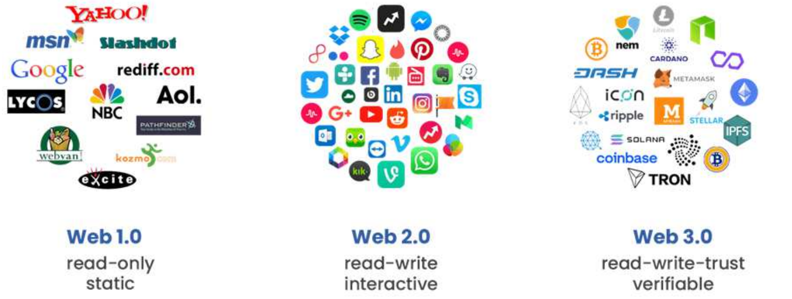
Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής

Ευφυή Κινητά Δίκτυα: Web 3 (& 4, 5), Digital wallets-identities-credentials

Εαρινό Εξάμηνο 2024-25

Βασίλειος Σύρης

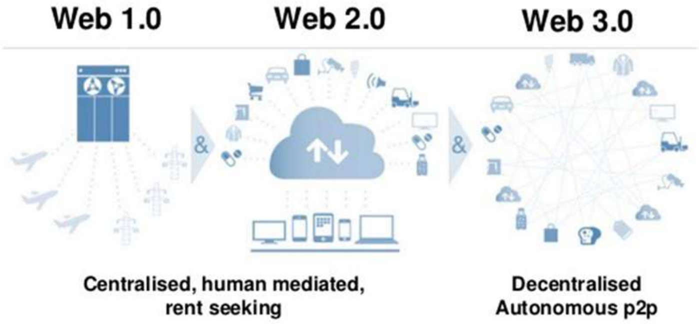
Web 1.0, Web 2.0, Web 3.0



Source: Myraah

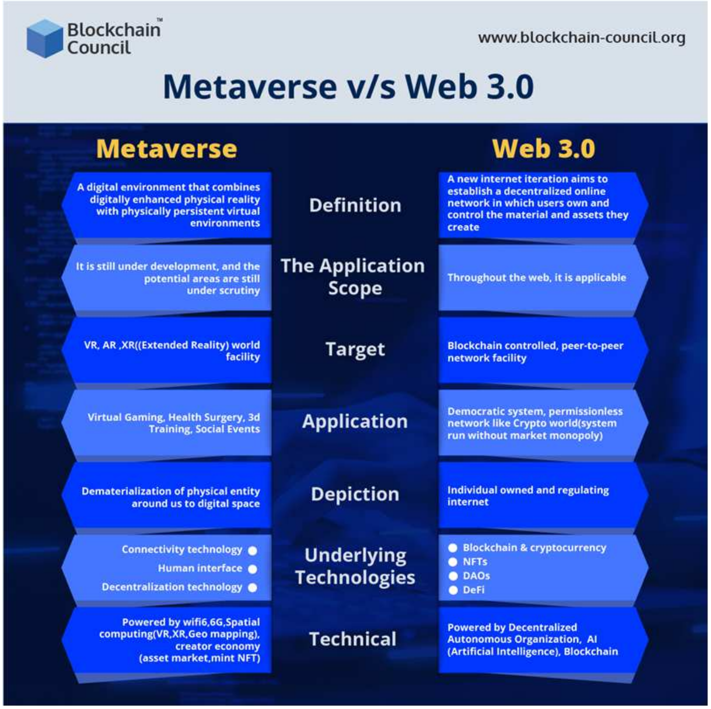
- Web 2.0 had Server-side (programs executed on a server) and Client-side (programs executed in a browser) programming
- Web 2.0: user generated content and social media, but centralized control
- Web 3.0: decentralized, trust and verifiable

Centralization - decentralization


Web 1.0
Web 2.0
Web 3.0
&
&
Centralised, human mediated, rent seeking
Decentralised Autonomous p2p

