HOLISEUM

Blockchains dans la cybersécurité et cybersécurité des blockchains

Lundi de la Cybersécurité – March, 14th 2022

Renaud Lifchitz, Chief Scientific Officer

Version	1.0	Classification	Public

Présentation de l'intervenant

- Expert en sécurité informatique,
  Directeur Scientifique chez Holiseum

- Principales activités:
  - Tests d'intrusion & audits de sécurité
  - Recherche
  - Formations & sensibilisations

- Centres d'intérêt :
  - Sécurité des protocoles (authentification, cryptographie, fuites d'information, preuves à divulgation nulle de connaissance...)
  - Théorie des nombres (factorisation, tests de primalité, courbes elliptiques...)

Holiseum : une vision holistique de la Cybersécurité

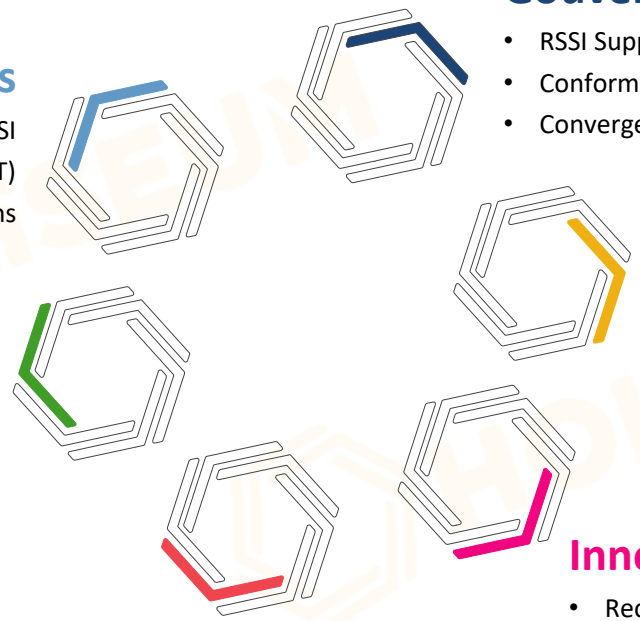
Notre approche globale de la sécurité vise à faire converger les disciplines connexes telles que la sécurité physique et l'intelligence économique afin de mettre en évidence leurs interdépendances et de proposer des réponses de sécurité adaptées aux métiers.
Nous proposons des services sur l'ensemble de la chaîne de valeur des services de cybersécurité, de la gouvernance aux opérations.

Gouvernance

- RSSI Support / as a Service / Starter
- Conformité Réglementaire (LPM / NIS)
- Convergence Cybersécurité et Sûreté

Opérations

- Back-office opérationnel du RSSI
- Réponse à incidents et forensics (CSIRT)
- Exploitation et MCS de solutions



Audits

- Audits 360° : organisation / technique / physique / humain
- Audits et Pentests

Remédiation

- Cadrage et pilotage de projets de sécurisation et/ou de mise en conformité
- Sécurisation des SI de sûreté (vidéo surveillance, Contrôle d'Accès, Anti-intrusion, etc.)
- Formations et Sensibilisations

Innovation (R&D)

- Recherche & Développement
- Tests et qualifications de solutions (POC)

Solutions

- Intégrations de solutions de Cybersécurité
- Ingénierie d'offres de services

Ils nous font confiance

ENGIE · TOTAL · GRTgaz · EDF · BOUYGUES · LVMH MOËT HENNESSY • LOUIS VUITTON · SOCIETE GENERALE · CRÉDIT AGRICOLE IMMOBILIER

Nos partenaires

SAMSIC SECURITE · HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY · EXERA · EDHEC BUSINESS SCHOOL · utc SORBONNE UNIVERSITES · AN2V

Introduction

« Blockchains are known for their financial applications, which unfortunately often overshadows many of their other interests. We will focus here on the principles, techniques and concrete blockchain projects that bring a real interest from a confidentiality, integrity, availability or authentication point of view. Thus, properly used blockchains allow to drastically reduce single points of failure ("SPoF"), to decrease our dependency on the cloud or to reduce our infrastructure costs, by relying on existing decentralized networks where costs are shared. Many techniques democratized by blockchains are also under-exploited in cybersecurity (security proofs, protocol proofs, "zero-knowledge" proofs, ...) and could see a boom in our next software developments. Blockchains can also be a great tool for digital sovereignty by allowing us to get away from centralized foreign actors that we permanently trust (certification authorities, DNS root servers, ICANN, RIPE ...) »

