Decentralization and web3 technologies

Gaurish Korpal and Drew Scott

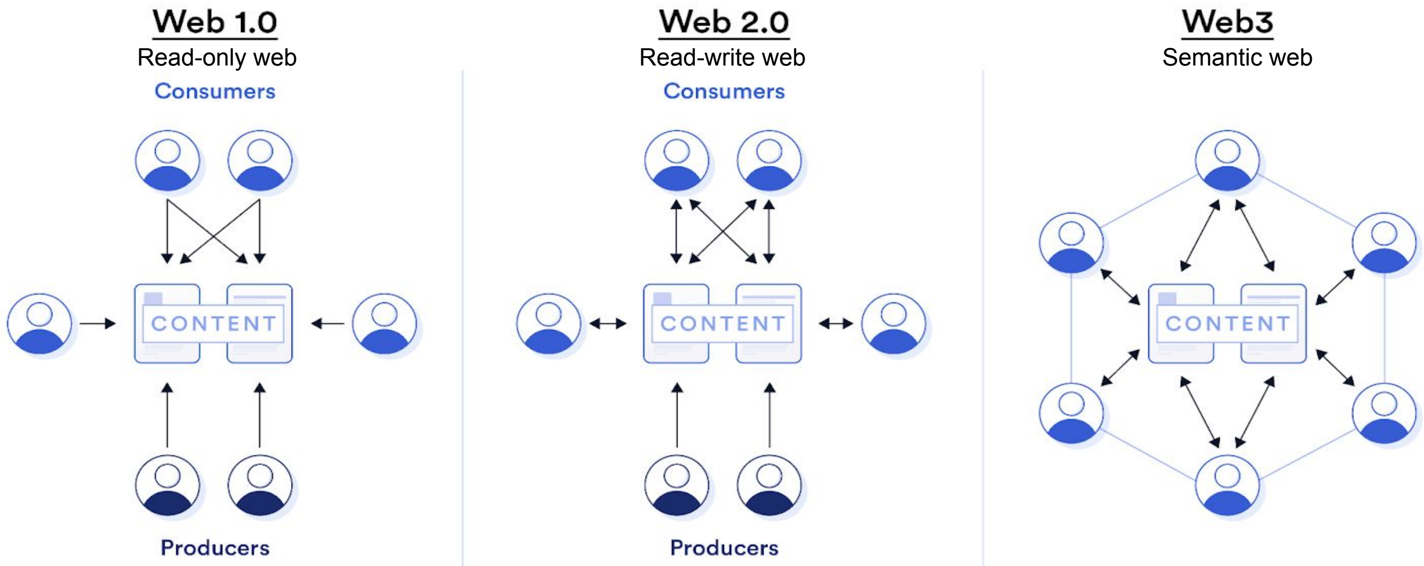
Outline

- What is web3?
- Why do we need web3?
- How can we create web3?
- What’s next?

What is web3?

Self-Certifying Web

Self-certifying protocols, based on **cryptographic user identifiers** and **content-addressed data**, can help us achieve **user-generated authority**.



Host-generated content,
host-generated authority.

User-generated content,
host-generated authority.

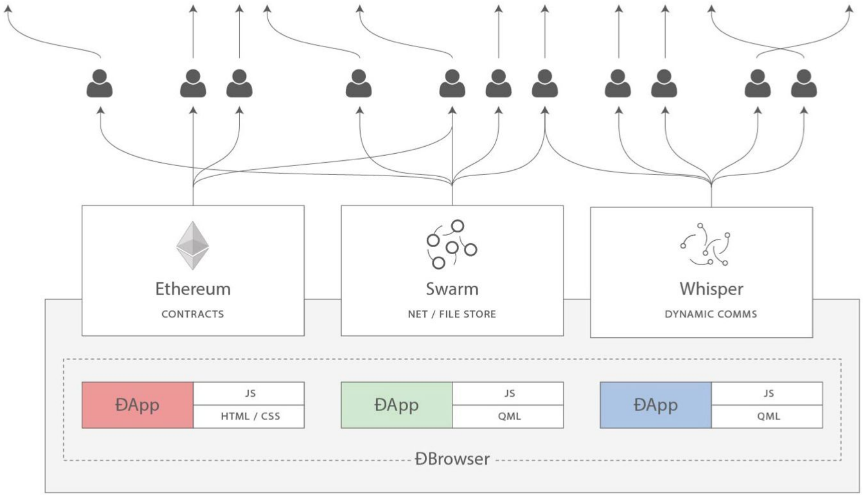
User-generated content,
user-generated authority.

https://chain.link/education/web3

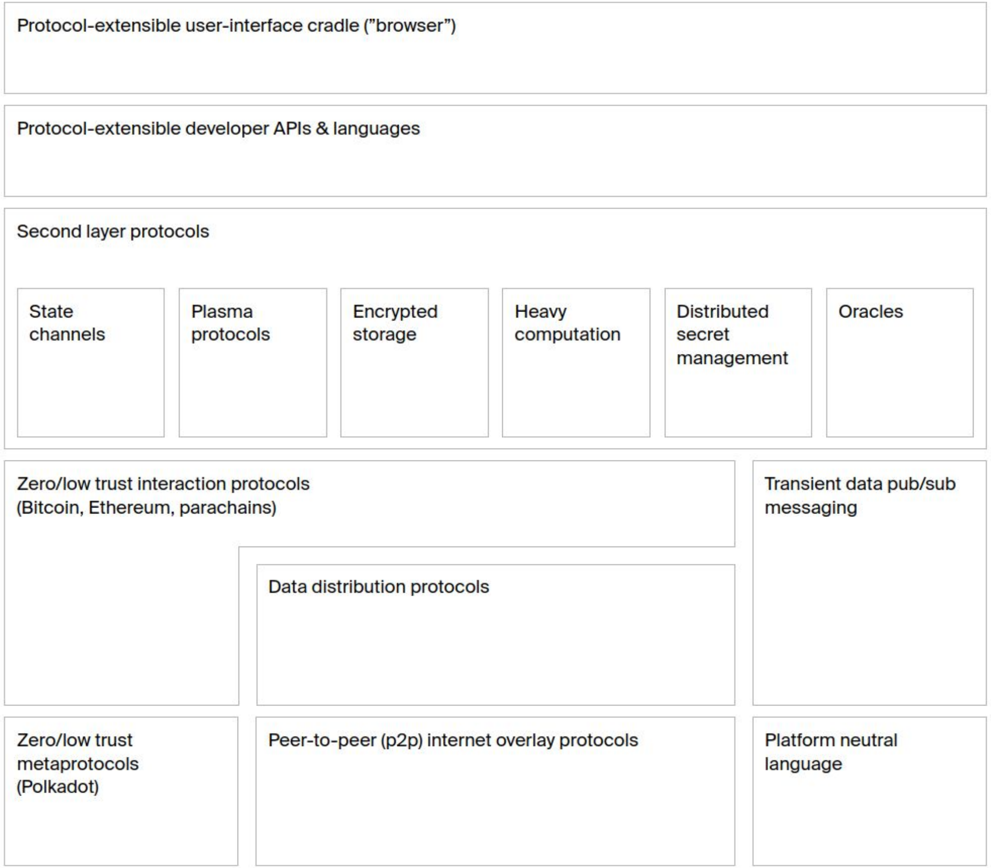
https://jaygraber.medium.com/web3-is-self-certifying-9dad77fd8d81

