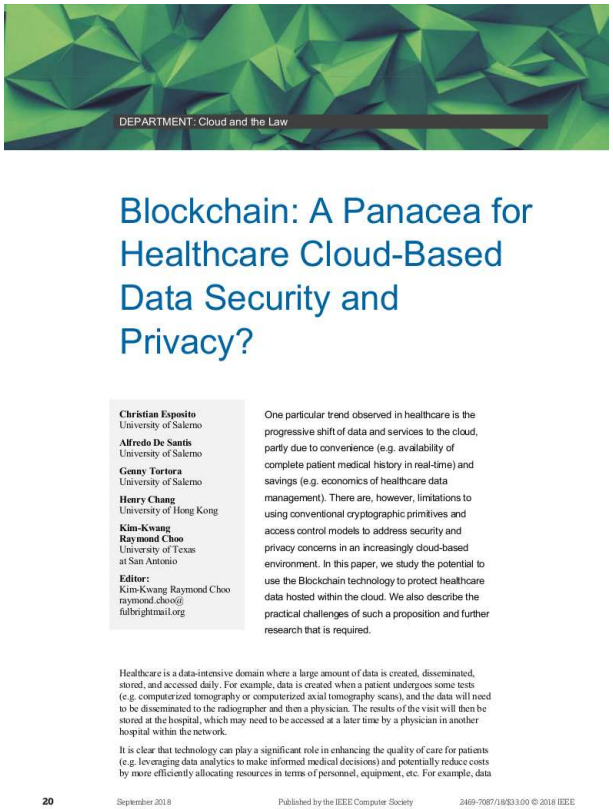
- Provides a ledger of authenticated information;
- Impractical to modify past entries;
- Some temporal ordering in data structure;
- Currency application best-known, might not be best use.

Gartner hype cycle



- ☐ Technologies go through the hype cycle;
- ☐ Blockchain is “hot”;
- ☐ Unreasonable claims being made;
- ☐ Over-inflated expectations and inappropriate applications;
- ☐ Backlash is starting.

Blockchain health records



DEPARTMENT: Cloud and the Law

Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?

Christian Esposito
University of Salerno

Alfredo De Santis
University of Salerno

Genny Tortora
University of Salerno

Henry Chang
University of Hong Kong

Kim-Kwang Raymond Choo
University of Texas at San Antonio

Editor:
Kim-Kwang Raymond Choo
raymond.choo@fulbrightmail.org

One particular trend observed in healthcare is the progressive shift of data and services to the cloud, partly due to convenience (e.g. availability of complete patient medical history in real-time) and savings (e.g. economics of healthcare data management). There are, however, limitations to using conventional cryptographic primitives and access control models to address security and privacy concerns in an increasingly cloud-based environment. In this paper, we study the potential to use the Blockchain technology to protect healthcare data hosted within the cloud. We also describe the practical challenges of such a proposition and further research that is required.

Healthcare is a data-intensive domain where a large amount of data is created, disseminated, stored, and accessed daily. For example, data is created when a patient undergoes some tests (e.g. computerized tomography or computerized axial tomography scans), and the data will need to be disseminated to the radiographer and then a physician. The results of the visit will then be stored at the hospital, which may need to be accessed at a later time by a physician in another hospital within the network.

It is clear that technology can play a significant role in enhancing the quality of care for patients (e.g. leveraging data analytics to make informed medical decisions) and potentially reduce costs by more efficiently allocating resources in terms of personnel, equipment, etc. For example, data

- ☐ Store health records on blockchain to allow global access;
- ☐ Access authorization TBD;
- ☐ Data updates TBD.