Outline

1. Why a blockchain?
2. Resilience
3. Electronic notary
4. Confidentiality

01 Why a blockchain?

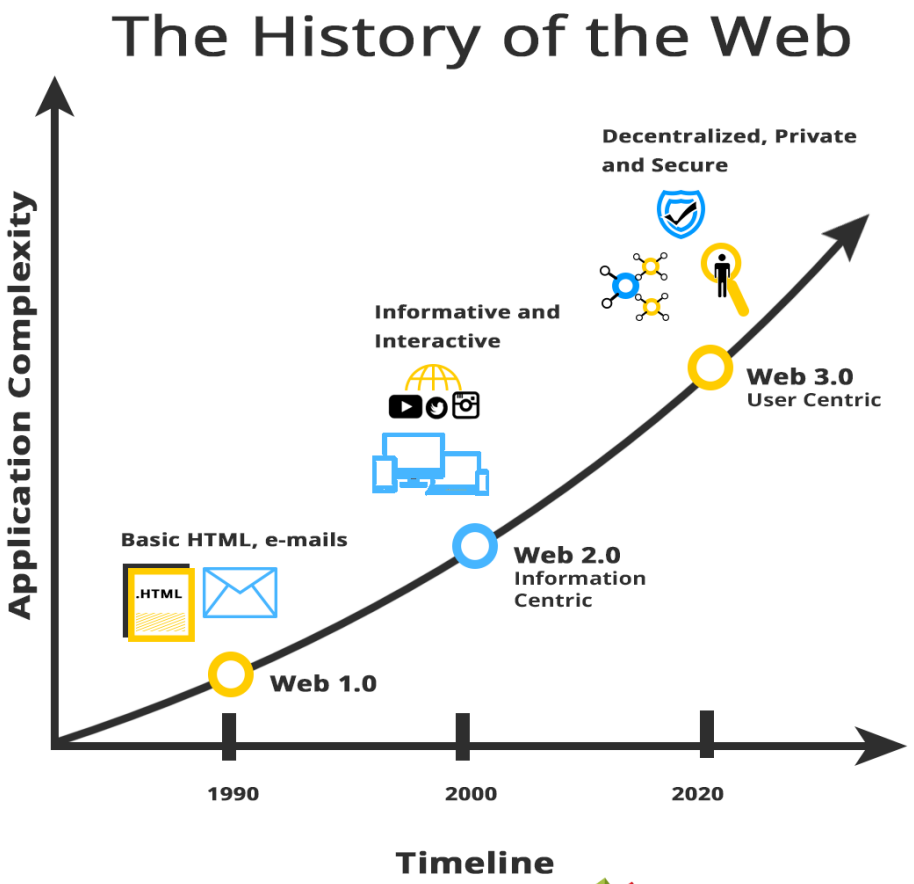
HOLISEUM

01. Why a blockchain? (1/2)

- The Web has been designed to be decentralized BUT…
  - It’s more and more centralized: Google, Apple, Amazon, Microsoft, …
  - That makes the spying and data leaks easier
  - A single server is not enough even to serve a single popular Youtube video
  - Hosting changes ⇨ URLs are broken
  - A lot of DDoS attacks succeed
  - Load balancing is complex, costly, depends on the web technologies involved: efficient DDoS protection is hard

01. Why a blockchain? (2/2)

- A blockchain is like a trusted third party, without requiring any trust!
- « Zero Trust » security model: avoid unnecessary trust
- Benefits of blockchain applications:
  - Scalable since the beginning
  - Redundant
  - DoS & DDoS resistant
  - No downtime
  - Censorship resistant
  - Fault tolerant



101 Blockchains
Created by 101blockchains.com

01. Examples of well-known everyday centralized actors

- Root DNS (DNS nameservers)
- ICANN (IP blocks and AS numbers)
- RIPE (EU based)
- Most SSL/TLS/PKI certification authorities

☞ The USA controls almost the entire Internet:

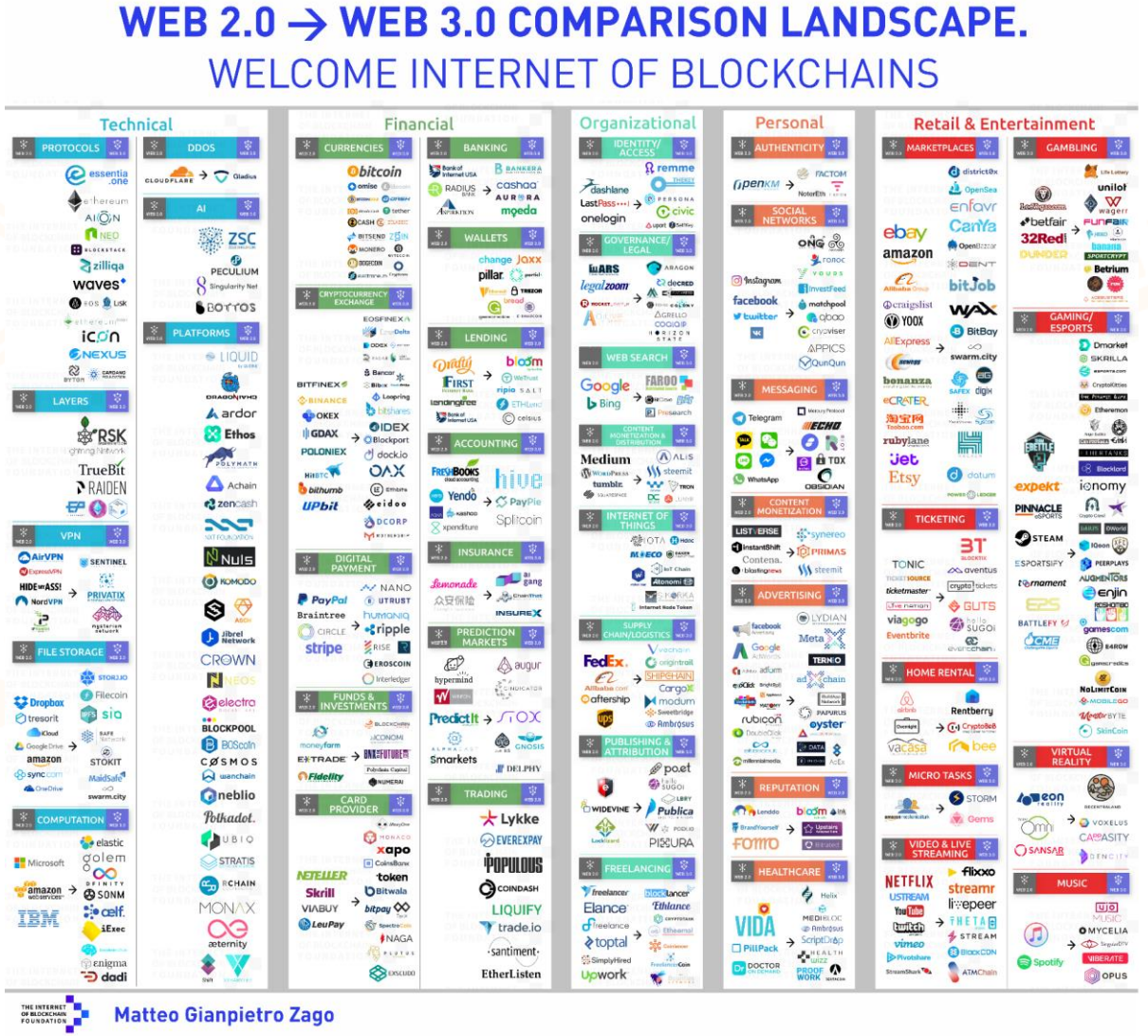
- Absolutely no Internet sovereignty for other countries
- A lot of centralized Single Points of Failure (« SPoF »)
- « Cloud Act » gives USA the access to most data in the world
- Outstanding control of the CAs market share

