Block chains: miracle cure or snake oil?

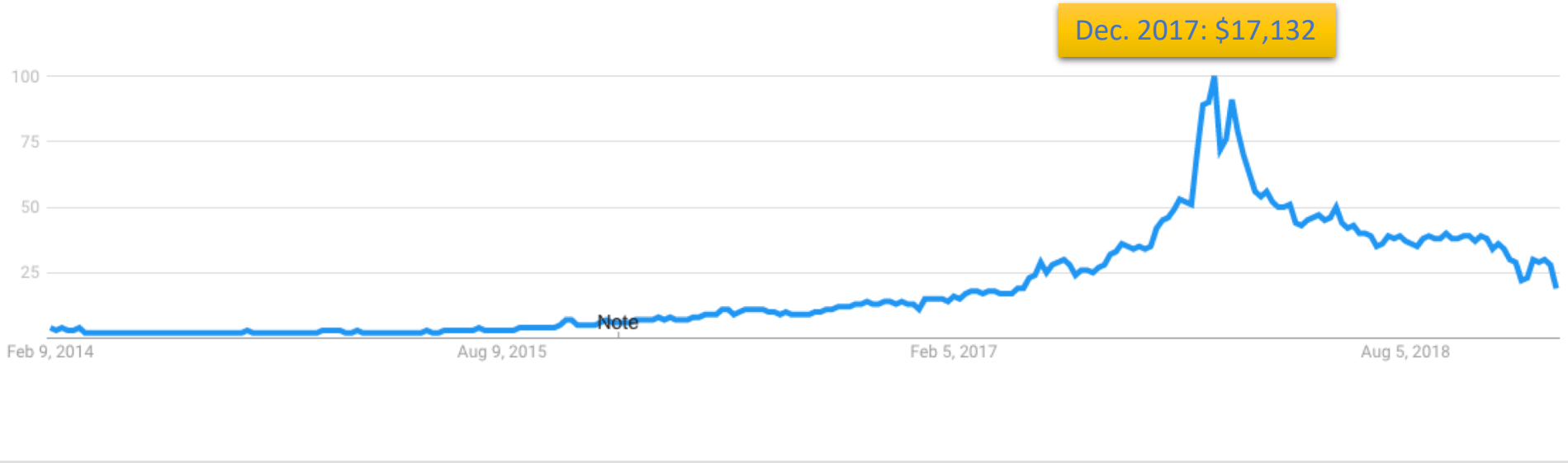
Henning Schulzrinne (Columbia University)

February 2019

Federal Reserve New York

"ML is programmed in Python, AI in PowerPoint."
Blockchain in exclamation marks!

Google searches: blockchain



Bitcoin (1 year)

store of value?
unit of account?

Bitcoin is the new gold – is it?

High on blockchain

1,055 views | Jan 21, 2019, 05:58am

How Blockchain Technology Can Help Cannabis Recovery Efforts In Natural Disasters

Andre Bourque Contributor ⓘ

Vices

I provide insight and advice on cannabis and blockchain.

Recording research precedence

TOOLBOX · 04 FEBRUARY 2019

Bitcoin for the biological literature

Scientific publishing is increasingly adopting the technology underlying cryptocurrencies.

Telecom

Howard said blockchain is even less understood by the telecommunications industry than AI and ML, since most public discussions around it have been in regards to cryptocurrencies.

"Many executives believe that blockchain could be used to maintain data integrity and support peer-to-peer trust in call detail records (CDR), once the technology is ready and its value has been defined," Howard **wrote** in his report. "A few hopeful operators are confident that blockchain is a strong candidate to ease overall telecommunications business transactions."

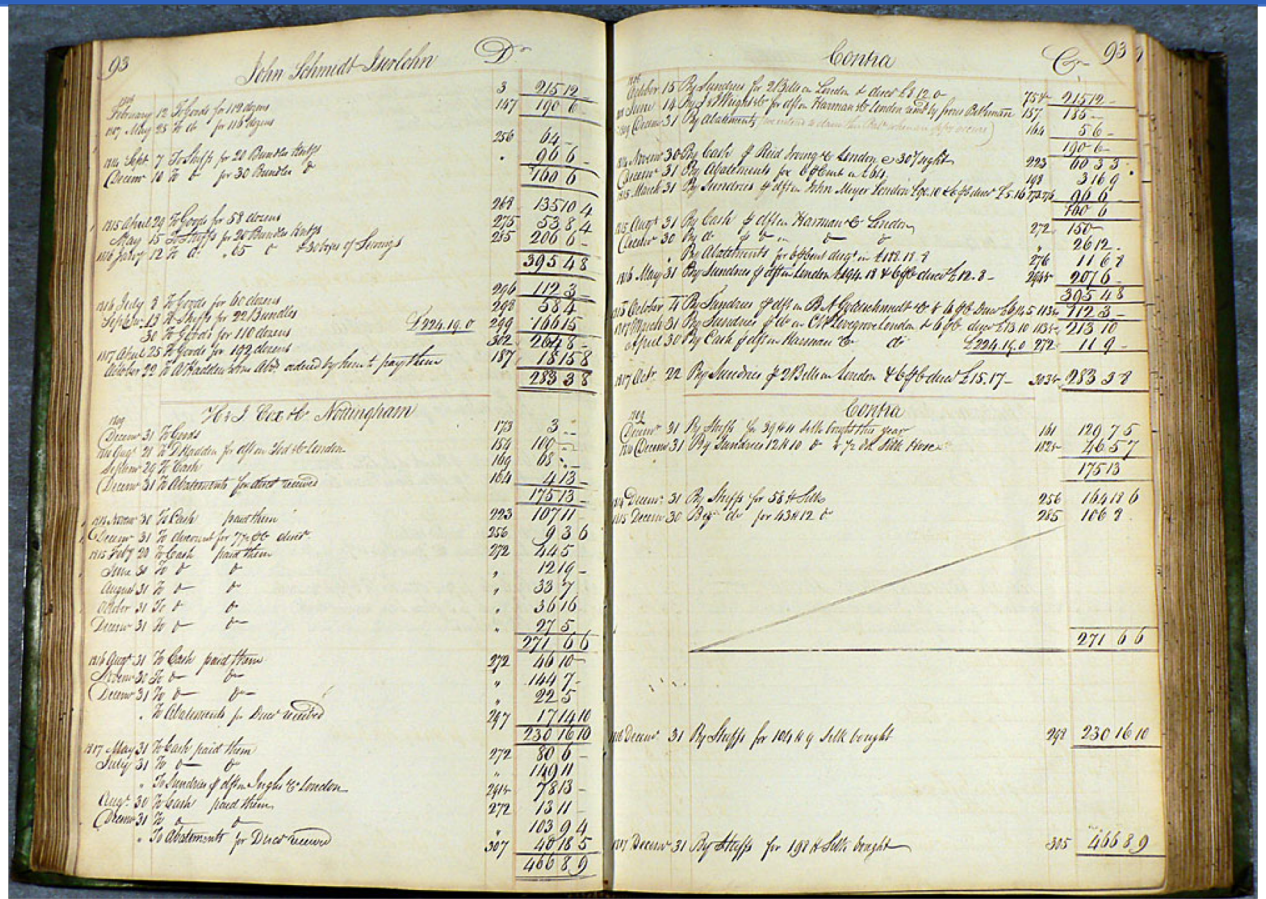
There has been a fair amount of activity on the blockchain front over the past year. MEF showed its support for blockchain at **its MEF18 conference** in October. In addition to the blockchain demos at the conference, MEF CTO Pascal Menezes said the standards development organization was using blockchain to exchange money and allocate resources between carriers.

RELATED: Colt and Zeetta Networks to demonstrate blockchain marketplace at MEF18

One of the proof-of-concept (PoC) demonstrations at MEF18 was the MEF Lifecycle Service Orchestration (LSO) Sonata API to enable transactions across a blockchain-based marketplace. LSO Sonata includes intercarrier quoting capabilities and blockchain-based billing and settlement features.