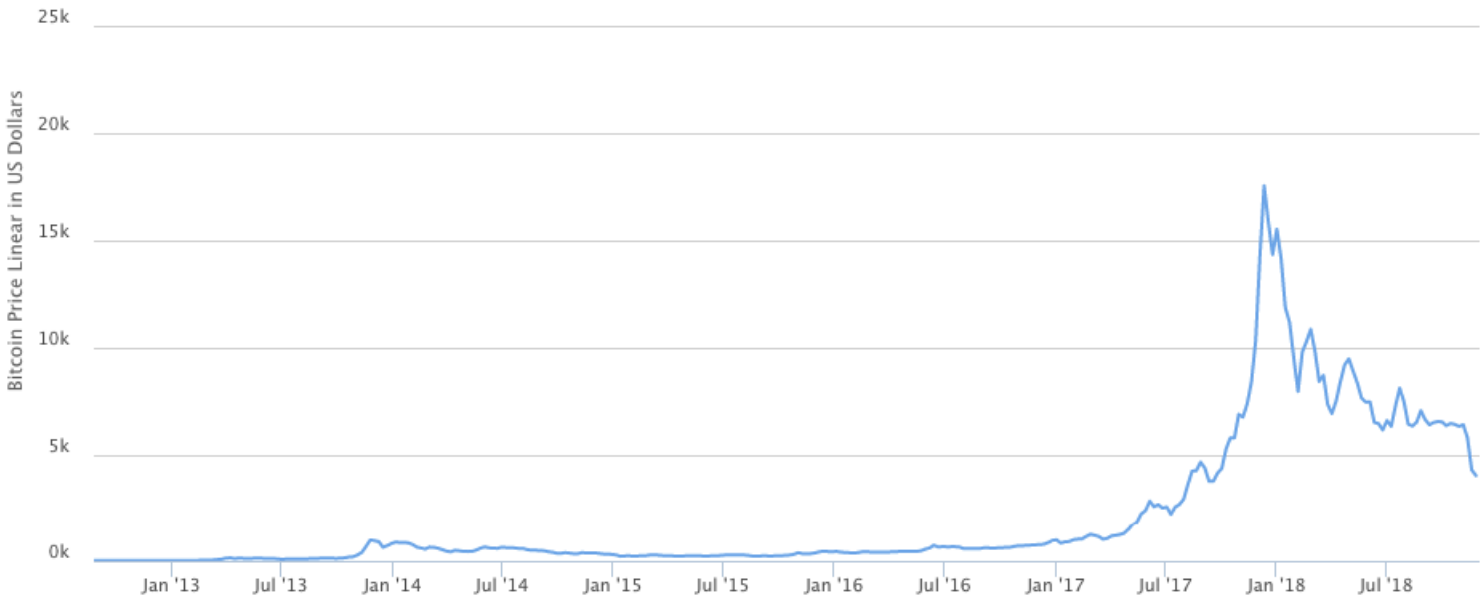
Clinical trial data

- Pharma representatives:
  - "Security and privacy of blockchain assured."
  - "Participants more willing to share data"
  - "Easy to find study participants with specific profile."
- "We will email them directly about participating in new trials."

Overheard in business meetings

- "Blockchain makes your data universally accessible."
- Most businesses do not want that.
- "Blockchain makes your data reliable."
- Verification makes your data reliable.
- Signing the data entries can make your employees accountable, though.