Rank	Issuer	Usage	Market share
1	IdenTrust	45.0%	52.7%
2	DigiCert	16.5%	19.3%
3	Sectigo	14.3%	16.8%
4	GoDaddy	5.5%	6.4%
5	GlobalSign	2.2%	2.6%
6	Let's Encrypt	1.6%	1.8%
7	Certum	0.4%	0.5%
8	Secom	0.2%	0.2%
9	Entrust	0.2%	0.2%
10	Actalis	0.1%	0.1%
11	E-Tugra	0.1%	0.1%
12	WISeKey Group	< 0.1%	0.1%
13	Deutsche Telekom	< 0.1%	0.1%
14	Network Solutions	< 0.1%	0.1%

Top Certification Authorities
(https://en.wikipedia.org/wiki/Certificate_authority)
Top 4 are US-based and account for more than 80% usage and 95% market share

01. Are fully decentralized application possible? (1/2)

- Are fully decentralized application possible?
- Several parts should be decentralized:
  - Back end (core logic/app)
  - Web front end (storage of HTML/JS/CSS)
  - Domain name (storage and resolver)
- It is little known that full decentralized web applications already exist thanks to blockchains and Web 3.0!



01. Are fully decentralized application possible? (2/2)

Requirements to use a decentralized application:

- Network access:
  - through P2P / blockchain node (can be a light node)
  - or public gateway (HTTP/HTTPS)
- Client application:
  - Browser (native) or with extension
  - or heavy client

02 Resilience

HOLISEUM

02. Decentralized domain names

- Goal: provide both the storage of the registry and the resolver logic in a decentralized way
- A domain name is nothing more than a Non-Fungible Token (« NFT »)
- 2 main projects:
  - Ethereum Name Service - ENS (https://ens.domains/):
    - Oldest provider, works on Ethereum blockchain only (https://www.ethernodes.org/)
    - Limited time ownership of domains
  - Unstoppable Domains (https://unstoppabledomains.com/):
    - Newest provider, adds some other blockchain support
    - Lifetime ownership of domains

- Native support under browsers like Opera and Brave (Chrome-based), otherwise throught a web extension
- Domain names can be used for websites or individual crypto wallets
- Can work with IPFS decentralized storage (« InterPlanetary File System ») through IPNS
- Unlike normal domain names, ownership of domains can be transferred without any third party consent

02. Decentralized storage

Key advantages compared to public cloud providers:

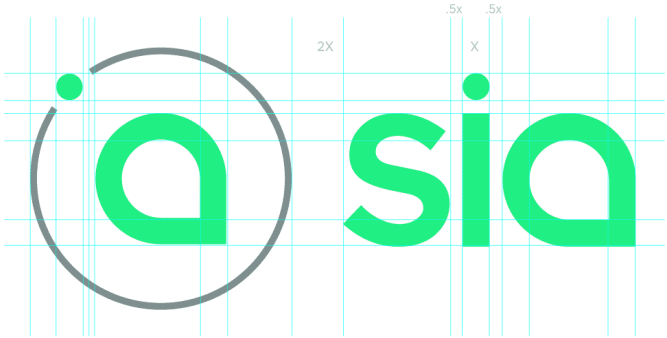
- Redundancy
- Cost up to 20x cheaper
- No SPoF
- Near 100% SLA (« Service Level Agreement »)
- May provide native confidentiality/encryption
- May provide permanent storage for a one-time fee