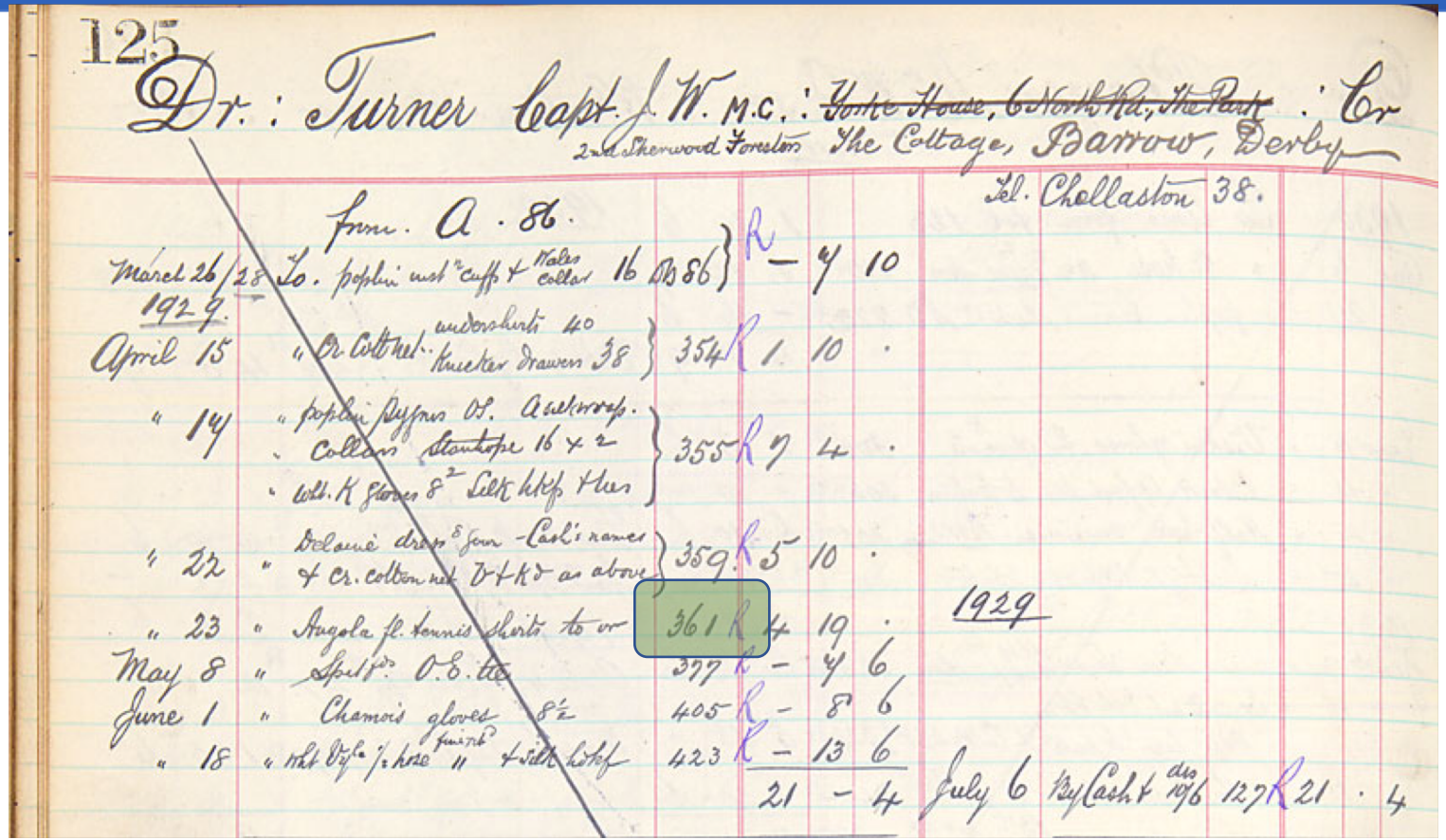
BT, Colt, HGC Global, Telefonica and Telstra conducted a trial early last year that used blockchain for wholesale settlement. In August, CBCcom, PCCW Global, Sparkle, Tata Communications, Clear Blockchain Technologies and Cataworx announced **a blockchain PoC trial**.

An early analog blockchain



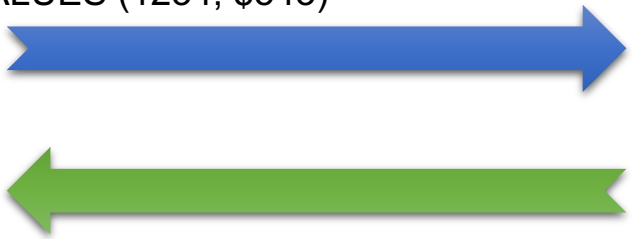
Nottingham, 1790

Key idea: linkage



What does a database do?

INSERT INTO ledger (customer, amount)
VALUES (1234, $543)