- Web1: server-based
- Web2: cloud-based, but centralized control – hyperscalers (Google, Facebook, …)
- Web3: decentralized, blockchains and smart contracts

3



Blockchain Council

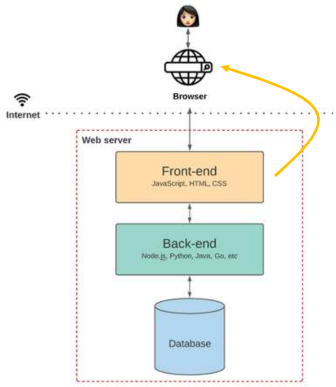
www.blockchain-council.org

Metaverse v/s Web 3.0

Metaverse		Web 3.0
A digital environment that combines digitally enhanced physical reality with physically persistent virtual environments	Definition	A new internet iteration aims to establish a decentralized online network in which users own and control the material and assets they create
It is still under development, and the potential areas are still under scrutiny	The Application Scope	Throughout the web, it is applicable
VR, AR ,XR((Extended Reality) world facility	Target	Blockchain controlled, peer-to-peer network facility
Virtual Gaming, Health Surgery, 3d Training, Social Events	Application	Democratic system, permissionless network like Crypto world(system run without market monopoly)
Dematerialization of physical entity around us to digital space	Depiction	Individual owned and regulating internet
Connectivity technology ● Human interface ● Decentralization technology ●	Underlying Technologies	● Blockchain & cryptocurrency ● NFTs ● DAOs ● DeFi
Powered by wifi6,6G,Spatial computing(VR,XR,Geo mapping), creator economy (asset market,mint NFT)	Technical	Powered by Decentralized Autonomous Organization, AI (Artificial Intelligence), Blockchain

4

Web 2.0 versus Web 3.0 browser



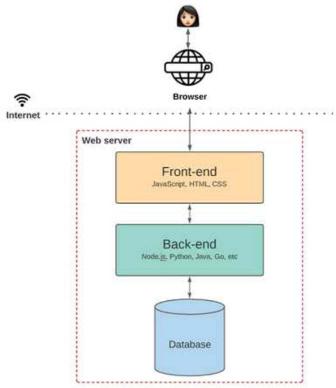
Executed in browser

Web 2.0

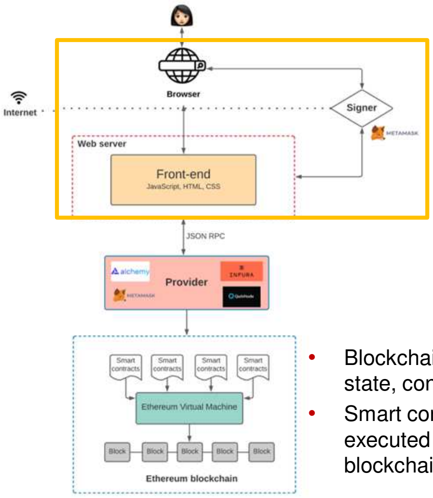
Source: https://www.preethikasireddy.com/

5

Web 2.0 versus Web 3.0 browser



Web 2.0



Web 3.0 browser

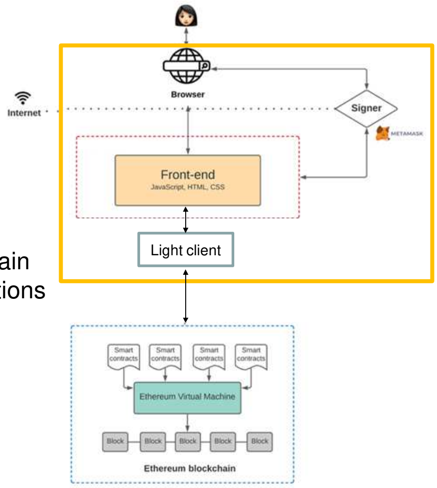
- Blockchain: global state, consensus
- Smart contracts executed by all blockchain nodes