Cryptocurrency investments

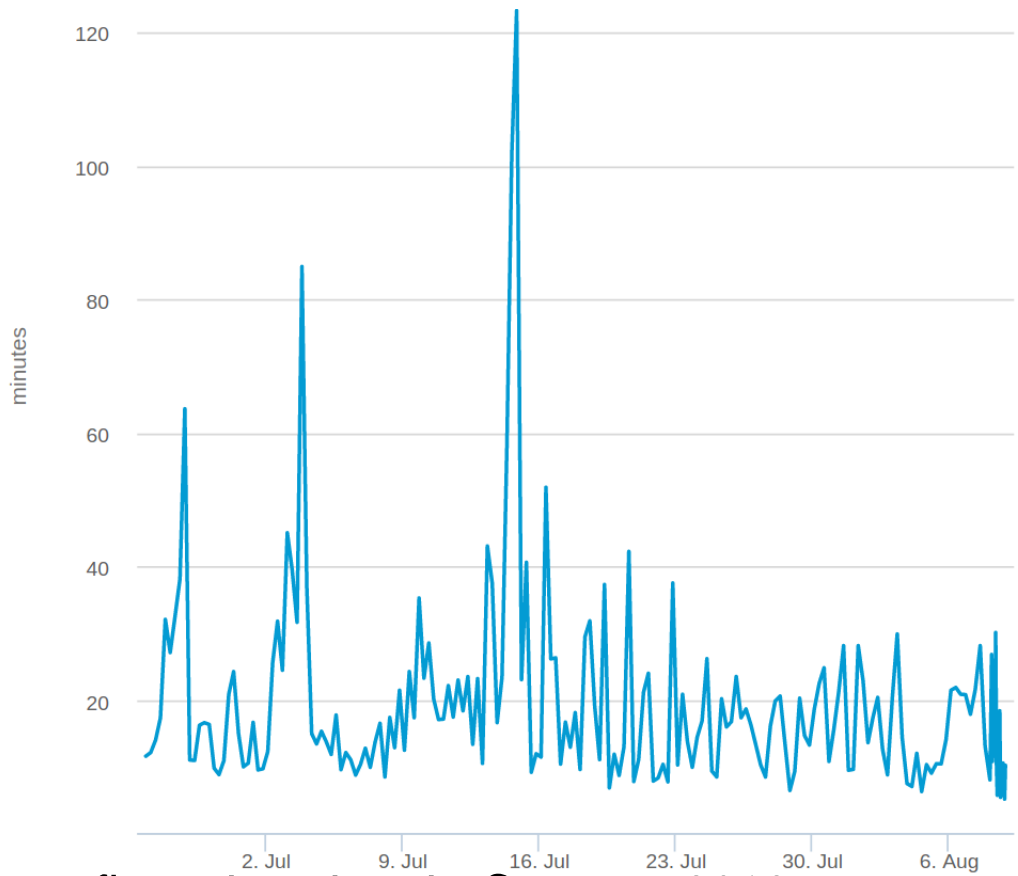


- ☐ BTC design sets limit on max number of BTC.
- ☐ No central bank.
- ☐ No regulation of value over time.