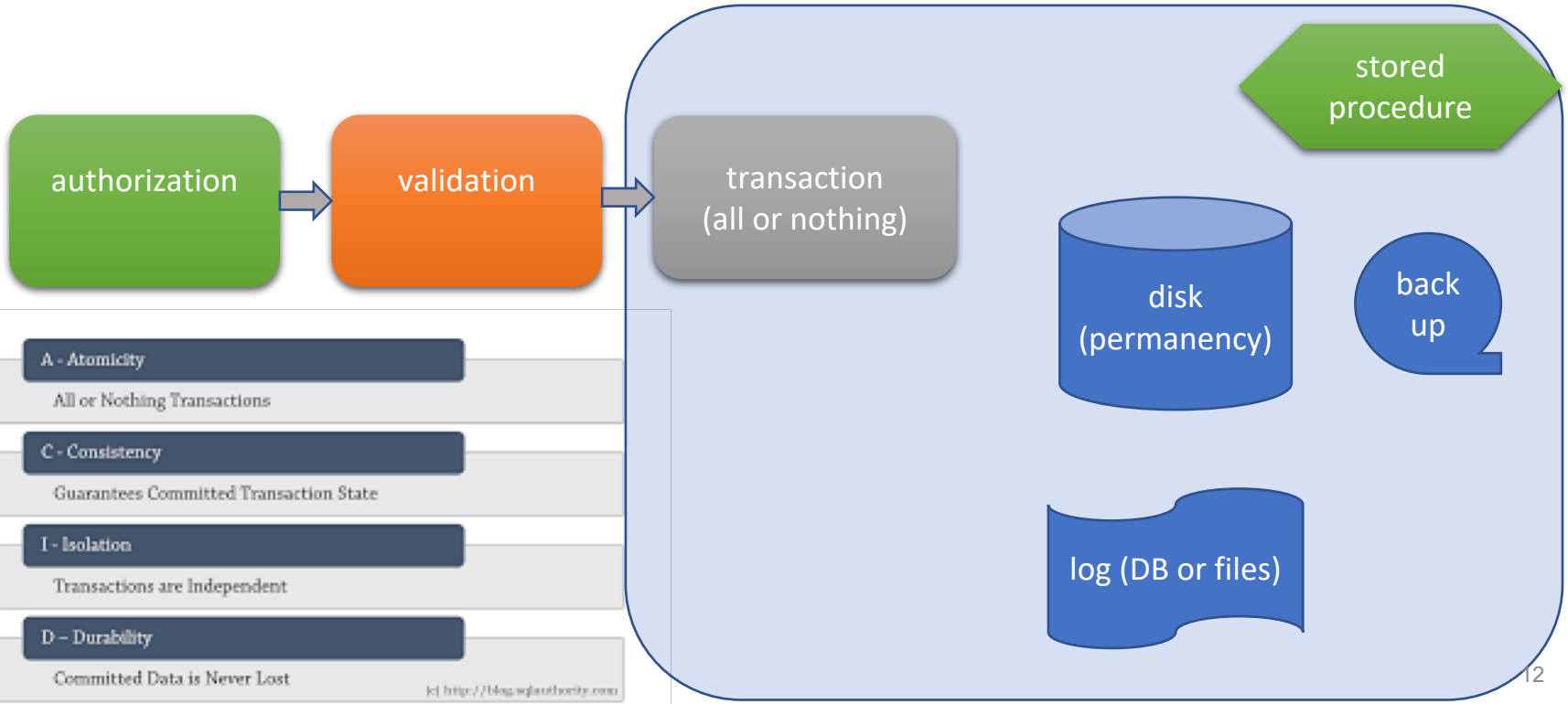


SELECT sum(amount) FROM ledger
WHERE customer = 1234

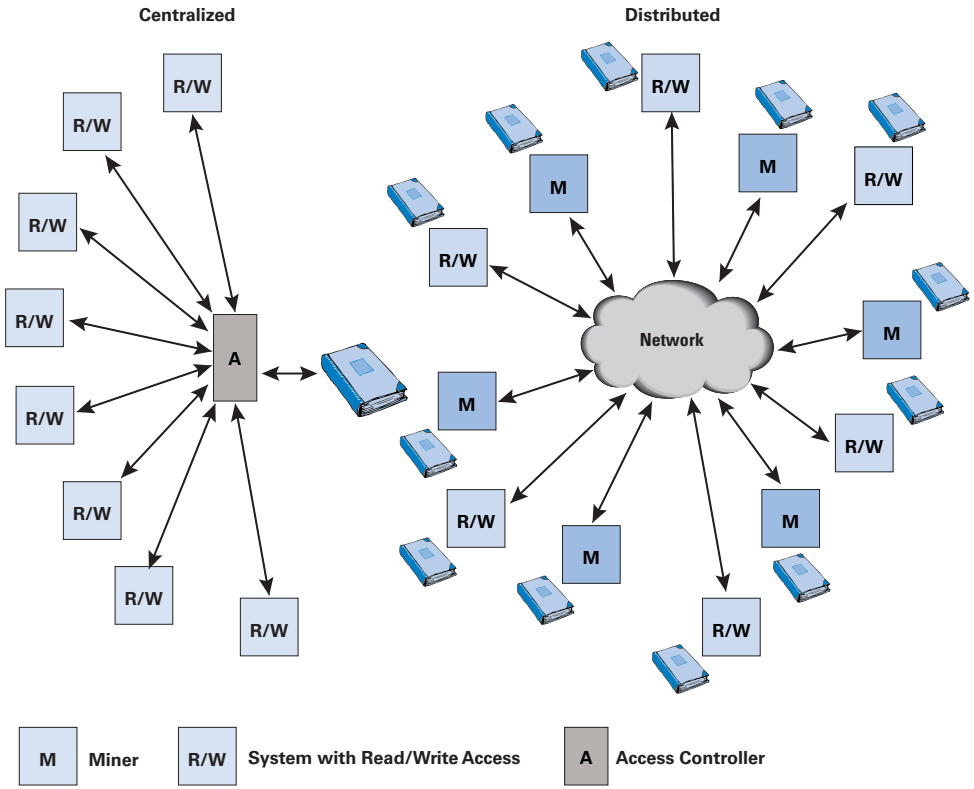
- trusted, reliable data store
- may be operated by third party (AWS, Azure, GC, …)
- transaction may be signed by originator
- content may be encrypted

Modern datastore architecture (simplified)

SELECT person, amount FROM payment JOIN person USING (person) WHERE …



Centralized → distributed



Concept: non-repudiation

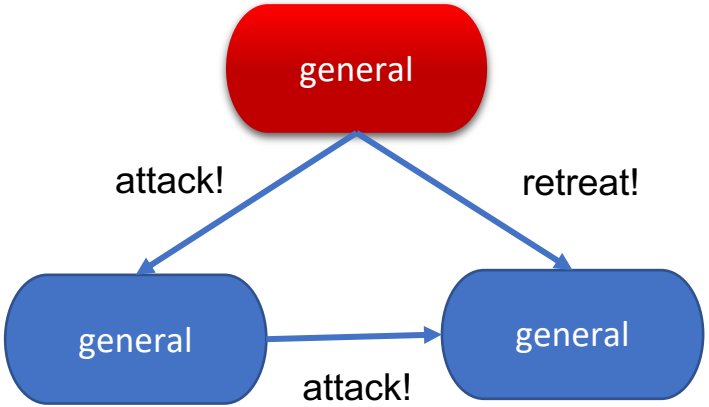
- “A statement's author cannot successfully dispute its authorship or the validity of an associated contract (or signature).”
- Traditional grounds (McCullagh):
  - The signature is a forgery;
  - The signature is not a forgery, but was obtained via:
    - Unconscionable conduct by a party to a transaction;
    - Fraud instigated by a third party;
    - Undue influence exerted by a third party.
- Crypto:
  - A service that *provides proof of the integrity and origin of data,* both in an *unforgeable relationship,* which can be verified by any third party at any time; or,
  - In authentication, an authentication that with high assurance can be asserted to be genuine, and *that can not subsequently be refuted*.
  - Typically, uses public-private key pair for validation and signing.
  - Refutation: author has to make plausible case that somebody stole their key.

BAR actors: Byzantine, altruistic, rational

Byzantine: may deviate from protocol for any reason
- technical failure
- deliberate harm
- gratuitous maliciousness

Rational: self interested
- maximize short-term or long-term benefit
- including any penalties or rewards

Altruistic: follow protocol exactly
- extrinsic or intrinsic motivation



What is a blockchain?

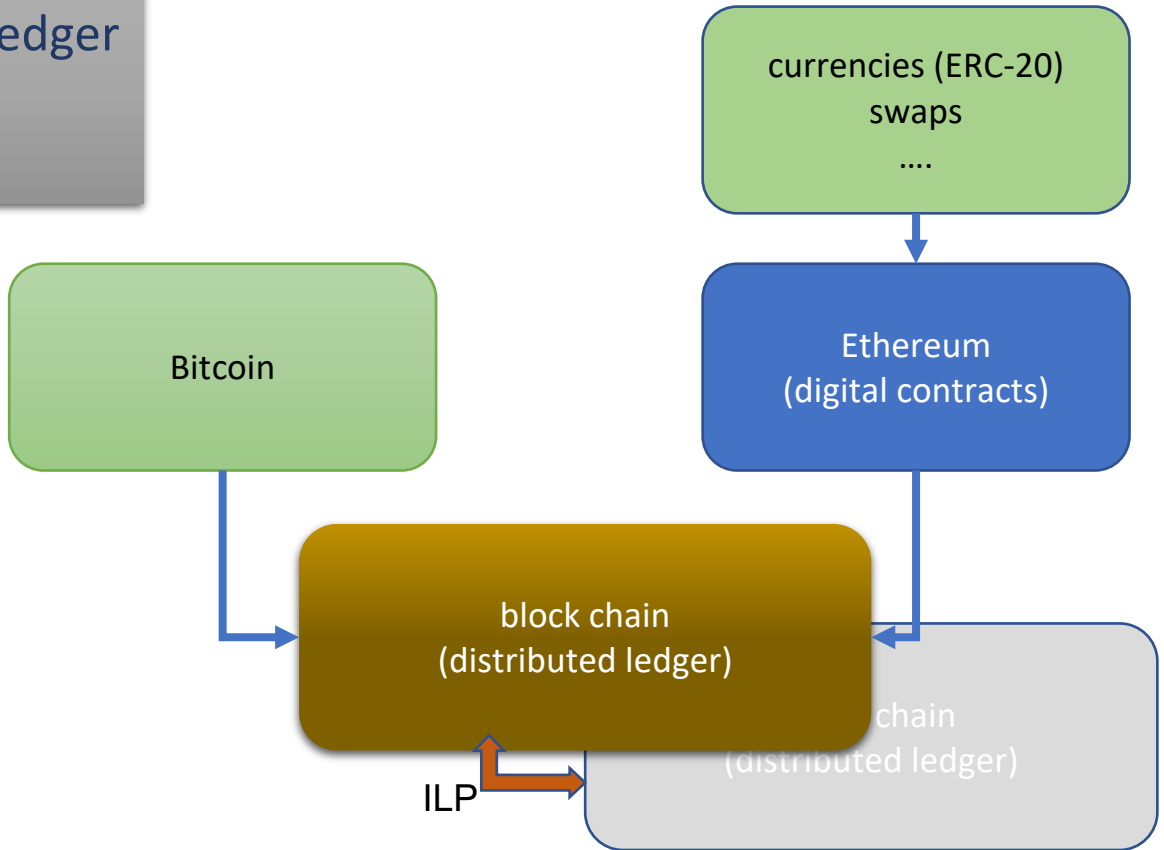
- Distributed ledger
- *Indelible*, append-only log of transactions between parties
- Which transactions happened?
  - "Alice transferred 10 coins to Bob”
- Order of transactions
  - "Alice transferred 10 coins to Bob, and then Bob transferred title to his car to Alice”
- Public (mostly) & accessible to all parties
- Tamper-proof: no party can add, delete, or modify ledger entries once they have been recorded

➔ *Ledgers must be immune to attack, ensuring the ledger remains secure even if some parties misbehave, whether accidentally or maliciously.*