02. Decentralized storage: IPFS

- All content is adressed by a hash: no more broken URLs!
- Content is de-duplicated on a given hoster
- MPEG streaming over IPFS over HTTP/HTTPS is native in all browsers: music and video sharing is easy
- Content should be voluntarily « pinned » by nodes, can be incentivized (Filecoin)
- Example (same content, transparent HTTPS, different entry point):
  - https://ipfs.io/ipfs/QmcniBv7UQ4gGPQQW2BwbD4ZZHzN3o3tPuNLZCbBchd1zh
  - https://gateway.pinata.cloud/ipfs/QmcniBv7UQ4gGPQQW2BwbD4ZZHzN3o3tPuNLZCbBchd1zh
  - http://ipfs.localhost:8080/ipfs/QmcniBv7UQ4gGPQQW2BwbD4ZZHzN3o3tPuNLZCbBchd1zh
- Some public gateways (Cloudflare officially hosts one): https://ipfs.github.io/public-gateway-checker/
- Project page: https://ipfs.io/
- Wikipedia page: https://en.wikipedia.org/wiki/InterPlanetary_File_System

02. Decentralized storage: Sia

- Peer-to-peer marketplace that provides storage for a custom duration and redundancy requirements
- Security by design:
  - Everything is always encrypted, the space provider never knows what it hosts
  - Data is redundant by default
- Multimedia streaming is possible
- As of September 2021:
  - Storage Capacity: 4.0 PB
  - Storage Providers: 649
  - Used Storage: 1698 TB

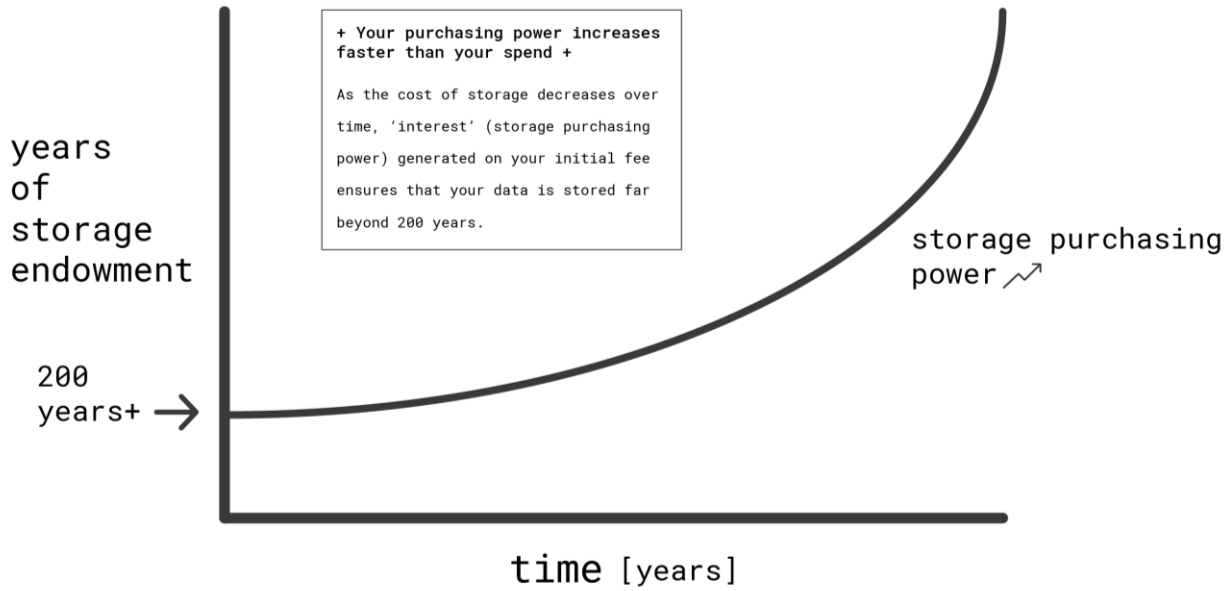


- Project page: https://sia.tech/
- Even provides a decentralized public cloud storage: https://siasky.net/

02. Decentralized storage: Arweave (1/2)

- Unlimited time (permanent) storage for a onetime fee!
- Called « the permaweb »
- A browser extension is available to archive any web content
- Has its own blockchain and token ($AR), token can be mined
- Miners must provide a « Proof of Access » to old data in order to add new blocks

arweave.org



02. Decentralized storage: Arweave (2/2)

arweave.org

- Arweave gateways are able to enforce their own content policy
- Partners with the Internet Watch Foundation (https://www.iwf.org.uk/) to keep the permaweb safe from abusive material
- Public block explorer: https://viewblock.io/arweave
- A layer of encryption can be added for applications with privacy:
  - Ardrive (https://ardrive.io/): fully private personal cloud storage
  - Weavemail (https://github.com/ArweaveTeam/weavemail): fully private mail application
- Project page: https://www.arweave.org/

02. Decentralized storage: other projects

Other similar and interesting projects:

- Filecoin (https://filecoin.io/): incentivized file storage
- StorJ (https://www.storj.io/)
- Aleph.im (https://aleph.im/): cross-blockchain storage