- ☐ To date, speculation makes the price unstable.

Low cost transaction medium

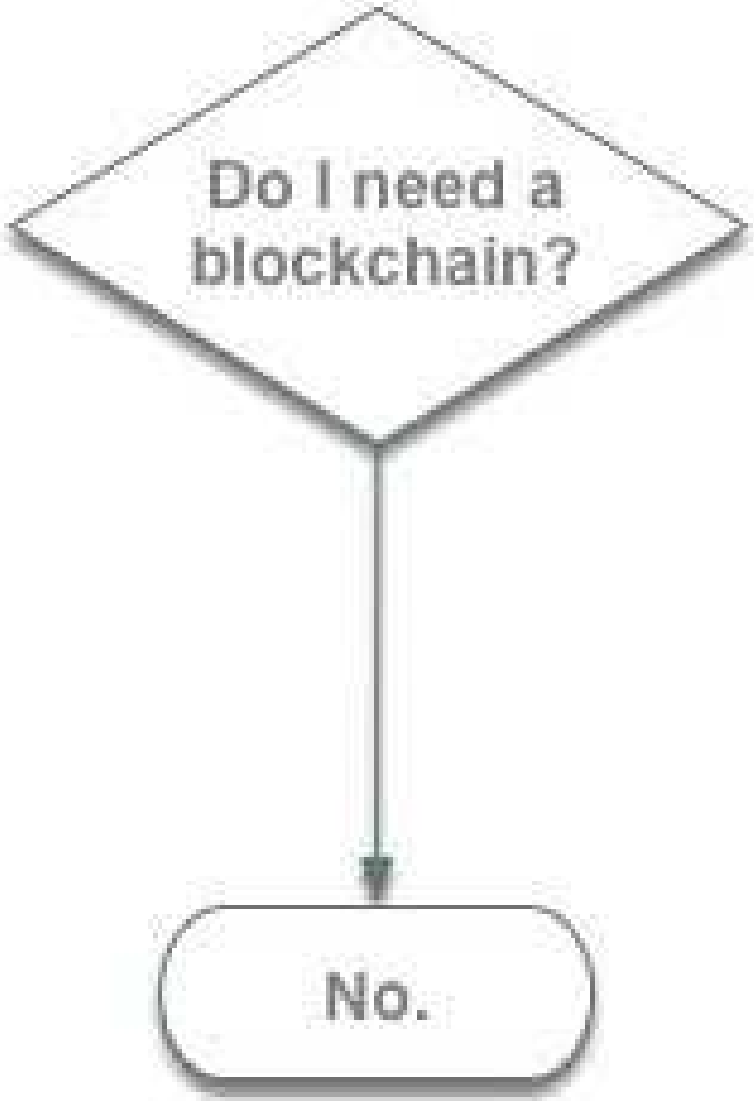
- ☐ Average weekly transfer fee over time.
- ☐ Neither cheap nor reliable.
- ☐ Logarithmic scale.