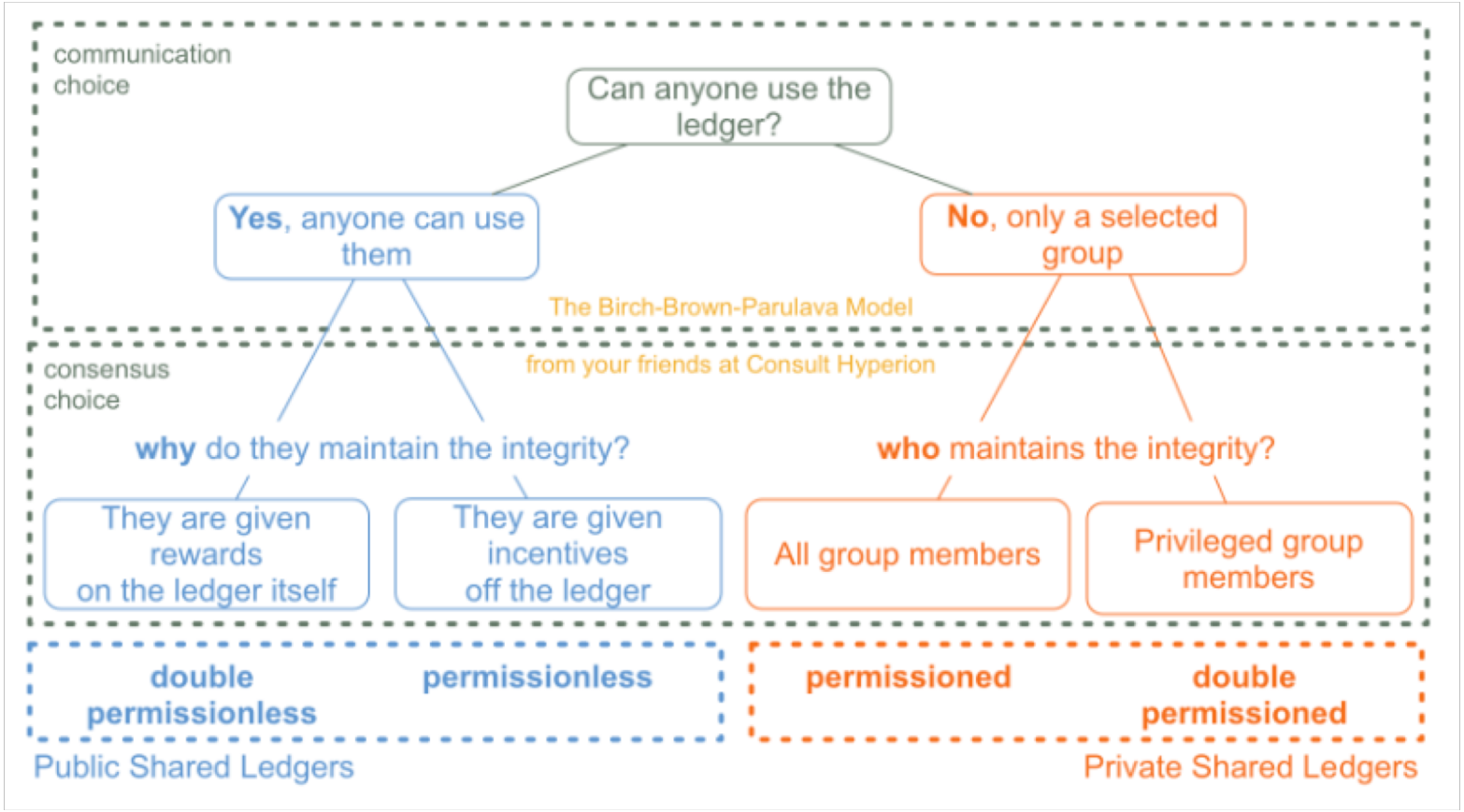
M. Herlihy, CACM 2/2019

Public blockchain architecture

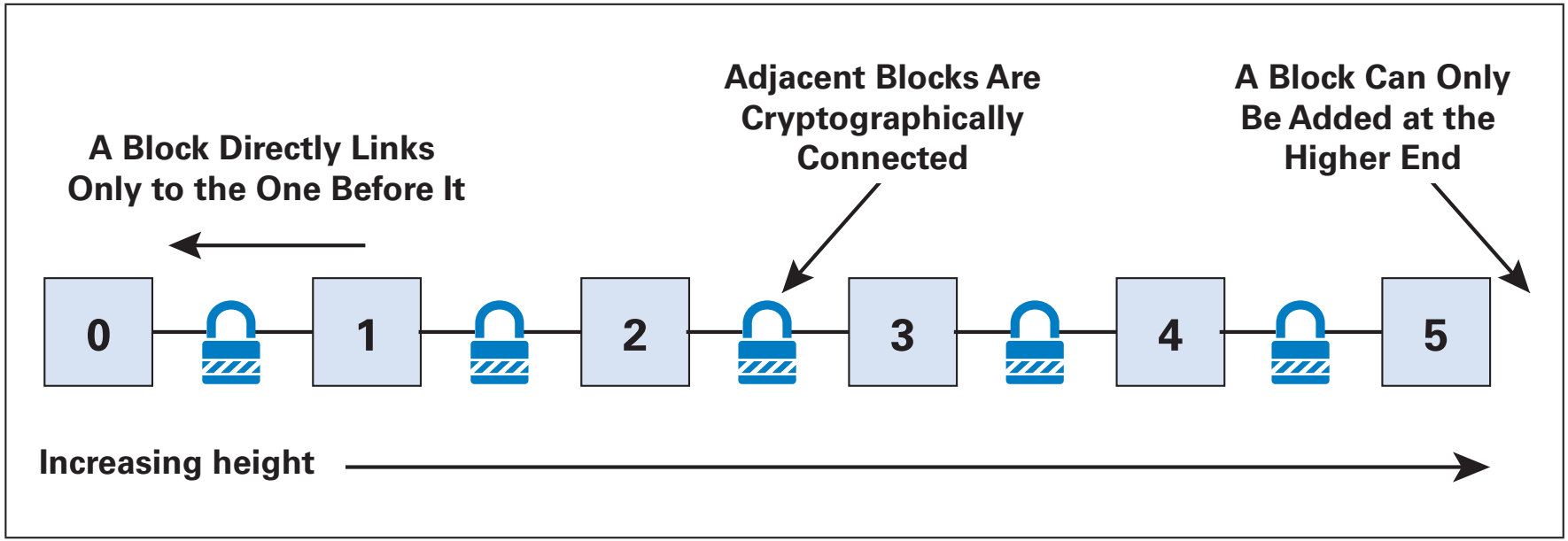
distributed ledger
+ consensus
+ currency



What kind of ledger?

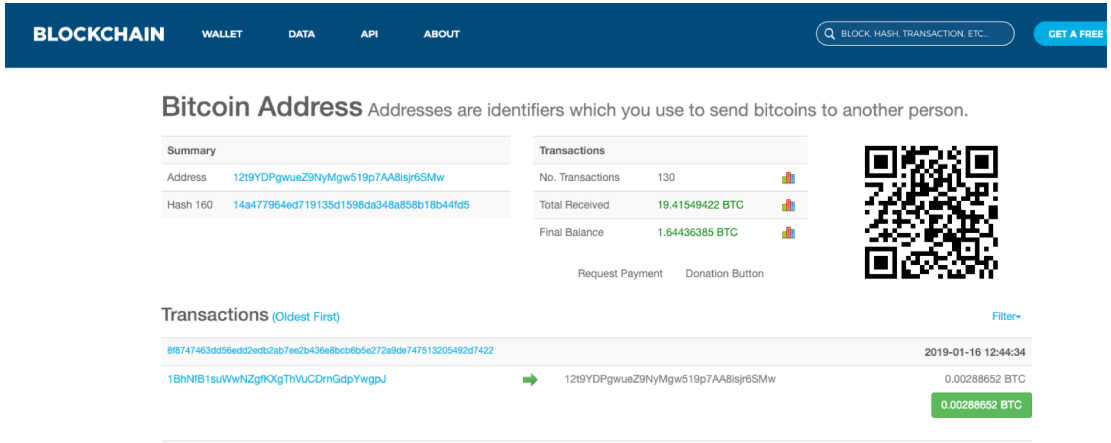


Block chaining

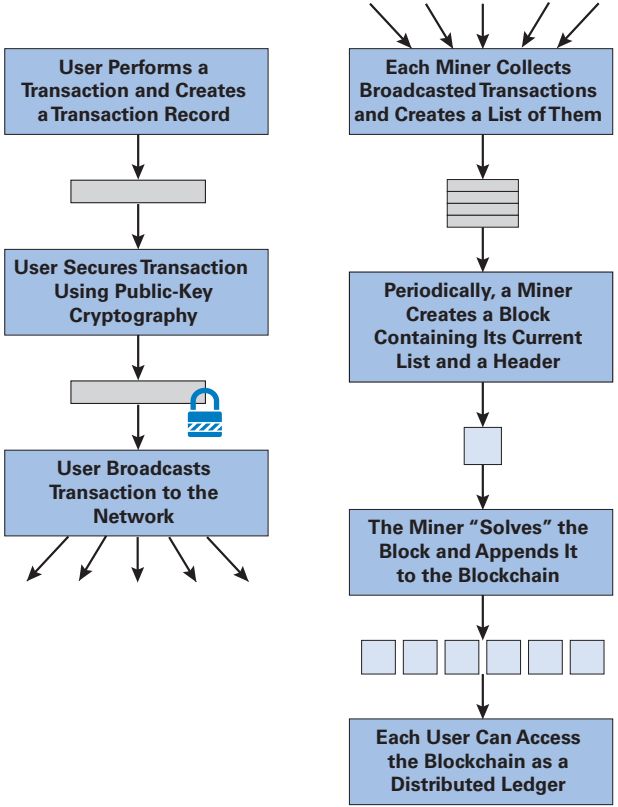


Concept: identifier

- Bitcoin addresses are tokens
- May (should) use unique address for each transaction
- Examples
  - P2PKH: 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2
  - Bech32: bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq



Adding transactions



What's in a block?