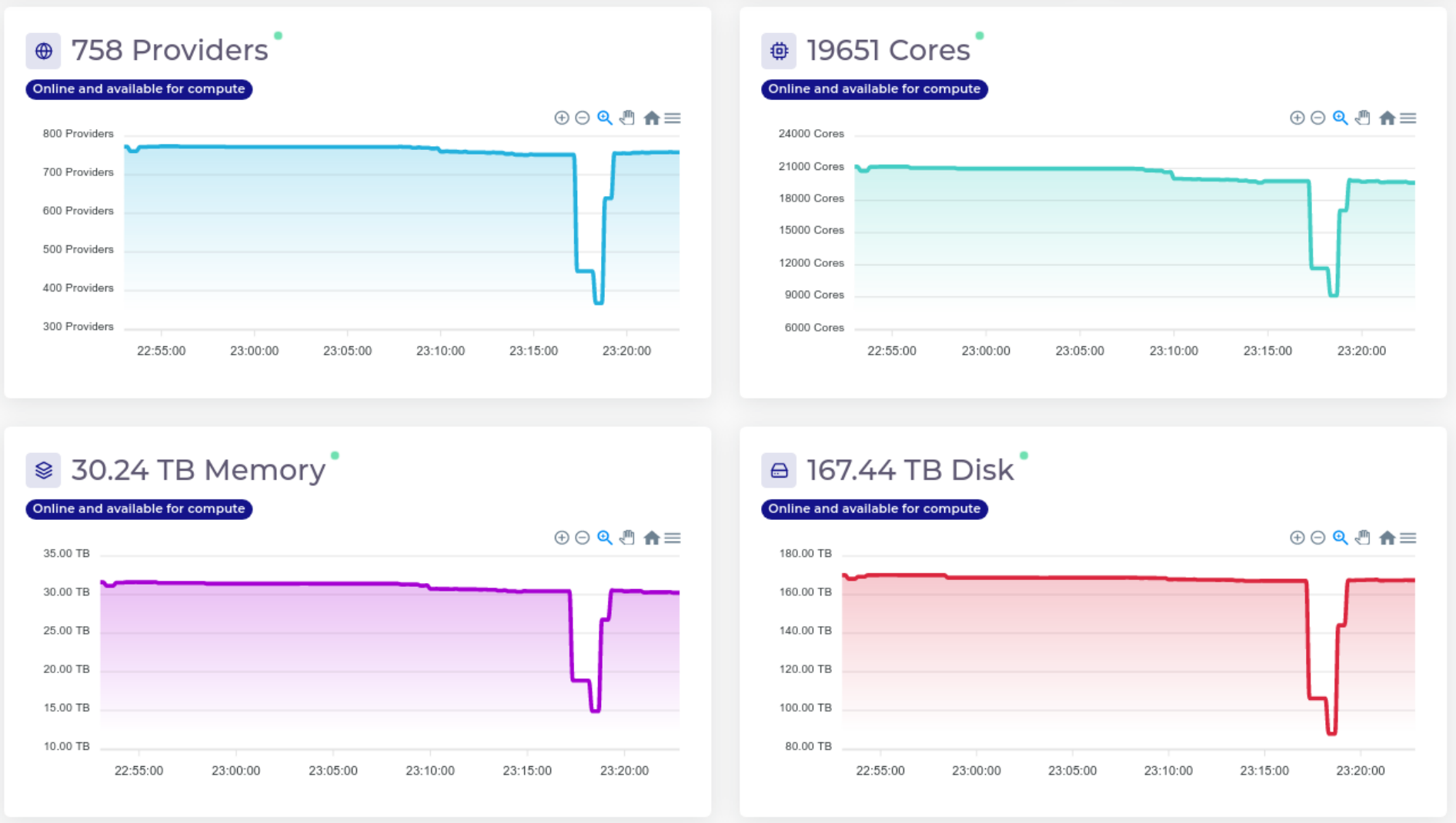
02. Decentralized computing (1/2)

Two main projects:

- Golem (https://www.golem.network/)
- iExec (https://iex.ec/)

- Marketplaces with computing power sellers and buyers
- Provide a complete framework for contained execution:
  - Containers (Docker)
  - Webassembly (WASM) programs for portability
- Provides a TEE SDK for confidential computing on TEE enclaves