Web3

Blockchains are self-certifying protocols that create consensus on global state, emulating a centralized database without any one party being in control.



https://blog.ethereum.org/2014/08/18/building-decentralized-web/



Protocol-extensible user-interface cradle ("browser")

Protocol-extensible developer APIs & languages

Second layer protocols

State channels

Plasma protocols

Encrypted storage

Heavy computation

Distributed secret management

Oracles

Zero/low trust interaction protocols (Bitcoin, Ethereum, parachains)

Transient data pub/sub messaging

Data distribution protocols

Zero/low trust metaprotocols (Polkadot)

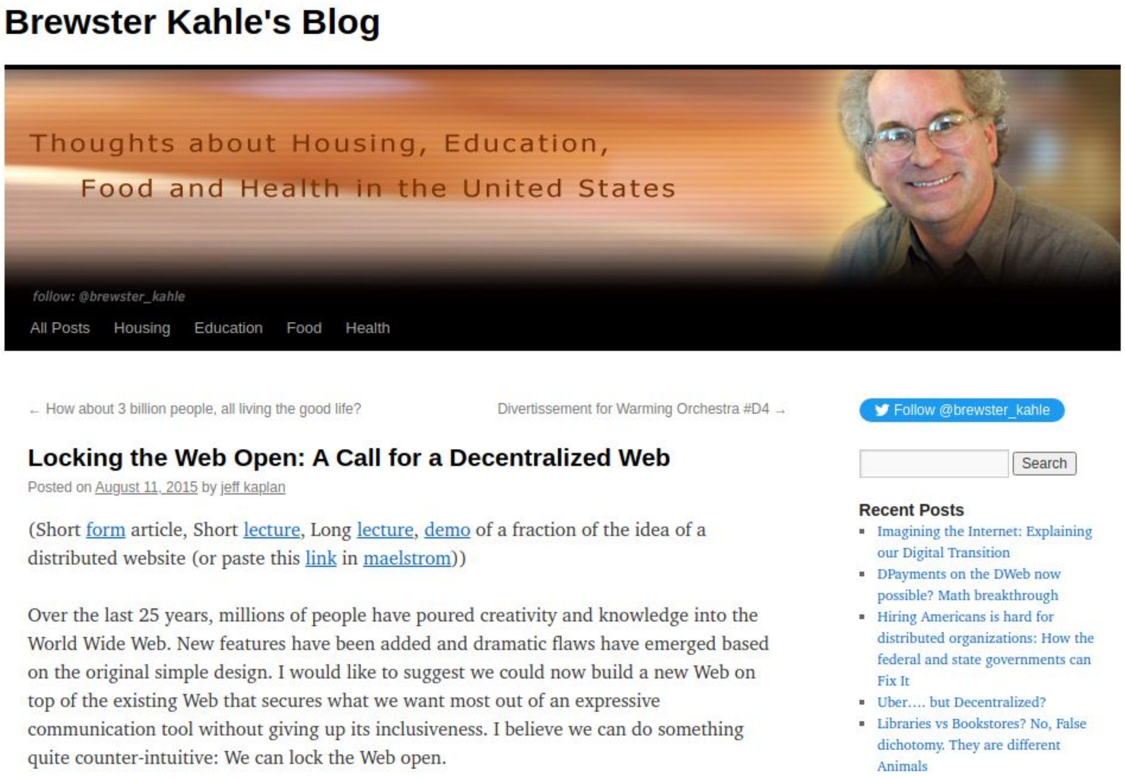
Peer-to-peer (p2p) internet overlay protocols

Platform neutral language

https://web3.foundation/about/

DWeb

git WebRTC I2P bitcoin IPFS



Brewster Kahle's Blog

Thoughts about Housing, Education, Food and Health in the United States

follow: @brewster_kahle

All Posts Housing Education Food Health

← How about 3 billion people, all living the good life? Divertissement for Warming Orchestra #D4 →

Locking the Web Open: A Call for a Decentralized Web

Posted on August 11, 2015 by jeff kaplan

(Short form article, Short lecture, Long lecture, demo of a fraction of the idea of a distributed website (or paste this link in maelstrom))

Over the last 25 years, millions of people have poured creativity and knowledge into the World Wide Web. New features have been added and dramatic flaws have emerged based on the original simple design. I would like to suggest we could now build a new Web on top of the existing Web that secures what we want most out of an expressive communication tool without giving up its inclusiveness. I believe we can do something quite counter-intuitive: We can lock the Web open.

Follow @brewster_kahle

Search

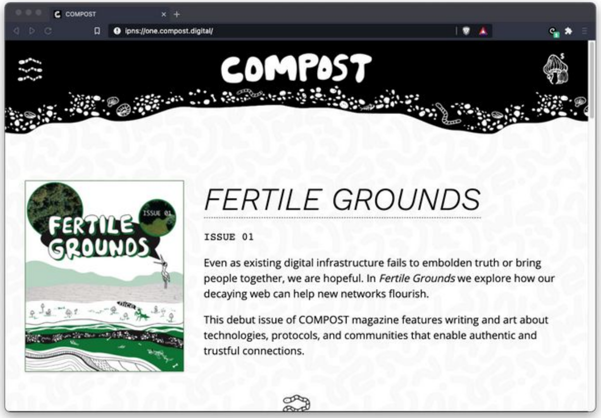
Recent Posts

- Imagining the Internet: Explaining our Digital Transition
- DPayments on the DWeb now possible? Math breakthrough
- Hiring Americans is hard for distributed organizations: How the federal and state governments can Fix It
- Uber…. but Decentralized?
- Libraries vs Bookstores? No, False dichotomy. They are different Animals

https://brewster.kahle.org/2015/08/11/locking-the-web-open-a-call-for-a-distributed-web-2/

Distributed Press

Check out COMPOST, a magazine about the digital commons, telling stories about people building the web as a shared resource. COMPOST is published to the web and DWeb using the Distributed Press API.



COMPOST

ipns://one.compost.digital/

COMPOST

FERTILE GROUNDS

ISSUE 01

Even as existing digital infrastructure fails to embolden truth or bring people together, we are hopeful. In *Fertile Grounds* we explore how our decaying web can help new networks flourish.

This debut issue of COMPOST magazine features writing and art about technologies, protocols, and communities that enable authentic and trustful connections.

COMPOST magazine viewed over IPFS on the Brave Browser with Web Monetization extension.

https://distributed.press/

Why do we need web3?