Item	Description
Magic Number	A unique identifier for the blockchain; remains constant for all subsequent blocks
Blocksize	Number of bytes following up to end of block
Version Number	Block format version
Link to Previous Block	Hash of preceding block header
Transaction Hash	The root node of a Merkle Tree, a descendant of all the hashed pairs in the tree. The root node is a 256-bit hash based on all of the transactions in the block.
Timestamp	When block was created
Mining Difficulty	A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.
Nonce	Used to calculate proof-of-work
Transaction Counter	Number of transactions in this block
Transactions	The (nonempty) list of transactions

Consensus algorithms

- Goal: make it difficult for (cheating) participants to collude – 51% problem
  - may also provide incentive to participate in validation – e.g., 12.5 BTC reward
- Idea: make it expensive to cheat
  - preferably more than you can gain
- Encourage distribution of block approver → decentralization
  - assumes implicitly linear cost → no or limited efficiencies of scale or scope
  - only needed if identities are easily forged and no external recourse (e.g., criminal prosecution)
- Variations, among many:
  - **Proof of Work (PoW)**: solve "hard" problem that requires computation → hardware + energy cost
    - reward given to first miner who solves cryptopuzzle
    - scale: mining farms (human labor, ASICs)
    - scope: own or access to cheap electricity or specialized circuits (ASICs)
  - **Proof of Stake (PoS):** validator chosen based on wealth

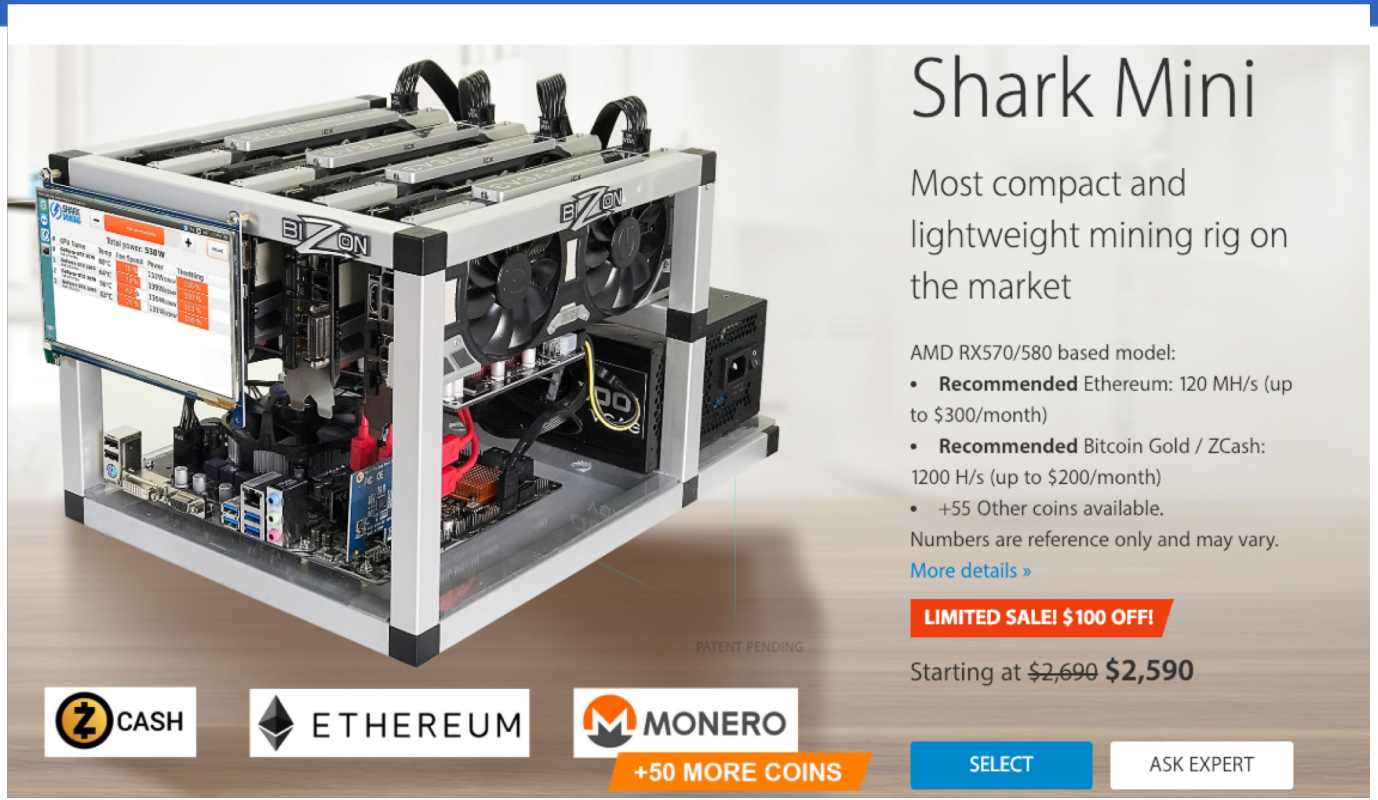
PoW ingredient: hash

Hash (SHA-256 for Bitcoin
ethash for Ethereum)

```
hash('sha256', 'The quick brown fox jumped over the lazy dog.');
68b1282b91de2c054c36629cb8dd447f12f096d3e3c587978dc2248444633483
```

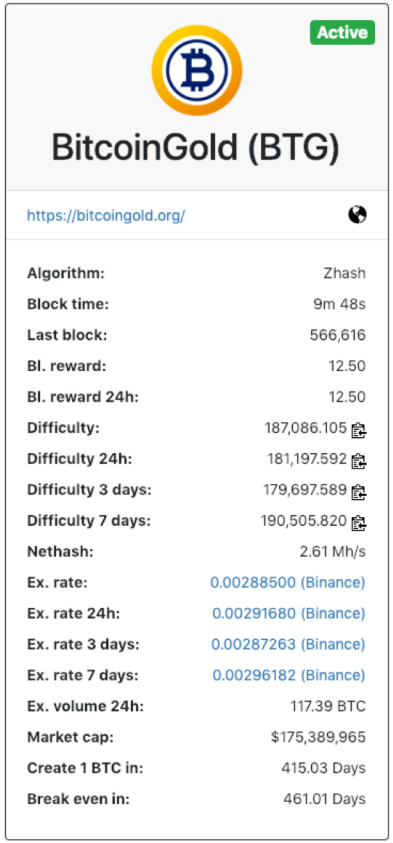
- Transforms any text or bit string into 32-byte (256 bit) number.
- 256 bit = 1.15 10^{77} = ~0.1% of number of atoms in visible universe.
- Need exhaustive search to construct string that creates same hash.
- Difficulty can be calibrated (number of matching digits).

Mine bitcoins at home!



Shark Mini, $2,590

This is not investment advice



Active

BitcoinGold (BTG)

https://bitcoingold.org/

Algorithm:	Zhash
Block time:	9m 48s
Last block:	566,616
Bl. reward:	12.50
Bl. reward 24h:	12.50
Difficulty:	187,086.105
Difficulty 24h:	181,197.592
Difficulty 3 days:	179,697.589
Difficulty 7 days:	190,505.820
Nethash:	2.61 Mh/s
Ex. rate:	0.00288500 (Binance)
Ex. rate 24h:	0.00291680 (Binance)
Ex. rate 3 days:	0.00287263 (Binance)
Ex. rate 7 days:	0.00296182 (Binance)
Ex. volume 24h:	117.39 BTC
Market cap:	$175,389,965
Create 1 BTC in:	415.03 Days
Break even in:	461.01 Days

Hash rate: 1160.0 h/s

Power: 600.0 W

Cost: 0.194 $/kWh

Block reward Enable: 12.5 BTG

Pool fee: 1.0 %

Hardware cost: 2590.0 $

Difficulty Enable: 181197.592

Exchange rate Enable: 0.00288500 BTC

BTC value Enable: 3491.1 $

Reset | Calculate

nexo Pay for hardware & electricity with crypto backed Nexo loans. Don't sell on the dip.

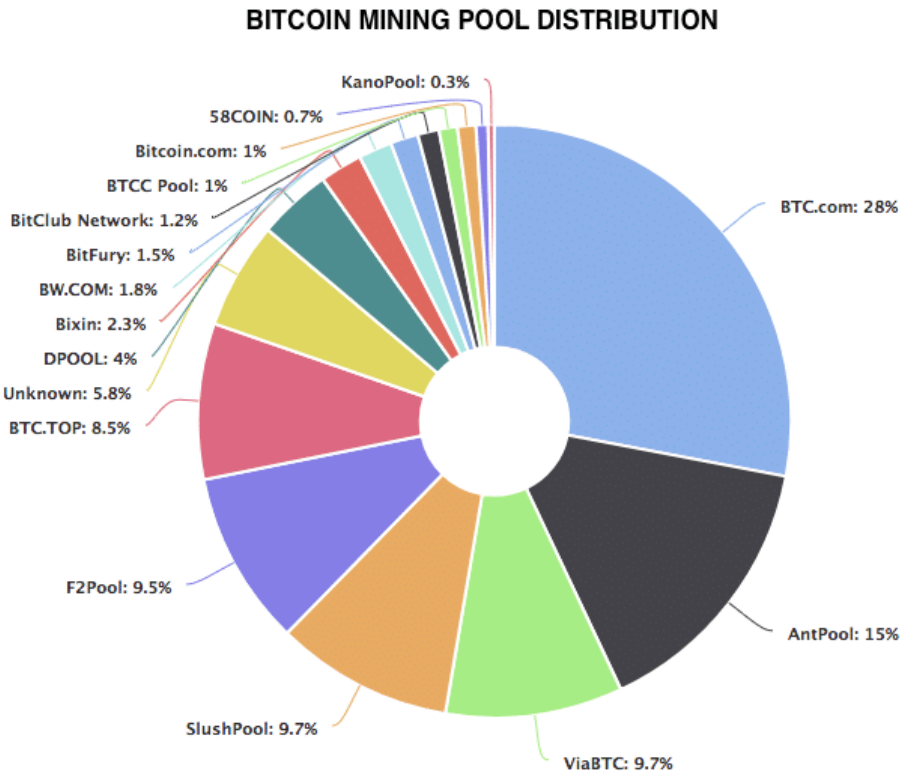
Please note that calculations are based on mean values, therefore your final results may vary.