Web 3.0

Source: https://www.preethikasireddy.com/

6

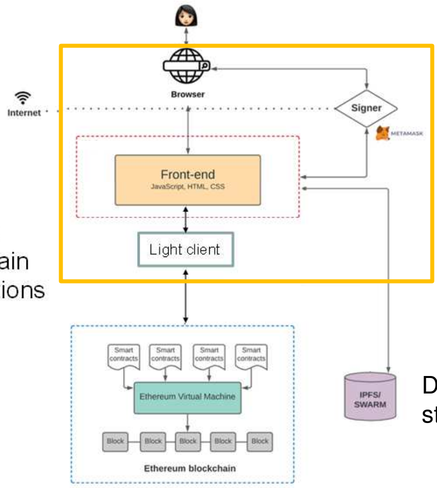
Web 3.0 browser & architecture evolution



Web 3.0 browser

Verifies blockchain transactions

Web 3.0 browser & architecture evolution



Web 3.0 browser

Verifies blockchain transactions

Decentralized storage

Web3 versus Web2 browser

- Integrated “wallet”
  - Not only crypto but also digital identifiers and credentials
- Light client
  - Verify blockchain transactions

9

Web 5

- Core idea: users have complete control identity and data
- Introduced by former Twitter CEO Jack Dorsey

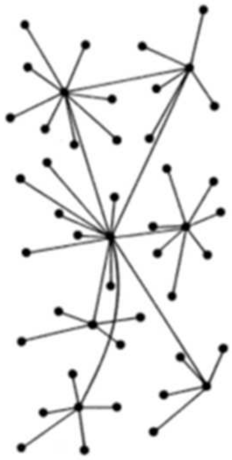
Key technology

- Decentralized identifiers (DIDs)
- Verifiable Credentials (VCs)

10

Web 3.0 versus Web 5.0

- Both are decentralized
- Web 3.0
  - Smart contracts/Decentralized applications (DApps) running on public blockchains
  - Decentralized internet that gives users control over their information
- Web 5.0
  - Data stored on decentralized web nodes
  - Users have full control over identities and data



11

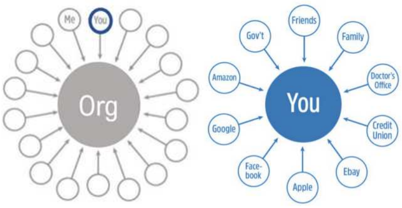
Web 4.0

- Does not have single meaning/intepretation
- More immersive and intuitive user experience
- Virtual reality and augmented reality technologies
- Sounds like metaverse

12

Traditional versus Decentralized Identifiers

- Self-sovereign identifiers for individuals, organizations, things, real or virtual
- Decentralized, persistent, resolvable, cryptographically verifiable
- Can be registered in a blockchain, decentralized network, or off-ledger (ledger-agnostic)
- W3C recommendation (considered a Web standard), 19 July 2022

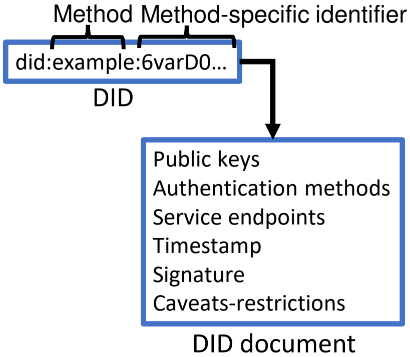


Organization in control of identity

User in control of identity

W3C Decentralized Identifiers - DIDs

- Decentralized Identifiers (DIDs) v1.0, W3C Recommendation, 19 July 2022
- DID is a URI associated to a DID document: “globally unique identifier, resolveable with high availability, and cryptographically verifiable”
- Generalizes linkage between name/id and a single public key
- DID-DID document association: DID document is usually maintained by a DID registry which is responsible for implementing proper security & access control
- DID contents and registry operations determined by DID method