Decentralized network

Even though the Internet was built on distributed protocols, the web needed to consolidate around a few curated service platforms in order to become practical for everyday people to use.

Therefore, in today's web, a small number of stakeholders have an outsized influence over the content the public can create and consume.

For example, **Facebook** is a *centralized network* where data is controlled by a central entity, and **Amazon Web Services** is a *distributed network* where the data is stored across a grid, but still controlled by a central entity.

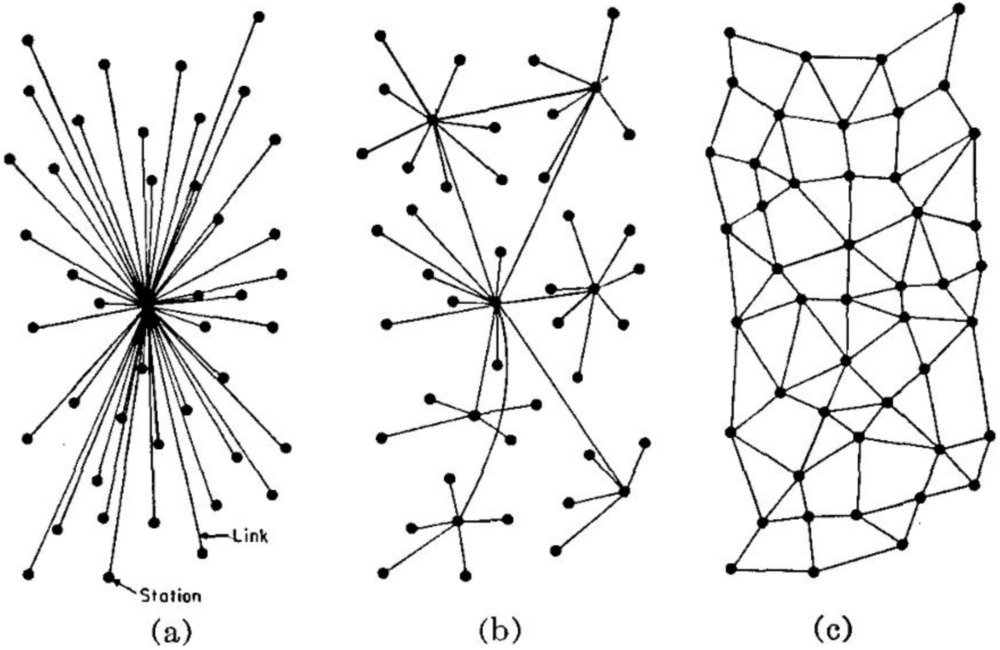
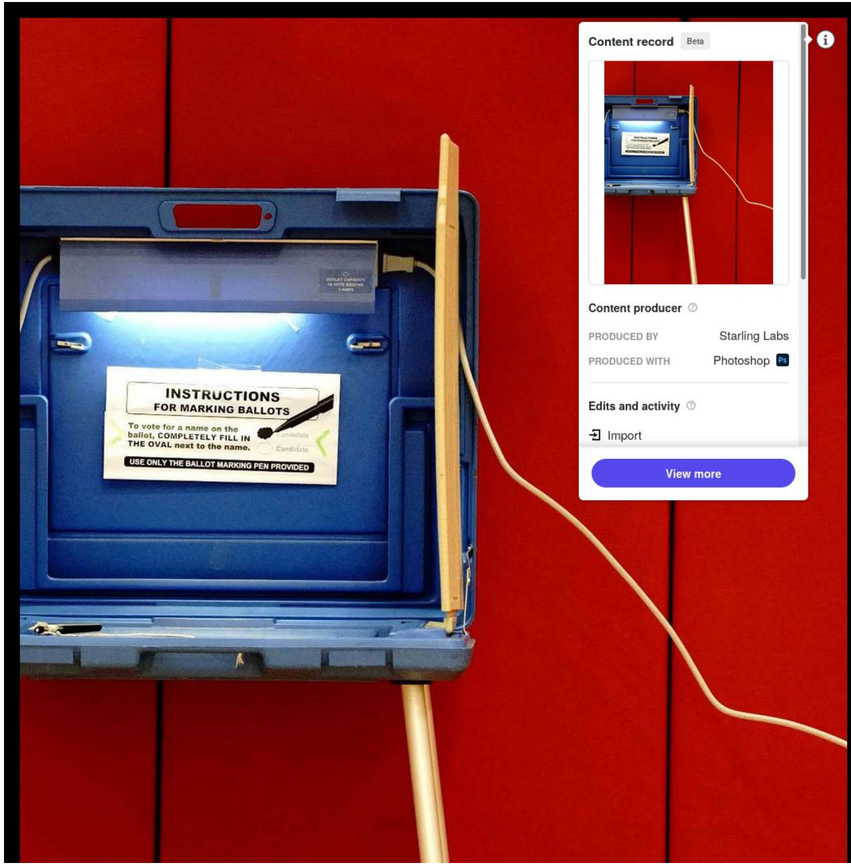


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

https://doi.org/10.1109/TCOM.1964.1088883

Re-decentralization


INSTRUCTIONS FOR MARKING BALLOTS
To vote for a name on the ballot, COMPLETELY FILL IN THE OVAL next to the name.
Candidate
Candidate
USE ONLY THE BALLOT MARKING PEN PROVIDED