Replacement for cash



- ☐ Average confirmation time in Summer 2018.
- ☐ Not reliable.
- ☐ Too long for most cash transactions.

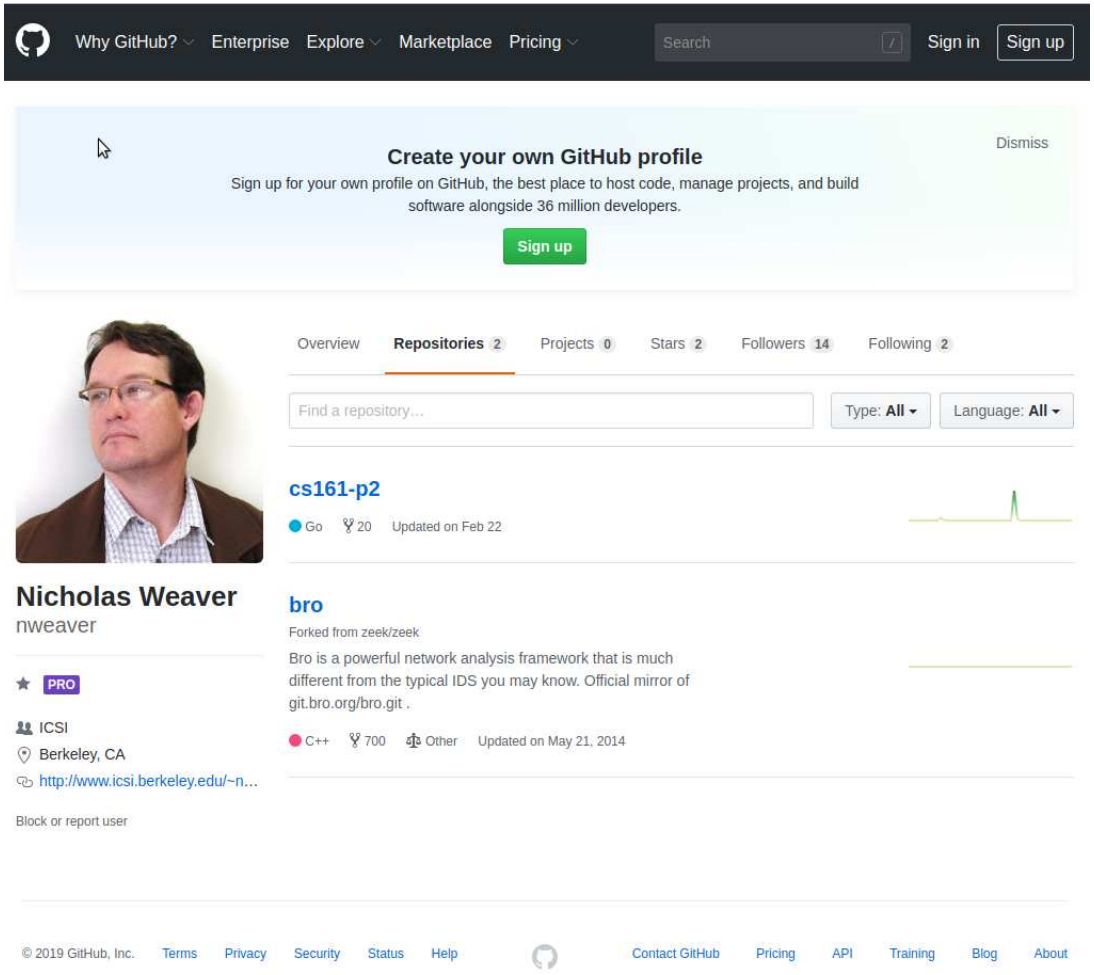
Flowchart



Nick Weaver

What is a private or permissioned blockchain? Just simply an append-only data structure with a limited number of authorized writers, a.k.a. a git archive. There's nothing fundamental in a private blockchain that hasn't been understood in the field for 20-plus years. It's just it has a buzzword that causes idiots to throw money at the problem.

Git



Matt Blaze

matt blaze @mattblaze

Follow

Covering blockchain voting in my election security class feels like having a syllabus in an organic chemistry class devote three lectures to alchemy just so that the students will know what to say when their future employers expect them to turn lead into gold.

11:46 AM - 4 Apr 2019

618 Retweets **1,753** Likes

25 618 1.8K

matt blaze @mattblaze · Apr 4

Anyway, I'm in the soul-crushing part of the course now.

3 3 140

matt blaze @mattblaze · Apr 4

The frustrating thing is you start with the Satoshi paper, as beautiful and accessible piece of cryptographic engineering as I've seen, and then it's straight downhill in a jet-powered handbasket from there.

4 42 305

matt blaze @mattblaze · Apr 4

(Actually, I start with Merkle, because everything interesting in crypto starts with Merkle)

5 12 158

Davos

WORLD ECONOMIC FORUM

Industry Agenda | Blockchain

Blockchain is facing a backlash. Can it survive?

Image: REUTERS/Dado Ruvic/Illustra

Quotes

- Cryptocurrency is 'Honestly Useless': Harvard Cryptographer – *Bruce Schneier*
- Economist Nouriel Roubini Says 'Blockchain Is Useless, All ICOs Are Scams'
- "Blockchain is not only crappy technology but a bad vision for the future" –Kai Stinchcombe
- "Bitcoin Is Ridiculous. Blockchain Is Dangerous" – Paul Ford
- "Blockchain is a useless technology" – Glenn Chan

The Good

- Blockchain is a data structure
  - The doubly-linked-list is worthless/dangerous/crappy?
  - A lot of computing undergrads might agree.
- How about: "The data structure has ... properties"?
- "Use the data structure when it is helpful."
- Integrating signed hashes into a system with adversarial incentives is interesting.
- Using it to avoid tampering with a ledger can be very useful.