Estimated Rewards

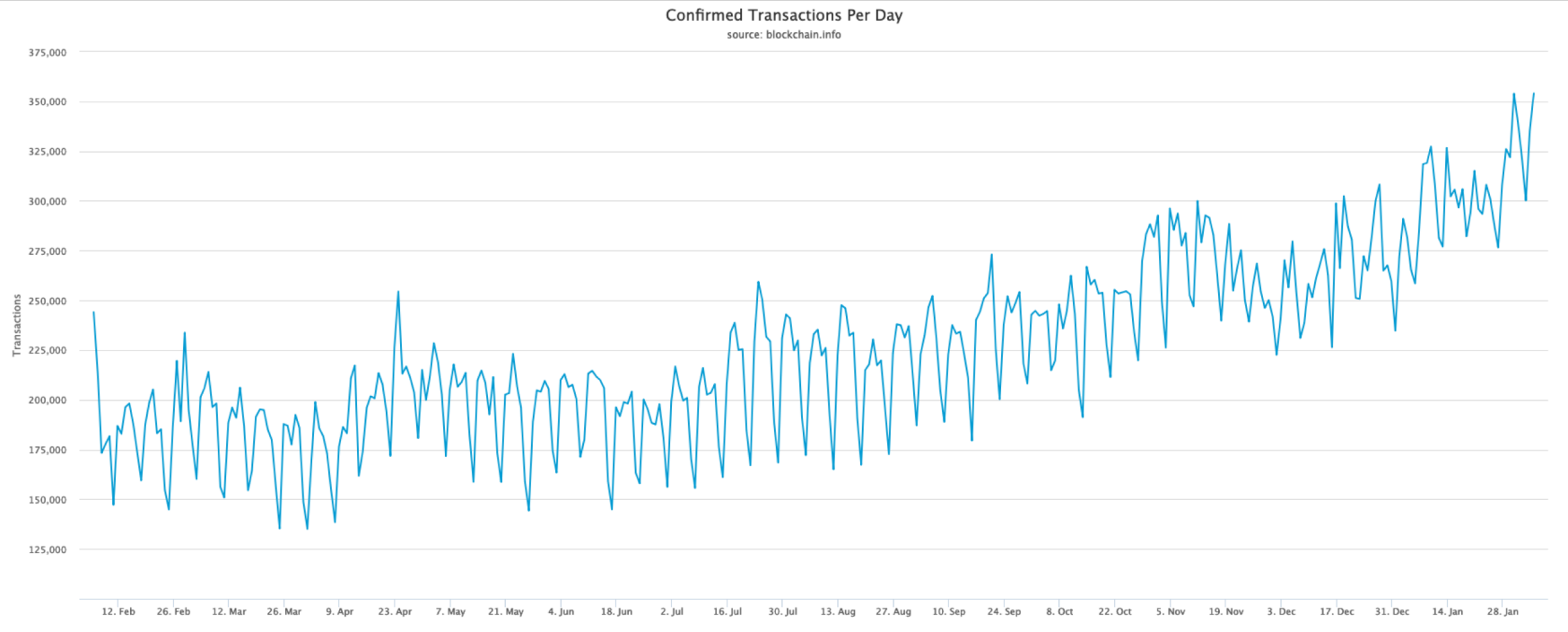
Per	Pool Fee	Est. Rewards	Rev. BTC	Rev. $	Cost	Profit
Hour	0.000352	0.034799	0.000100	$0.35	$0.12	$0.23
Day	0.008436	0.835170	0.002409	$8.41	$2.79	$5.62
Week	0.059052	5.846192	0.016866	$58.88	$19.56	$39.33
Month	0.253082	25.055110	0.072284	$252.35	$83.81	$168.54
Year	3.079163	304.837170	0.879455	$3,070.27	$1,019.66	$2,050.60

Bitmain Ordos facility, Inner Mongolia

Bitcoin mining pool distribution



Bitcoin transactions



medium of exchange?

Smart contracts

- Most financial service applications will need more than key-value storage
- Most blockchains (BTC, ETH) include a programming language
  - functions get executed on ”commit” by nodes
- Example asset transfer (Alice wants to trade share coupons for bitcoins):
  - *hashlock h* prevents an asset from being transferred until the contract receives a matching secret *s*, where $h = H(s)$
  - Alice creates a secret *s*, $h = H(s)$, and publishes a contract on the coupon blockchain with hashlock *h* and timelock 48 hours in the future, ensuring the contract will transfer the coupons to Bob if Bob can produce *s* within 48 hours. If he cannot, the coupons will be refunded to Alice.
  - When Bob confirms that Alice's contract has been published on the coupon blockchain, he publishes a contract on the Bitcoin blockchain with the same hashlock *h* but with timelock 24 hours in the future, ensuring the contract will transfer the bitcoins to Alice if Alice can produce *s* within 24 hours. If she cannot, the bitcoins will be refunded to Bob.
  - When Alice confirms that Bob's contract has been published on the Bitcoin blockchain, she sends the secret *s* to Bob's contract, taking possession of the bitcoins, and revealing *s* to Bob.
  - Bob sends *s* to Alice's contract, acquiring the coupons and completing the swap.

M. Herlihy, CACM 2/2019

AWS SQL server vs. bitcoin

AWS RDS server (m4.2xlarge)

- 2,100 SQL transactions/second
- $3,521/year
- **Intel Xeon E5-2676 v3: 120 W**

Bitcoin

- 3-7 transactions/second
- $6,800 ‘all-in’ cost per BTC
- 12.5 BTC per block reward
- 10 minutes per block
- → 657k blocks/year → $4.46B
- 3.4 GW

	Assertion	Answer
Network	A significant number of participants will be transacting on the network (>100)	Agree/Yes ☐
	You don't trust the participants in the network and don't need/want to know them	Agree/Yes ☐
Performance	A limited amount of data needs to be stored for every transaction (a few fields)	Agree/Yes ☐
	The business process doesn't requires a high throughput (scalability)	Agree/Yes ☐
Business logic	The business logic is simple	Agree/Yes ☐
	Privacy of transactions is not an important feature	Agree/Yes ☐
	The system will be standalone, it doesn't need to access external data or be integrated in the IT legacy	Agree/Yes ☐
Consensus	No arbitrator shall be involved in case of a dispute	Agree/Yes ☐
	All participants can be involved in the validation of transactions (Vs only a group of known validators)	Agree/Yes ☐
	You need strict immutability of the record (no amend & cancel, even by admin)	Agree/Yes ☐

Miracle cure vs. snake oil – public & private blockchain

Miracle cure (or at least good fit)

(all private)

- Distributed, semi-trusting users
- Limited ability to fund and administer common infrastructure
- Supply chain records
- Notary (time-stamped) services
  - non-repudiability (but limited time resolution)

Not FDA approved

(mostly public)

- Bitcoin, most digital currencies
- ICOs
- Consumer payments
- High-volume & low latency transactions (< minutes)
- Complex business logic

The blockchain conundrum

- Public blockchains don’t work all that well in practice
  - high cost
  - high risk
  - low performance
  - difficult governance (forks, ossification)
  - hard to balance privacy vs. prevention of illegal uses
- Private blockchains work
  - can avoid expensive consensus algorithms (no 51% problem)
  - can share computational resources (instead of paying a fee)
  - but if you have a trusted entity running the blockchain, why not run a database + cryptographically signed records?

What makes systems hard in practice?