Content record Beta

Content producer

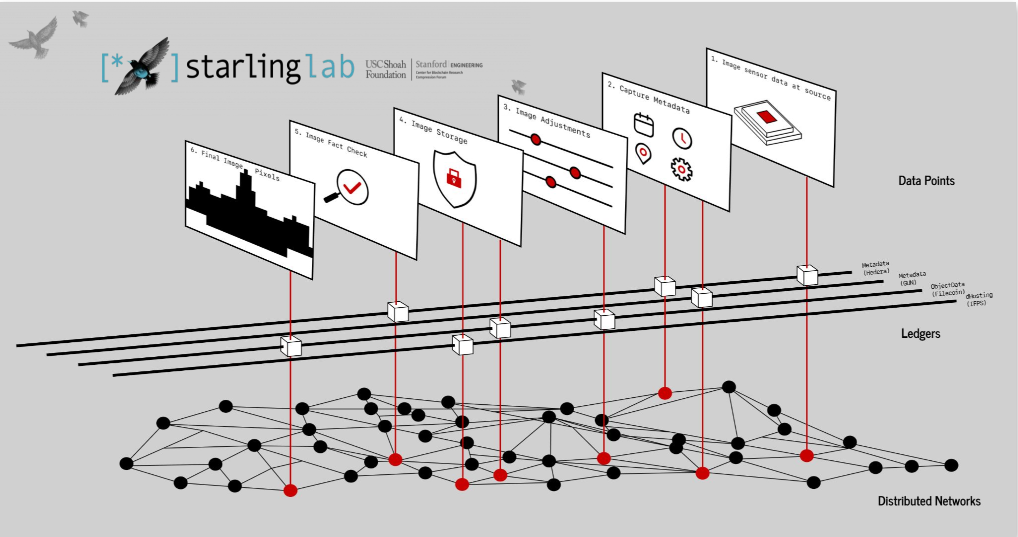
PRODUCED BY Starling Labs

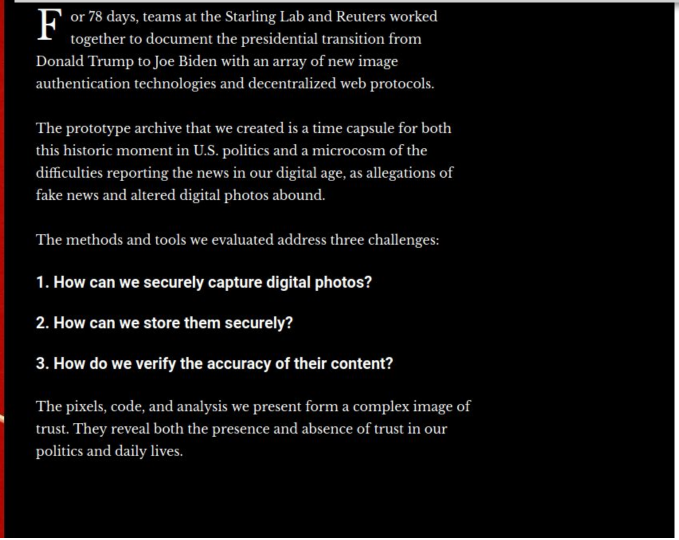
PRODUCED WITH Photoshop Ps

Edits and activity

Import

View more





For 78 days, teams at the Starling Lab and Reuters worked together to document the presidential transition from Donald Trump to Joe Biden with an array of new image authentication technologies and decentralized web protocols.

The prototype archive that we created is a time capsule for both this historic moment in U.S. politics and a microcosm of the difficulties reporting the news in our digital age, as allegations of fake news and altered digital photos abound.

The methods and tools we evaluated address three challenges:

1. How can we securely capture digital photos?

2. How can we store them securely?

3. How do we verify the accuracy of their content?

The pixels, code, and analysis we present form a complex image of trust. They reveal both the presence and absence of trust in our politics and daily lives.

Content Authenticity Initiative

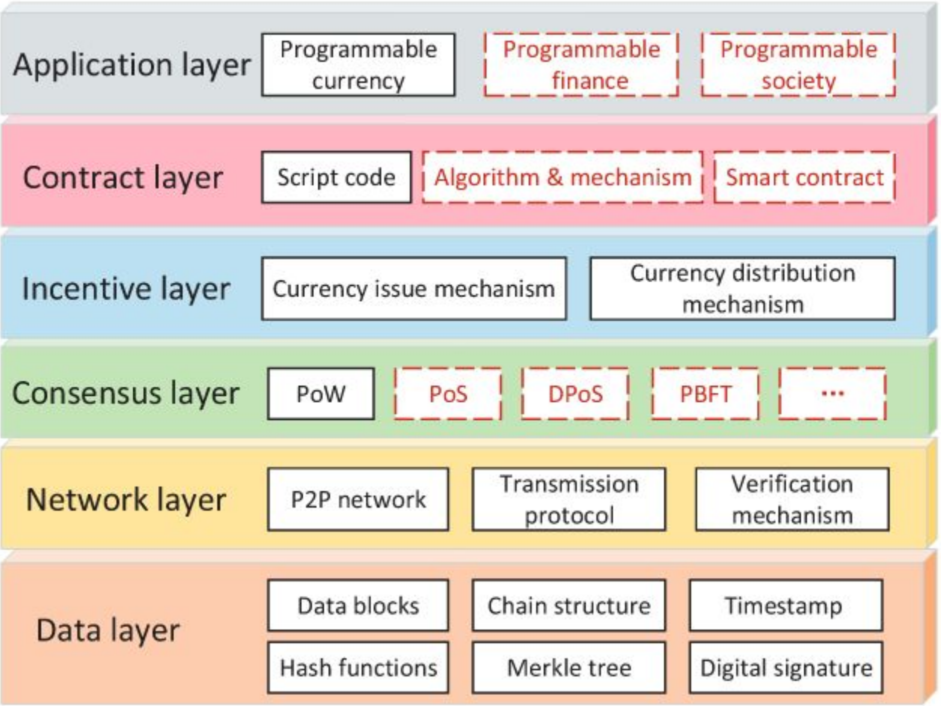
gun

https://www.starlinglab.org/78days/

How can we create web3?

Blockchains

- Publicly available “ledger” of the past
- Append-only, so that history cannot be re-written



Application layer: Programmable currency; Programmable finance; Programmable society

Contract layer: Script code; Algorithm & mechanism; Smart contract

Incentive layer: Currency issue mechanism; Currency distribution mechanism

Consensus layer: PoW; PoS; DPoS; PBFT; ...

Network layer: P2P network; Transmission protocol; Verification mechanism

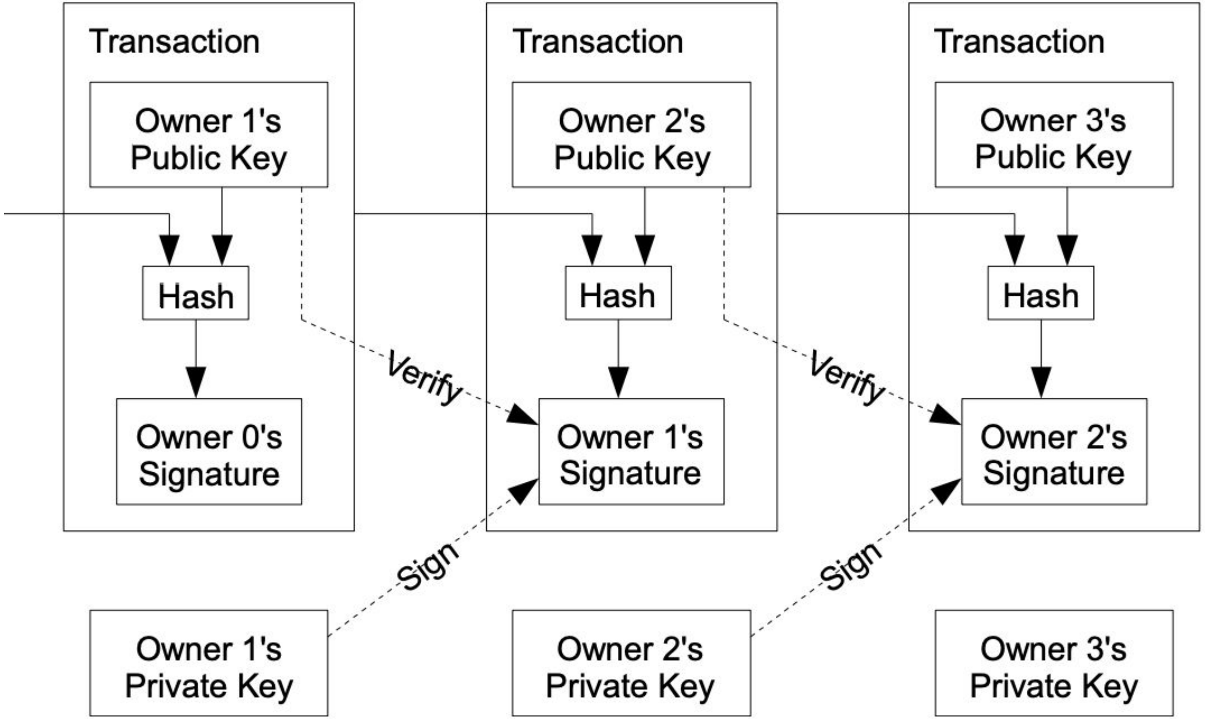
Data layer: Data blocks; Chain structure; Timestamp; Hash functions; Merkle tree; Digital signature