Method Method-specific identifier

did:example:6varD0…

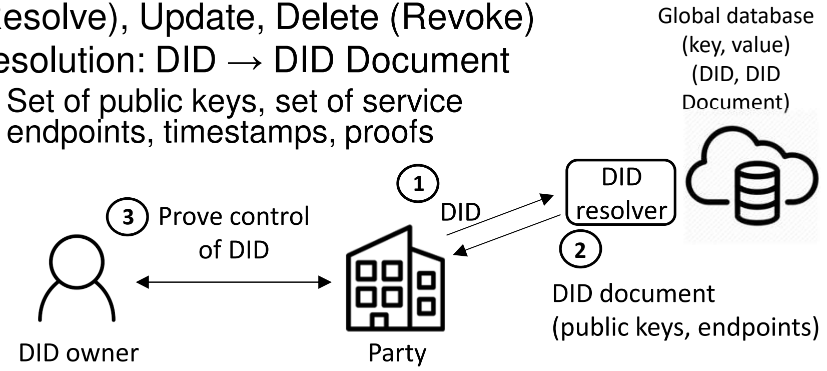
DID

Public keys
Authentication methods
Service endpoints
Timestamp
Signature
Caveats-restrictions

DID document

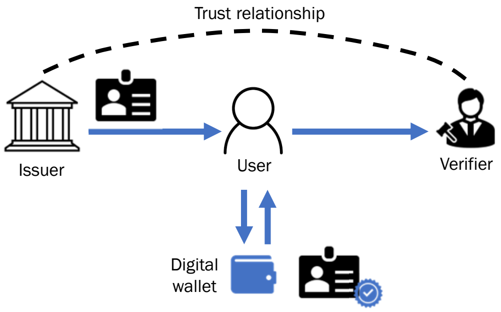
DID methods

- Different DID methods did:sov, did:btcr, did:v1, did:uport, ...
- CRUD for DIDs: Create, Read (Resolve), Update, Delete (Revoke)
- Resolution: DID → DID Document
  - Set of public keys, set of service endpoints, timestamps, proofs



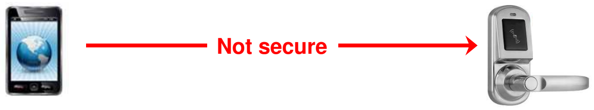
Verifiable Credentials data model

- W3C Recommendation 03 March 2022
- User control of identity & credentials
- Reduce PII (Personal Identifiable Information) on company servers by moving it to user wallets, GDPR compliance
- User can combine multiple credentials
- Interoperability: can interact with existing systems using common standards
- No communication or data exchange between access management systems, trust relationship is sufficient