02. Decentralized computing (2/2)

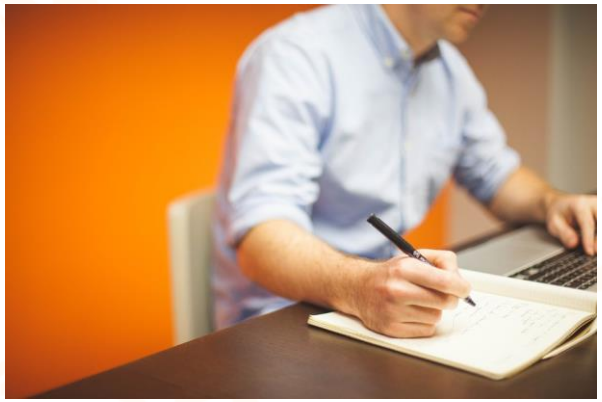


Golem network, as of September 7th, 2021

03 Electronic notary

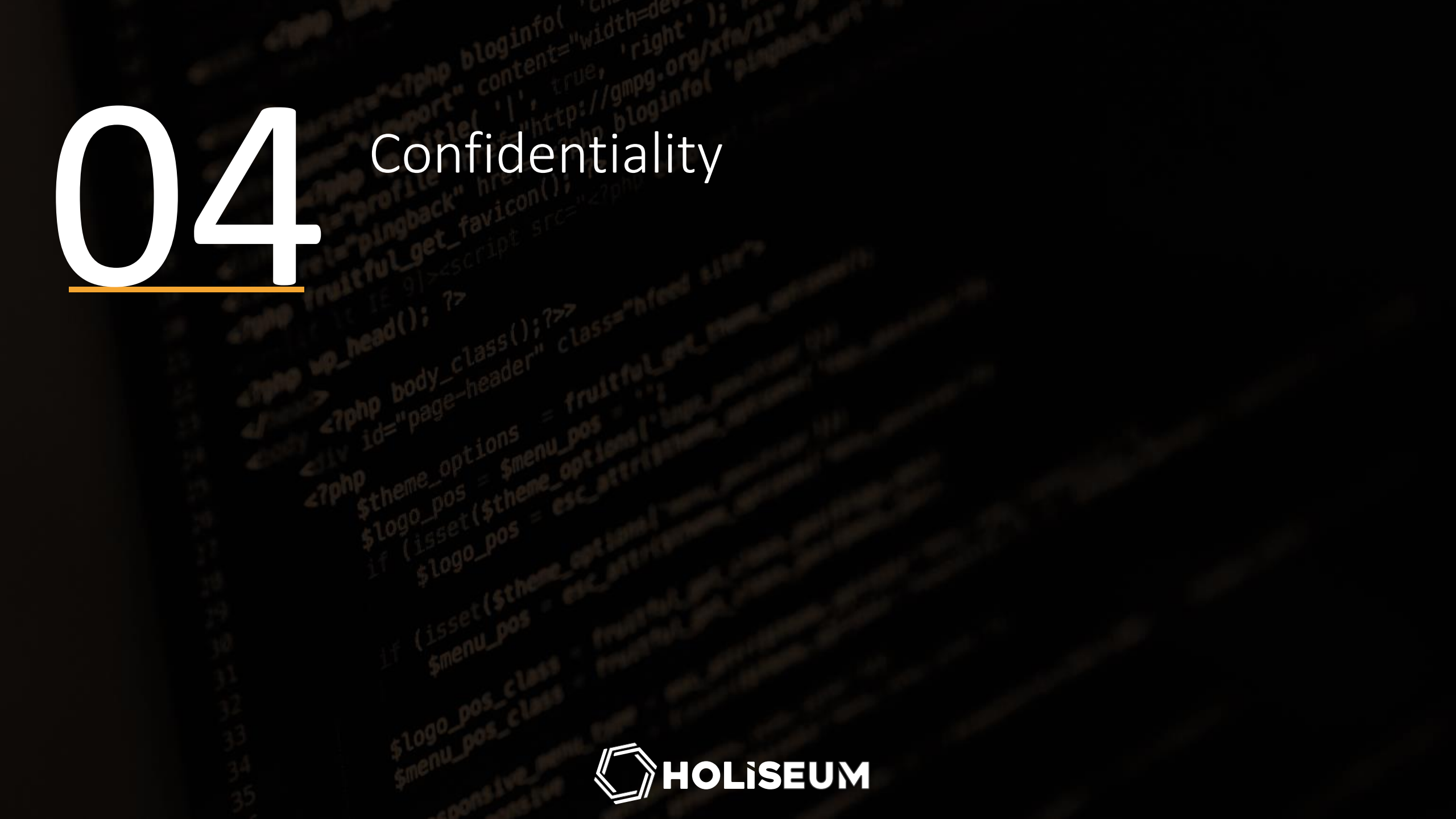
HOLISEUM

03. What is electronic notary?



- Digital Signature
- Thanks to blockchain block timestamping:
  - Anchoring at a given time
  - Electronic seals
  - Proof of Existence
  - Proof of Precedence: useful for Intellectual Property
- Fully scalable thanks to Merkle trees (https://en.wikipedia.org/wiki/Merkle_tree)
- Interesting project: Woleet (https://www.woleet.io/)
  - Any file can be anchored (only the hash is anchored) on the Bitcoin blockchain
  - Open specifications and file formats
  - API available
  - Anybody can verify a proof: https://auditor.woleet.io/

04 Confidentiality



04. Zero-knowledge proofs (“ZKP”)

- One prover, one or several verifiers
- A goal: prove any computation of the prover with public and private parameters to the verifier
- 3 basic properties:
  - **Completeness**: if the statement is true, the verifier will be convinced
  - **Soundness**: Cheating is not possible, or with very small probability
  - **Zero-knowledge**: the verifier doesn’t learn anything else than if the statement is true
- Many interests (« secure computation »):
  - Data integrity
  - Computation integrity
  - Confidentiality
- May be used with homomorphic encryption
- Many kinds of ZKP: interactive/not interactive, with/without trusted setup, quantum resistant or not
- Can be used for electronic voting

04. Confidentiality

Interesting blockchain projects:

- Ocean (https://oceanprotocol.com/):

  Marketplace to buy, sell and manage data in a privacy-preserving way

- NuCypher (https://www.nucypher.com/):

  Provides a secure computation framework :
  Fully Homomorphic Encryption and dynamic access control through proxy re-encryption

- Secret Network (https://scrt.network/):

  brings privacy to smart contracts, asset transfers and associated business data

- Mina (https://minaprotocol.com/):

  fixed-size blockchain (22kB) thanks to recursive ZKP, private smart contracts

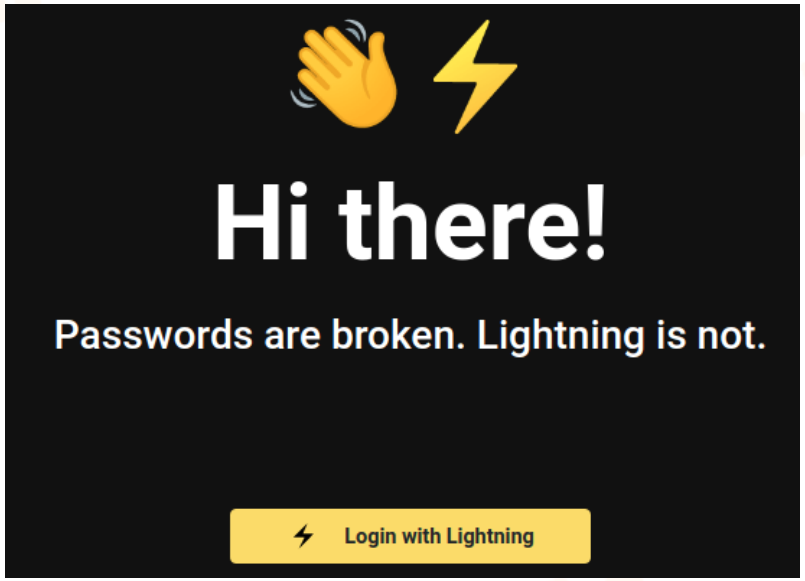
05 Authentication & Trust

HOLISEUM

05. Authentication & Trust

Bitcoin Lightning for strong authentication without any password!

- LN-AUTH-URL protocol
  (https://github.com/fiatjaf/lnurl-rfc/blob/legacy/lnurl-auth.md)
- Many benefits:
  - Strong authentication (I have+I know or I have+I am)
  - No more passwords!
  - Privacy protection (absolutely no personal data)
  - Active protection against phishing



- Demo: https://lightninglogin.live/
  (Use a Phoenix wallet https://phoenix.acinq.co/ on your smartphone, even empty.
  Also exists as a web extension)

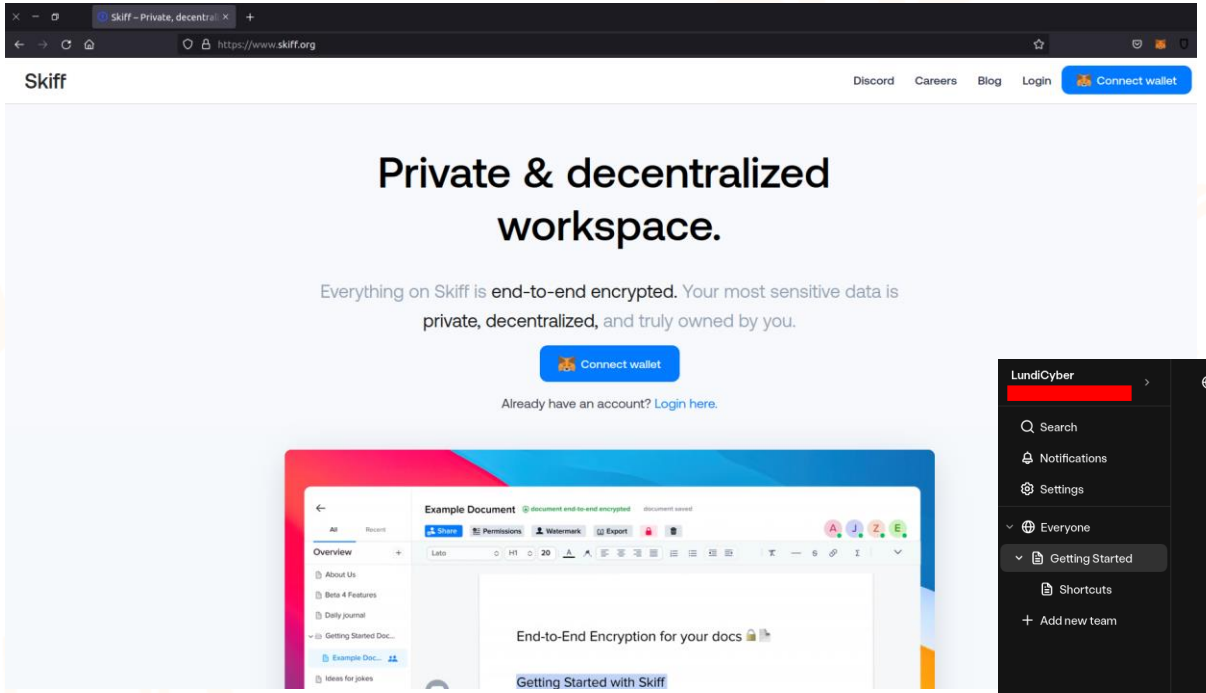
05. The ultimate combo: authentication, trust, privacy and decentralization! (1/2)