- Adversarial environment
  - attacker almost always has the advantage
    - has to find one flaw, you have to find all of them
  - particularly, if one cannot back out mistakes
- Near-100% uptime
- Unknown scaling
- Versioning and backward compatibility
  - no clear ability to upgrade
  - unknown dependencies
  - unclear governance (who gets to decide)

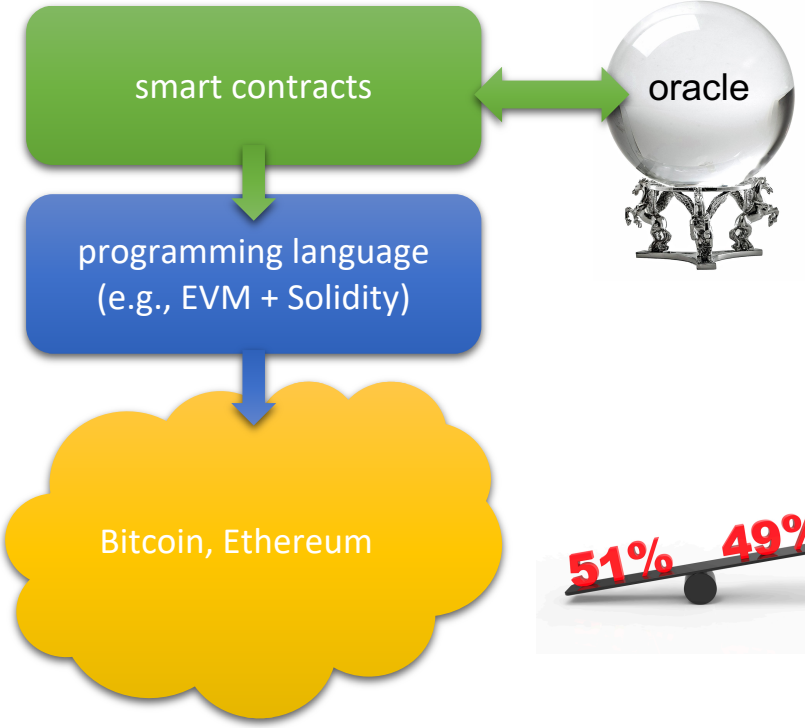
Leslie Lamport (1987): A distributed system is one in which the failure of a computer you didn't even know existed can render your own computer unusable.

Cryptography is (relatively) easy, security is hard

phishing

exchange

cyber attack
fraud



Security problems

Same as all software systems

- Specification flaws
  - protocol timing, bid down, man-in-the-middle, …
- Implementation flaws
  - in underlying system software
  - in application software
  - in configuration
- Credential theft or exposure
- Insider attacks
  - and other non-technical issues

Specific to public blockchains

- Little legal recourse
- International
- No “backup”
- No “undo” (fund reversal)
- No intermediary (e.g., credit card charge-back)
- May not be able to recover credentials

Limitations of computer science

- We do not know how to prove (most) specifications correct
  - People routinely find problems in security protocols years later
- Programming languages themselves are often buggy
- Distributed systems are much harder than centralized systems
  - “concurrency” – things can happen in various orderings
  - many more failure possibilities → impossibility results
- We depend on assumptions on the underlying system that may not be true
  - see Spectre & Meltdown
- Maintaining and configuring software is not well understood
  - dependencies
- Cryptographic key management is *logistically* hard

Random examples

GONE —

Digital exchange loses $137 million as founder takes passwords to the grave

QuadrigaCX survivors try to hack encrypted laptop in hopes of accessing cold wallet.

DAN GOODIN - 2/2/2019, 11:40 AM

By Saturday, 18th June, the attacker managed to drain more than 3.6m ether into a "child DAO" that has the same structure as The DAO. The price of ether dropped from over $20 to under $13.

Several people made attempts to split The DAO to prevent more ether from being taken, but they couldn't get the votes necessary in such a short time. Because the designers didn't expect this much money, all the ether was in a single address (bad idea), and we believe the attacker stopped voluntarily after hearing about the fork proposal (see below). In fact, that attack, or another similar one, could continue at any time.

bitfloor

The group found ways of hacking hardware wallets via four different methods; **supply chain attack**, firmware vulnerability, side-chain attack, and chip-level vulnerability. All techniques required access to the actual device, so if your wallet has never left your possession...then you could still be at risk from a supply chain attack.

Unalterable is maybe not that great an idea

Someone added images of child sexual abuse to an immutable blockchain ledger, the BBC reported. The images were added to the Bitcoin Satoshi Vision (BSV) core ledger through the payment processing app Money Button.

"We have confirmed that was the case and we have banned the user responsible for creating those transactions," Money Button wrote. "We believe it is important to be proactive about moderating content. Now that Bitcoin SV has the ability to write large amounts of data to the blockchain, it is likely that criminals will continue to attempt to abuse this technology for illegal purposes."

My tentative questions & recommendations

- Can a simpler (less general) system do the same thing?
  - E.g., a digital notary service
- What other systems are connected to the blockchain and what effects can they have?
  - Eco system, not blockchain (e.g., exchanges, wallets, mining pools, …)
- Governance and sustainability is more important than technical details
  - Who gets to do overrides when things go wrong?
  - Who decides and how when there are conflicts between stake holders?
- Speed kills – slow down execution and allow reversals
  - see Bangladesh Bank cyber heist
- What are the emergency brakes?
  - see autonomous cars (remote control) – autonomous driving is easy; it's the lack of braking that causes accidents
- What are the data privacy and accountability trade-offs?

JPMorgan report 2019

"Blockchain solutions making a meaningful difference for banks are at least three to five years away," JPMorgan said.

On the contrary, the bank believes the true potential of blockchain lies in its capability to streamline and automate cumbersome banking processes — for instance, it says that trade finance, which refers to monetary activities facilitating domestic and international trade) will benefit the most. The industry is worth $2 trillion and accounts for 15% of global trade, according to the report.

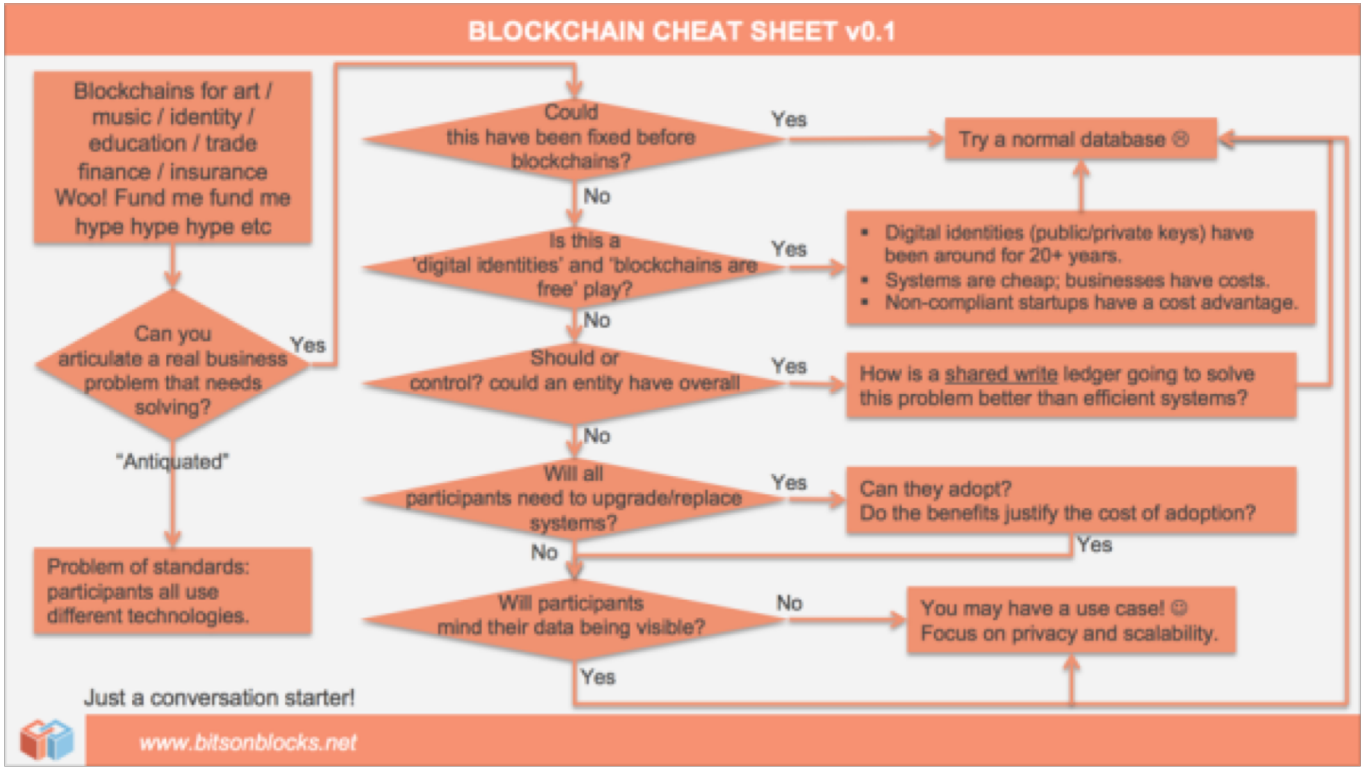
Conclusion

- Blockchain offers a variation of an old computing abstraction (database)
- Important to distinguish public vs. private blockchains
- Useful general-purpose service for mid-to-low trust interaction
- Distributed, decentralized, limited trust → at cost of energy, privacy
- But many of the permissioned blockchain problems can be solved with less effort and complexity
  - Does not ensure truth, but may ensure non-repudiation
  - But may offer convenient standard and infrastructure (”BaaS”)
- May assume more maturity of computer science than realistic
  - More potential security issues, not fewer

Useful not-too-technical tutorials and opinions

- NIST, ”Blockchain Technology Overview”, NISTIR 8202, Oct. 2018

  https://doi.org/10.6028/NIST.IR.8202
- W. Stallings, “A Blockchain Tutorial”, Cisco *Internet Protocol Journal,* Nov. 2017.
- Maurice Herlihy, “Blockchains From a Distributed Computing Perspective,” *Communications of the ACM* (CACM), Feb. 2019.
- Bruce Schneier, “There’s no good reason to trust blockchain technology,” Wired, Feb. 6, 2019.