https://dl.acm.org/doi/pdf/10.1145/3316481, page 12

Bitcoin

Bitcoin: Public Key Cryptography

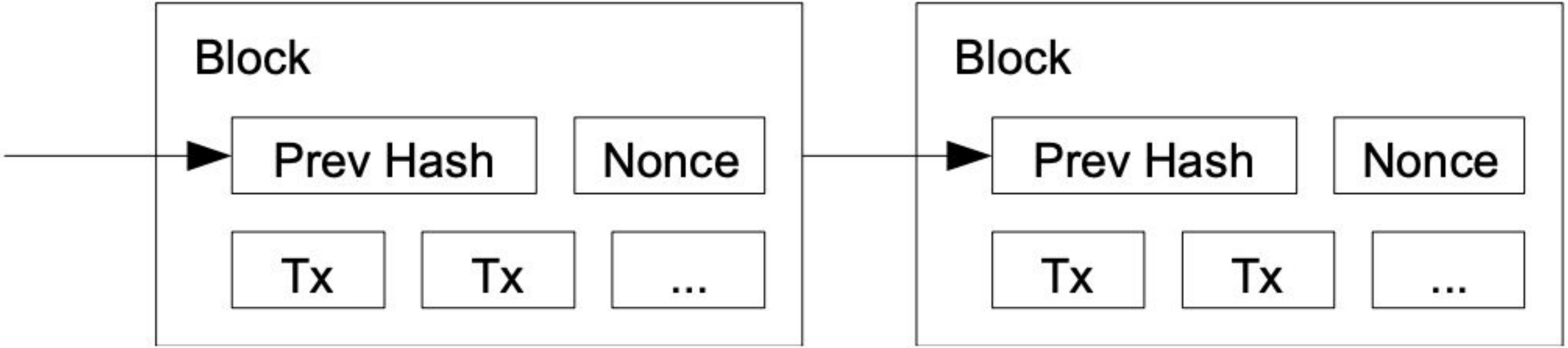
How is ownership transferred and verified?



https://bitcoin.org/bitcoin.pdf

Bitcoin: Solving Double Spending via a Blockchain

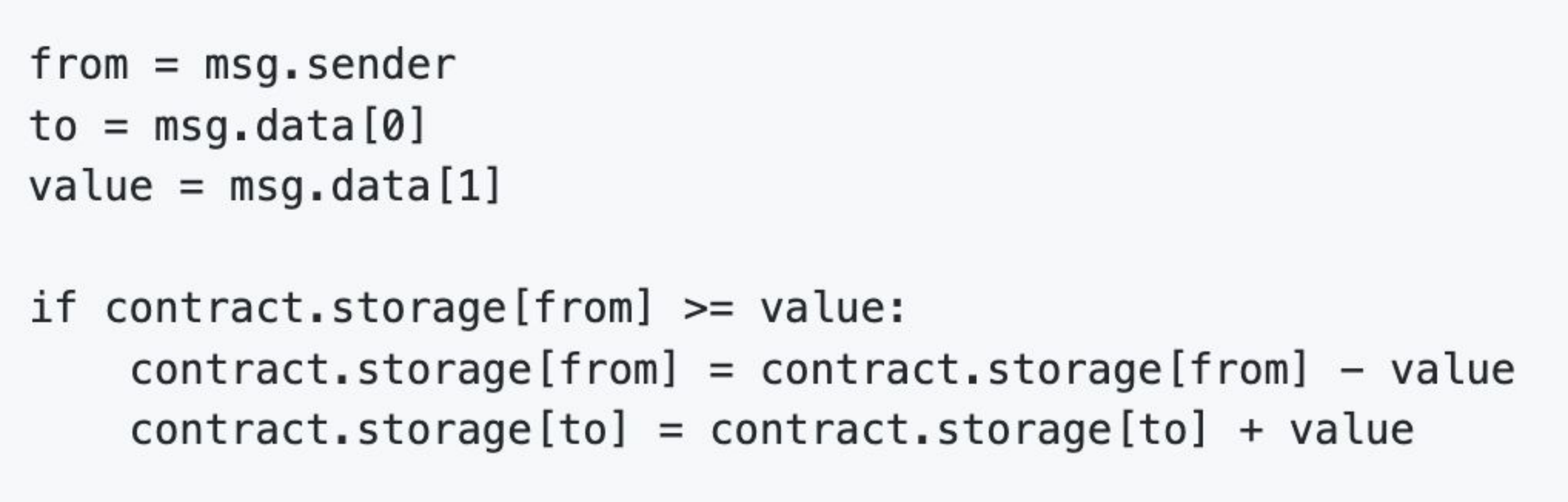
How is the public ledger created and made append-only?



https://bitcoin.org/bitcoin.pdf

Diverse Applications

Ethereum supports “smart contracts” which allow developers to write applications to be stored and executed on the blockchain