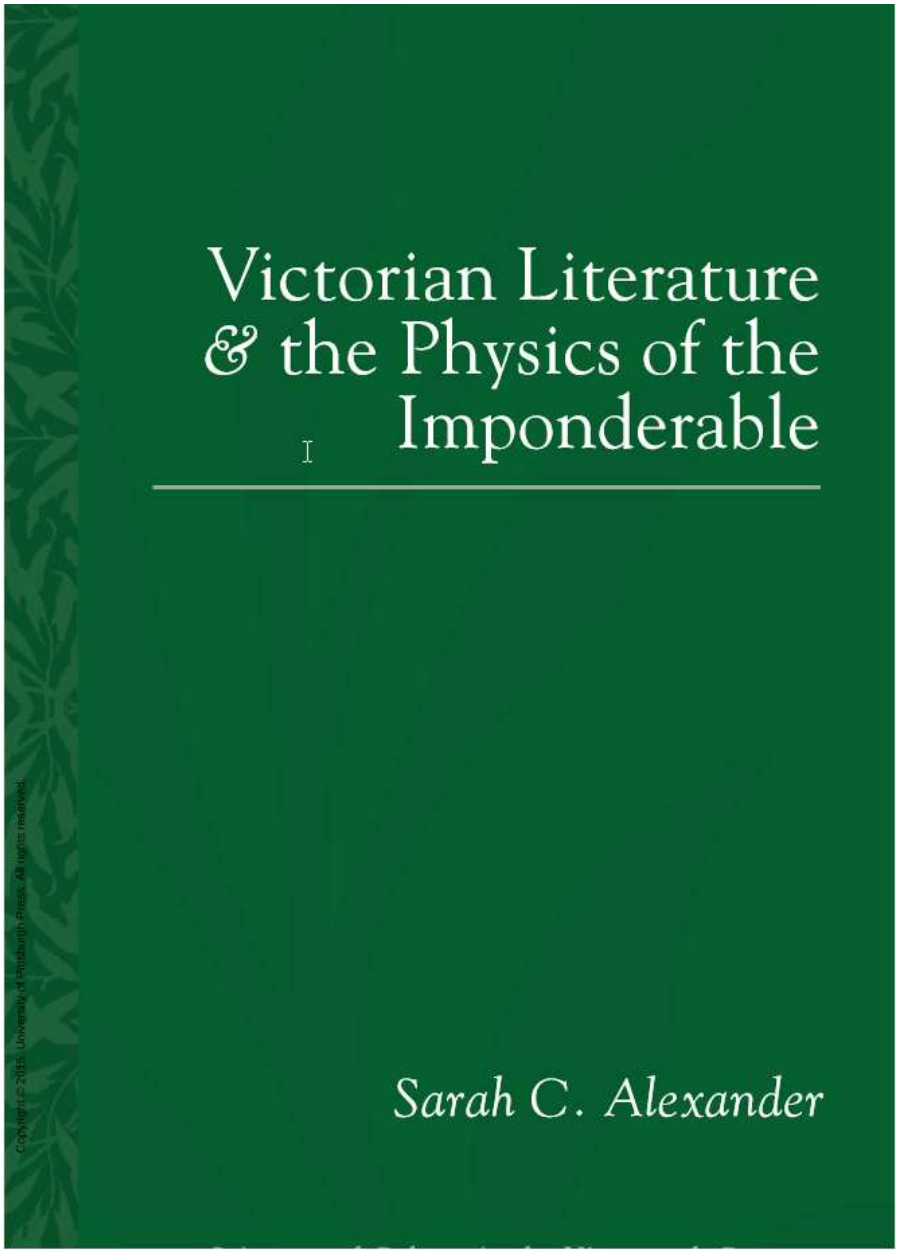
The Bad

- Blockchain does not assure security
- Blockchain does not make data private
- You can use blockchain to design secure systems.
- You can verify its properties.
- Nothing beats good engineering practice.
- Have never seen a data structure get such emotional responses.
- Just using the term to promise things it does not do is bad.

The Ugly

- Ridiculous hype does bring on a backlash.
- Negative hyperbole is no better than over promising.
- I really doubt that any data structure is on its own:
  - Useless
  - Crappy
  - Ridiculous
  - Dangerous
- Some applications of a data structure make sense, some do not.
- It can be used to add security and privacy, but you need to know what you are doing.

Questions?



https://www.jstor.org/stable/j.ctt1dwst10