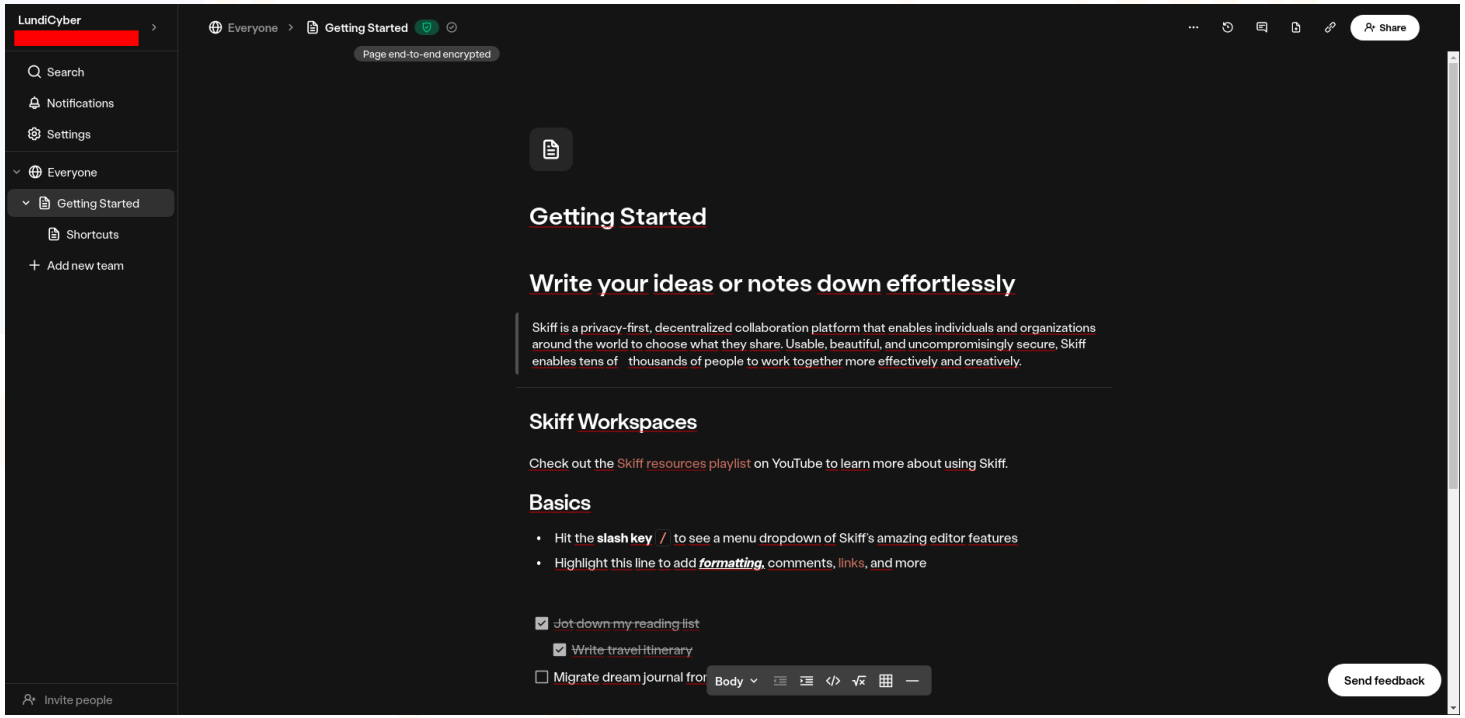
Skiff is a complete groupware, office and worksuite solution (« like Google Workspace »)

- Authentication using an Ethereum compatible wallet
  (no personal data asked): strong authentication, no password leaks!
- End-to-end encrypted:
  fully private even if the hosting company is compromised
- Fully decentralized if needed using IPFS
  (on premise backup still possible)

https://www.skiff.org/

05. The ultimate combo: authentication, trust, privacy and decentralization! (2/2)





Nos savoir-faire blockchain & cybersécurité

- Accompagnement à la conception et mise en œuvre de solutions blockchain
- Analyse des risques techniques et juridiques
- Formation aux technologies blockchain
- Audit de primitives cryptographiques
- Audits sécurité d'applications décentralisée et de smart contracts

HOLISEUM

Faïz DJELLOULI
Président & Co-Fondateur
+33 6 69 72 29 64 | faiz.djellouli@holiseum.com

An NGUYEN
Directeur Général & Co-Fondateur
+33 6 98 84 39 97 | an.nguyen@holiseum.com

Questions / réponses !

renaud.lifchitz@holiseum.com

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Holiseum est membre de Hexatrust, groupement français de la Cybersécurité et du Cloud de confiance

HOLISEUM

Faïz DJELLOULI
Président & Co-Fondateur
+33 6 69 72 29 64 | faiz.djellouli@holiseum.com

An NGUYEN
Directeur Général & Co-Fondateur
+33 6 98 84 39 97 | an.nguyen@holiseum.com