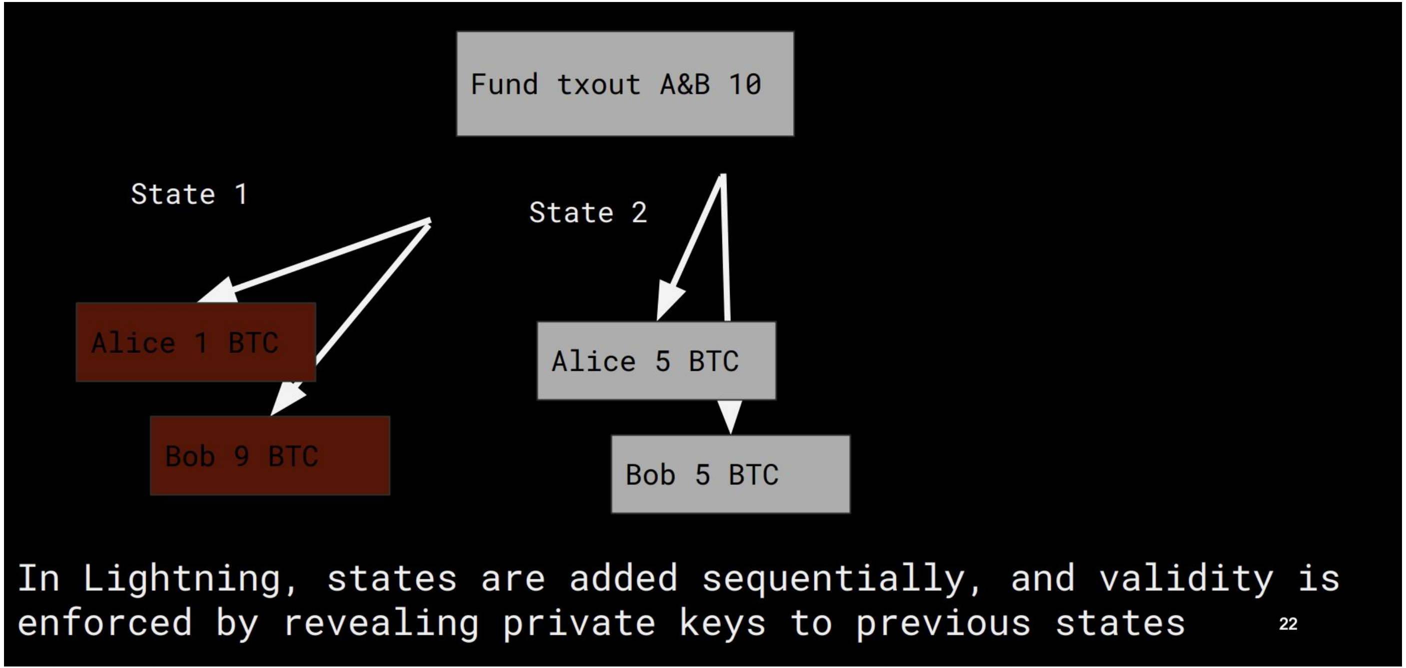
```
from = msg.sender
to = msg.data[0]
value = msg.data[1]

if contract.storage[from] >= value:
    contract.storage[from] = contract.storage[from] – value
    contract.storage[to] = contract.storage[to] + value
```

https://github.com/ethereum/wiki/blob/f83c4692be242ad350bef0c5f8757b7b3c27b2d9/%5BEnglish%5D-White-Paper.md

Scalability

The Bitcoin Lightning Network takes many payments “off chain” to alleviate burden on the blockchain



In Lightning, states are added sequentially, and validity is enforced by revealing private keys to previous states

https://ocw.mit.edu/courses/mas-s62-cryptocurrency-engineering-and-design-spring-2018/resources/lec13-payment-channels-and-lightning-network/

Diversity + Scalability

Polkadot enables interoperability between independent blockchains.

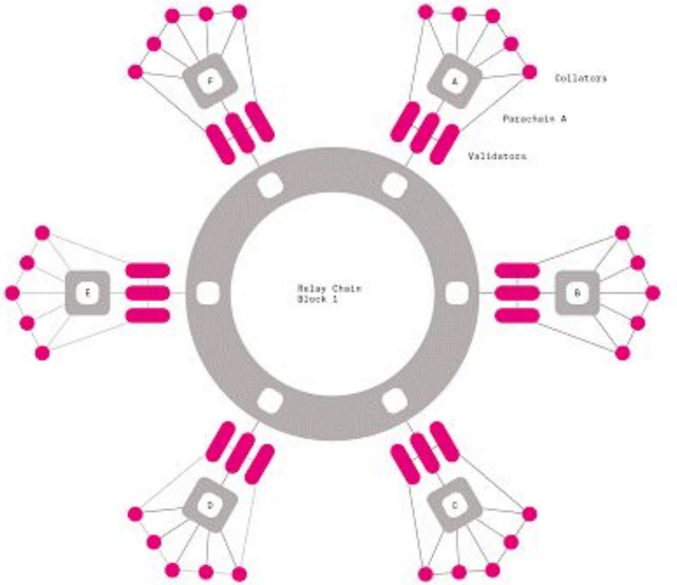
Relaychain

Shared security

Inter Chain Message Passing

Parachain

Blockchain that has own logic



https://techbullion.com/what-is-polkadot/

Consensus Algorithms

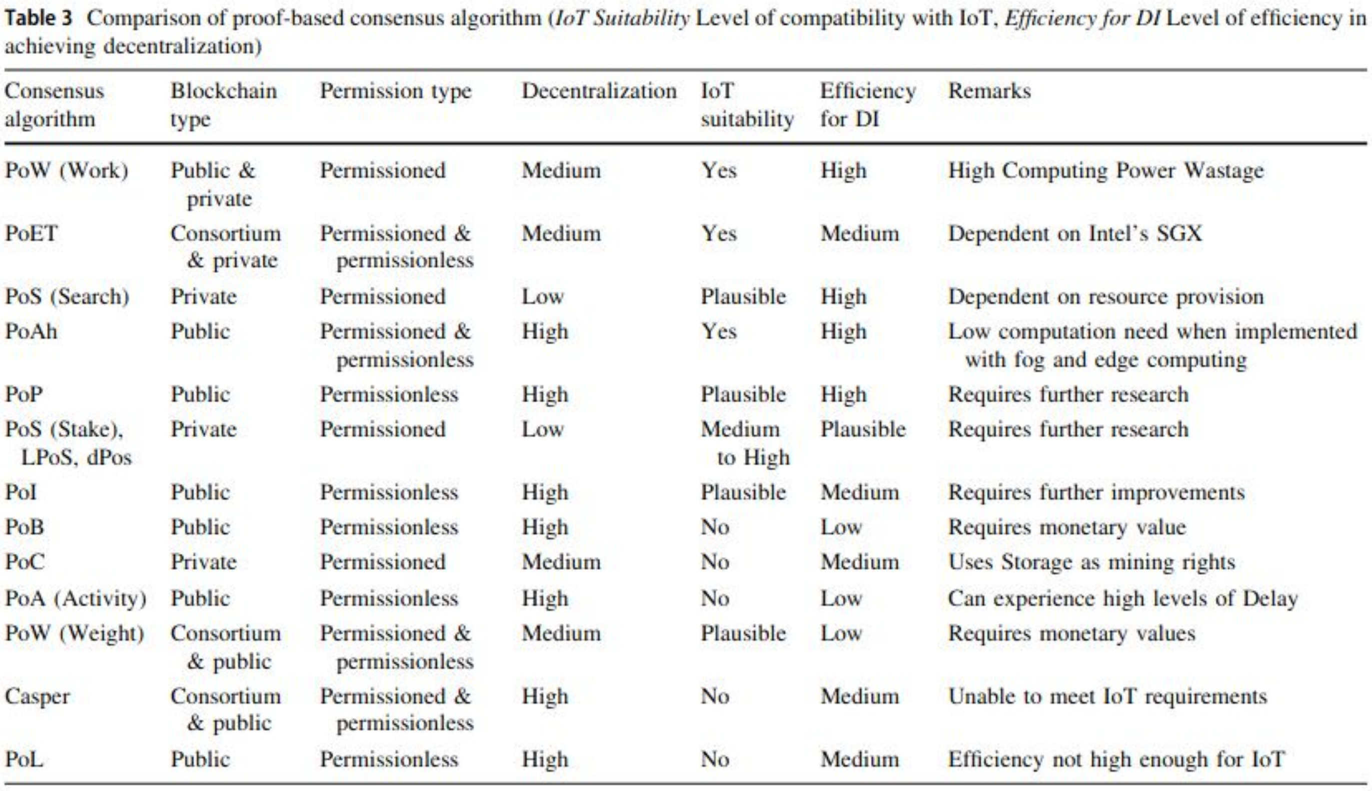


Table 3 Comparison of proof-based consensus algorithm (*IoT Suitability* Level of compatibility with IoT, *Efficiency for DI* Level of efficiency in achieving decentralization)