BLOCKCHAIN CHEAT SHEET v0.1
Blockchains for art / music / identity / education / trade finance / insurance Woo! Fund me fund me hype hype hype etc
Can you articulate a real business problem that needs solving?
Yes
"Antiquated"
Problem of standards: participants all use different technologies.
Could this have been fixed before blockchains?
Yes
Try a normal database ⊗
No
Is this a 'digital identities' and 'blockchains are free' play?
Yes
Digital identities (public/private keys) have been around for 20+ years.
Systems are cheap; businesses have costs.
Non-compliant startups have a cost advantage.
No
Should or control? could an entity have overall
Yes
How is a shared write ledger going to solve this problem better than efficient systems?
No
Will all participants need to upgrade/replace systems?
Yes
Can they adopt?
Do the benefits justify the cost of adoption?
No
Yes
Will participants mind their data being visible?
No
You may have a use case! ☺
Focus on privacy and scalability.
Yes
Just a conversation starter!
www.bitsonblocks.net

DHS model

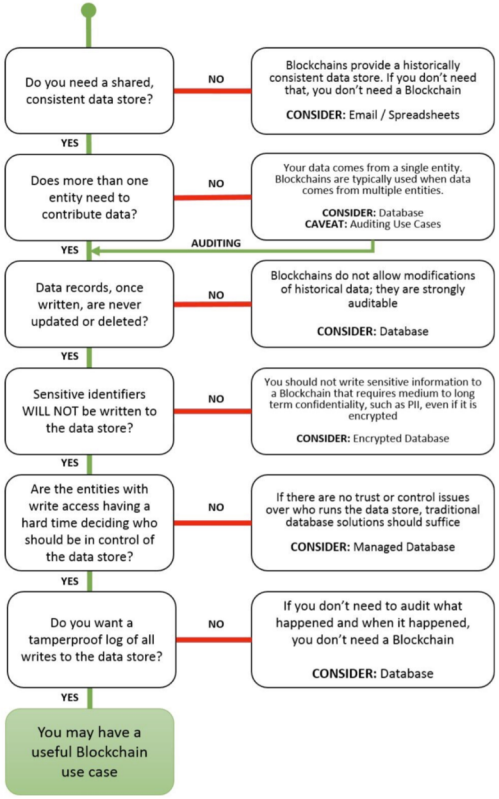


Figure 6 - DHS Science & Technology Directorate Flowchart

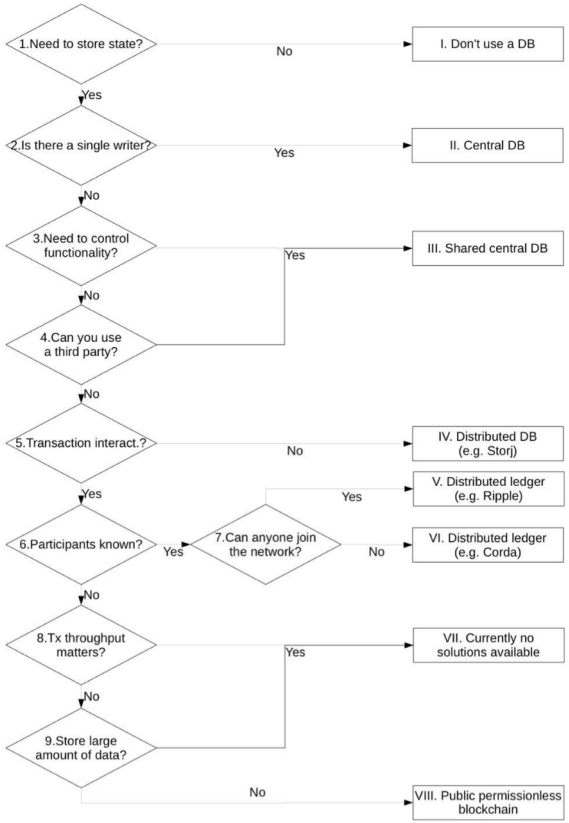
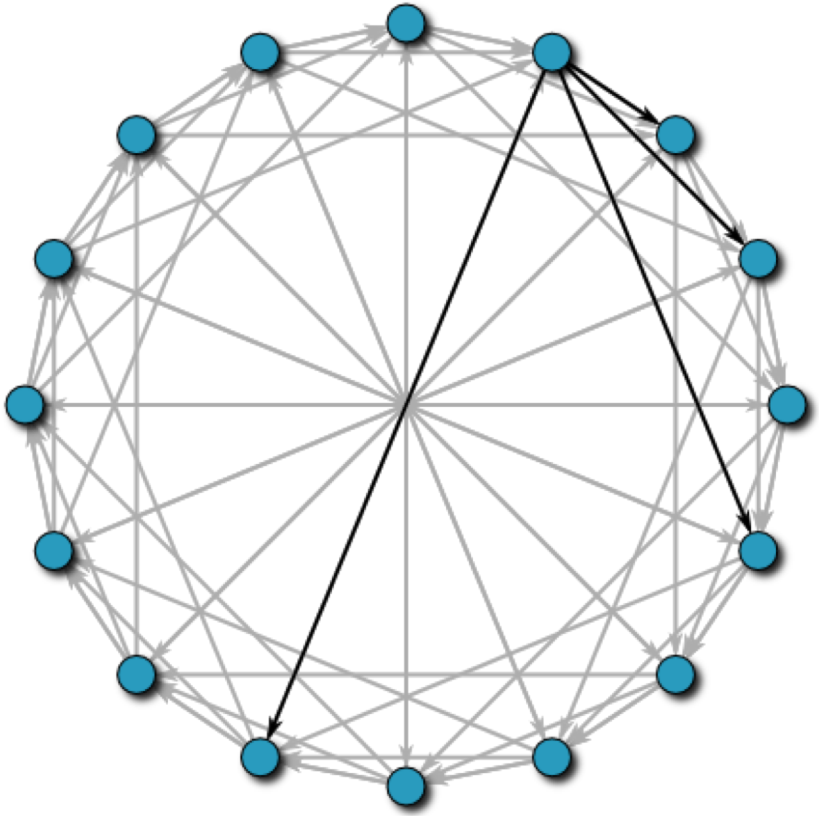


Fig. 2. Scheme for determining which type of database is appropriate

Predecessor: peer-to-peer systems

key – value mapping
(“noSQL”)
distributed storage
but: no inherent protection against



Bruce Schneier on private blockchains

Private blockchains are completely uninteresting. (By this, I mean systems that use the blockchain data structure but don't have the above three elements.) In general, they have some external limitation on who can interact with the blockchain and its features. These are not anything new; they're distributed append-only data structures with a list of individuals authorized to add to it. Consensus protocols have been studied in distributed systems for more than 60 years. Append-only data structures have been similarly well covered. They're blockchains in name only, and—as far as I can tell—the only reason to operate one is to ride on the blockchain hype.

Wired, 2019

Trust models

- *Liars and Outliers* (Schneier, 2012):
  - morals
  - reputation
  - institutions → ”laws formalize reputation” + sanctions + incentives (credit score)
  - security systems (locks, fences, alarm systems, audit systems, …)
- *Blockchain and the New Architecture of Trust* (Werbach, 2018):
  - peer-to-peer trust
  - leviathan trust (institutional)
    - contracts
  - intermediary trust
    - credit cards, escrow, …
  - distributed trust
    - blockchain (maybe also online review systems)

Practical CS: The power of a few service abstractions

- Key-value store → noSQL, file system, AWS S3
- Database → linked tables with predicates
- Process → protection domain → containers (Docker, Kubernetes)
- Virtual machine
- Queue → AWS SQS, work queues
- Messaging → email, SMS, EDI
- Query-Response (API) → HTTP
- Serialization: data structures → portable objects (ASN.1, XML, JSON, …)
- Pattern matching
- Public key systems