Consensus algorithm	Blockchain type	Permission type	Decentralization	IoT suitability	Efficiency for DI	Remarks
PoW (Work)	Public & private	Permissioned	Medium	Yes	High	High Computing Power Wastage
PoET	Consortium & private	Permissioned & permissionless	Medium	Yes	Medium	Dependent on Intel's SGX
PoS (Search)	Private	Permissioned	Low	Plausible	High	Dependent on resource provision
PoAh	Public	Permissioned & permissionless	High	Yes	High	Low computation need when implemented with fog and edge computing
PoP	Public	Permissionless	High	Plausible	High	Requires further research
PoS (Stake), LPoS, dPos	Private	Permissioned	Low	Medium to High	Plausible	Requires further research
PoI	Public	Permissionless	High	Plausible	Medium	Requires further improvements
PoB	Public	Permissionless	High	No	Low	Requires monetary value
PoC	Private	Permissioned	Medium	No	Medium	Uses Storage as mining rights
PoA (Activity)	Public	Permissionless	High	No	Low	Can experience high levels of Delay
PoW (Weight)	Consortium & public	Permissioned & permissionless	Medium	Plausible	Low	Requires monetary values
Casper	Consortium & public	Permissioned & permissionless	High	No	Medium	Unable to meet IoT requirements
PoL	Public	Permissionless	High	No	Medium	Efficiency not high enough for IoT

https://link.springer.com/article/10.1007/s10586-021-03301-8/tables/3

Privacy

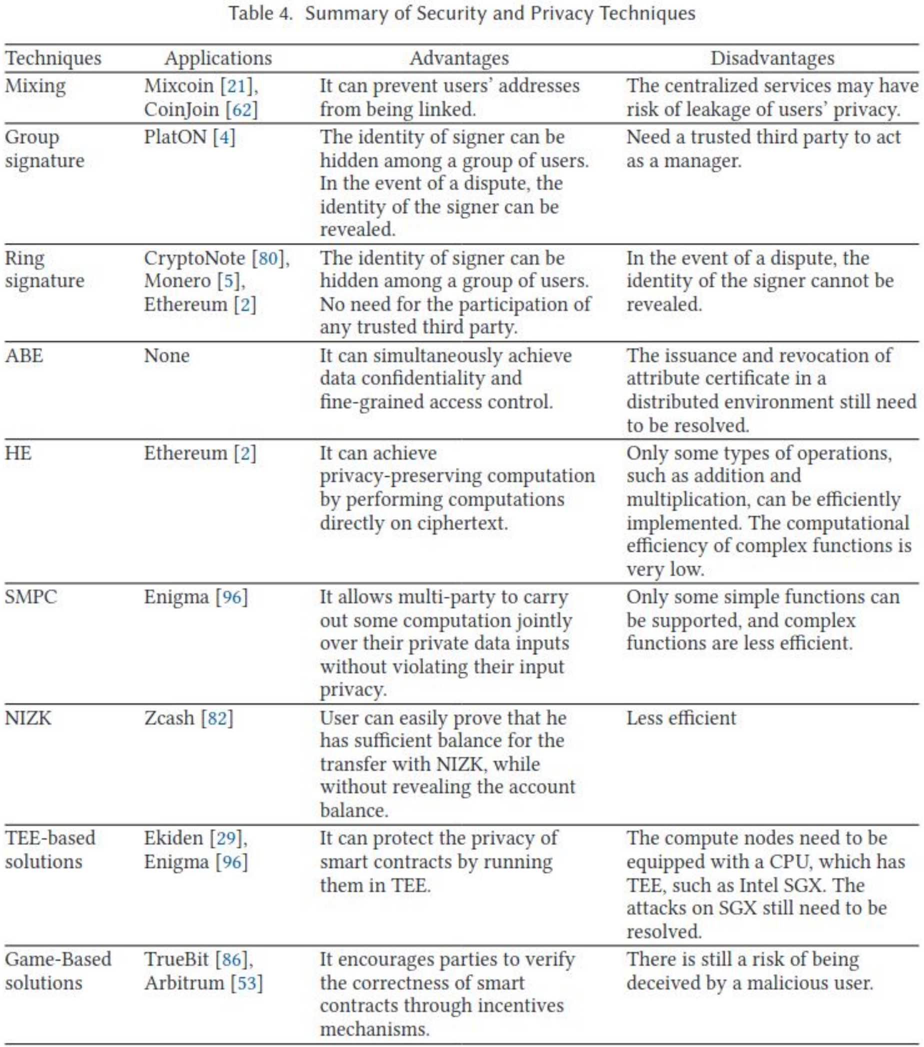


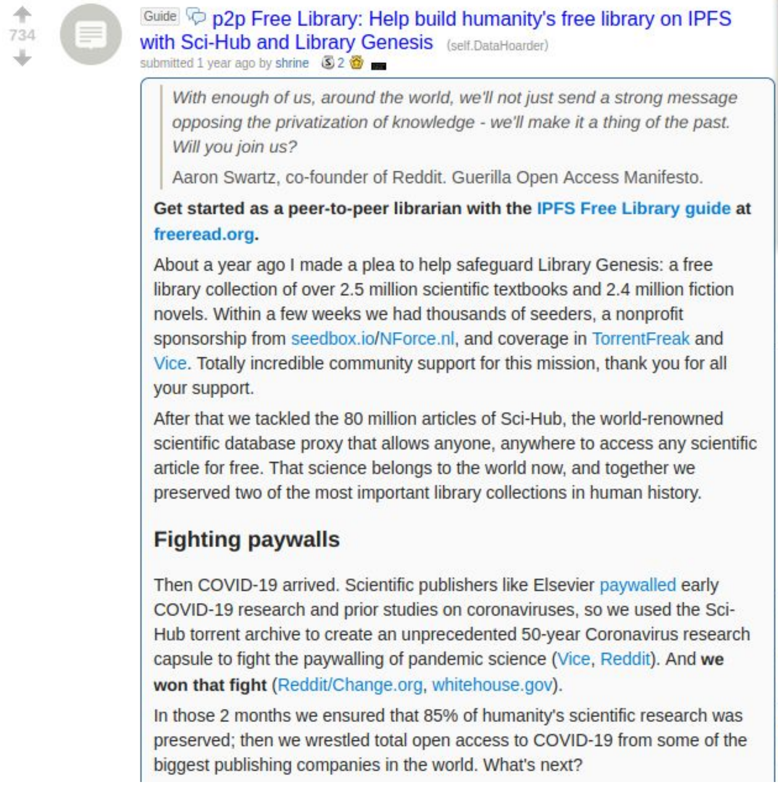
Table 4. Summary of Security and Privacy Techniques

Techniques	Applications	Advantages	Disadvantages
Mixing	Mixcoin [21], CoinJoin [62]	It can prevent users' addresses from being linked.	The centralized services may have risk of leakage of users' privacy.
Group signature	PlatON [4]	The identity of signer can be hidden among a group of users. In the event of a dispute, the identity of the signer can be revealed.	Need a trusted third party to act as a manager.
Ring signature	CryptoNote [80], Monero [5], Ethereum [2]	The identity of signer can be hidden among a group of users. No need for the participation of any trusted third party.	In the event of a dispute, the identity of the signer cannot be revealed.
ABE	None	It can simultaneously achieve data confidentiality and fine-grained access control.	The issuance and revocation of attribute certificate in a distributed environment still need to be resolved.
HE	Ethereum [2]	It can achieve privacy-preserving computation by performing computations directly on ciphertext.	Only some types of operations, such as addition and multiplication, can be efficiently implemented. The computational efficiency of complex functions is very low.
SMPC	Enigma [96]	It allows multi-party to carry out some computation jointly over their private data inputs without violating their input privacy.	Only some simple functions can be supported, and complex functions are less efficient.
NIZK	Zcash [82]	User can easily prove that he has sufficient balance for the transfer with NIZK, while without revealing the account balance.	Less efficient
TEE-based solutions	Ekiden [29], Enigma [96]	It can protect the privacy of smart contracts by running them in TEE.	The compute nodes need to be equipped with a CPU, which has TEE, such as Intel SGX. The attacks on SGX still need to be resolved.
Game-Based solutions	TrueBit [86], Arbitrum [53]	It encourages parties to verify the correctness of smart contracts through incentives mechanisms.	There is still a risk of being deceived by a malicious user.

https://dl.acm.org/doi/pdf/10.1145/3316481

What’s next?

Dark Web



Guide p2p Free Library: Help build humanity's free library on IPFS with Sci-Hub and Library Genesis (self.DataHoarder)

submitted 1 year ago by shrine 2

> *With enough of us, around the world, we'll not just send a strong message opposing the privatization of knowledge - we'll make it a thing of the past. Will you join us?*
>
> Aaron Swartz, co-founder of Reddit. Guerilla Open Access Manifesto.

Get started as a peer-to-peer librarian with the IPFS Free Library guide at freeread.org.

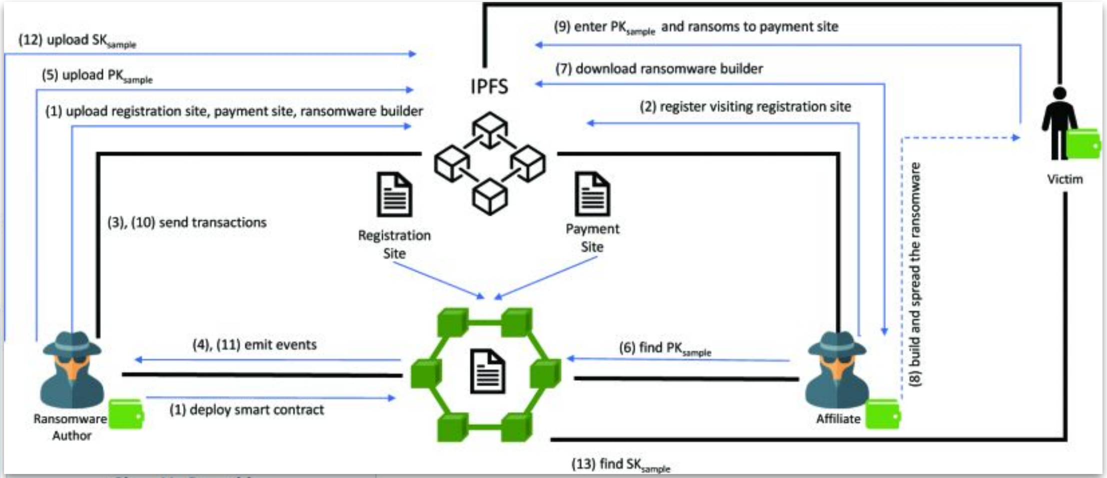
About a year ago I made a plea to help safeguard Library Genesis: a free library collection of over 2.5 million scientific textbooks and 2.4 million fiction novels. Within a few weeks we had thousands of seeders, a nonprofit sponsorship from seedbox.io/NForce.nl, and coverage in TorrentFreak and Vice. Totally incredible community support for this mission, thank you for all your support.

After that we tackled the 80 million articles of Sci-Hub, the world-renowned scientific database proxy that allows anyone, anywhere to access any scientific article for free. That science belongs to the world now, and together we preserved two of the most important library collections in human history.

Fighting paywalls

Then COVID-19 arrived. Scientific publishers like Elsevier paywalled early COVID-19 research and prior studies on coronaviruses, so we used the Sci-Hub torrent archive to create an unprecedented 50-year Coronavirus research capsule to fight the paywalling of pandemic science (Vice, Reddit). And **we won that fight** (Reddit/Change.org, whitehouse.gov).

In those 2 months we ensured that 85% of humanity's scientific research was preserved; then we wrestled total open access to COVID-19 from some of the biggest publishing companies in the world. What's next?



(12) upload SK$_{sample}$
(5) upload PK$_{sample}$
(1) upload registration site, payment site, ransomware builder
IPFS
(9) enter PK$_{sample}$ and ransoms to payment site
(7) download ransomware builder
(2) register visiting registration site
Victim
(3), (10) send transactions
Registration Site
Payment Site
(8) build and spread the ransomware
(4), (11) emit events
(6) find PK$_{sample}$
(1) deploy smart contract
Ransomware Author
Affiliate
(13) find SK$_{sample}$

https://doi.org/10.1109/ICBC48266.2020.9169451

DataHoarder

join 610,748 readers

○ 613 users here now

Who are we?

We are digital librarians. Among us are represented the various reasons to keep data -- legal requirements, competitive requirements, uncertainty of permanence of cloud services, distaste for transmitting your data externally (e.g. government or corporate espionage), cultural and familial archivists, internet collapse

https://www.reddit.com/r/DataHoarder/comments/jb1hkn/p2p_free_library_help_build_humanitys_free/

Decentralized storage

Decentralized storage network

Personal Data Stores

Decentralized Communication

[matrix]

Thank you!