Communicating with constrained IoT devices

- Constrained IoT devices (Things): limited/no connectivity, insecure channel

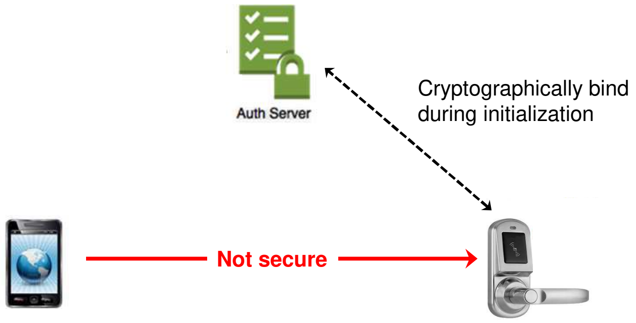


Connected device

Disconnected from the Internet device

Communicating with constrained IoT devices

- Constrained IoT devices (Things): limited/no connectivity, insecure channel

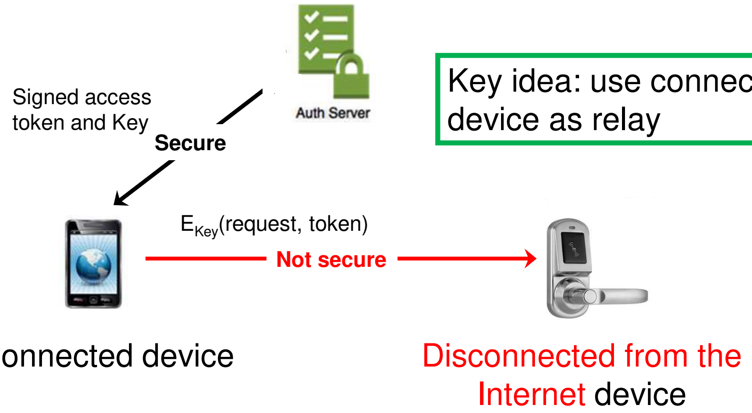


Connected device

Disconnected from the Internet device

Communicating with constrained IoT devices

- Constrained IoT devices (Things): limited/no connectivity, insecure channel



Auth Server

Signed access token and Key

Secure

E_{Key}(request, token)

Not secure

Connected device

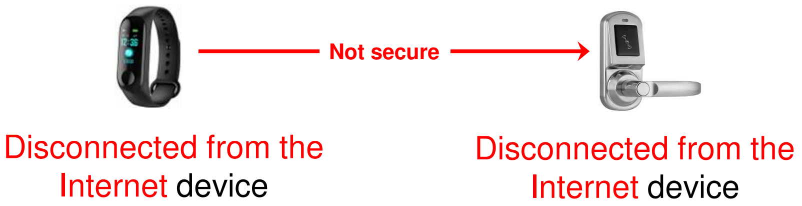
Disconnected from the Internet device

Key idea: use connected device as relay

19

Communicating **between** constrained IoT devices

- Constrained IoT devices (Things): limited/no connectivity, insecure channel



Not secure

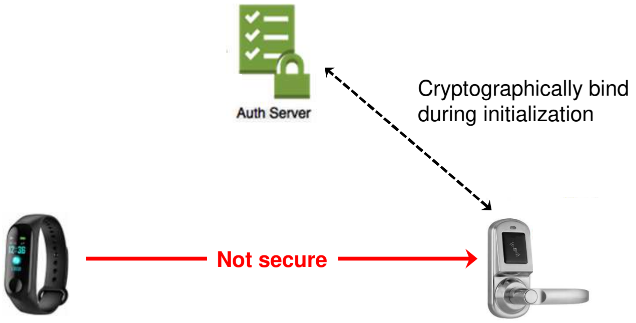
Disconnected from the Internet device

Disconnected from the Internet device

20

Communicating **between** constrained IoT devices

- Constrained IoT devices (Things): limited/no connectivity, insecure channel



Auth Server

Cryptographically bind during initialization

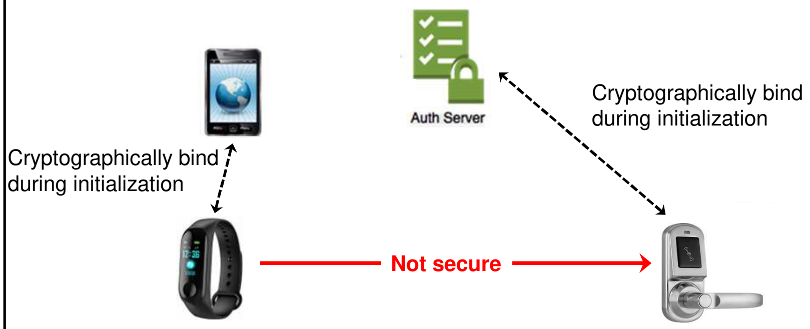
Not secure

Disconnected from the Internet device

Disconnected from the Internet device

Communicating **between** constrained IoT devices

- Constrained IoT devices (Things): limited/no connectivity, insecure channel



Auth Server

Cryptographically bind during initialization

Cryptographically bind during initialization

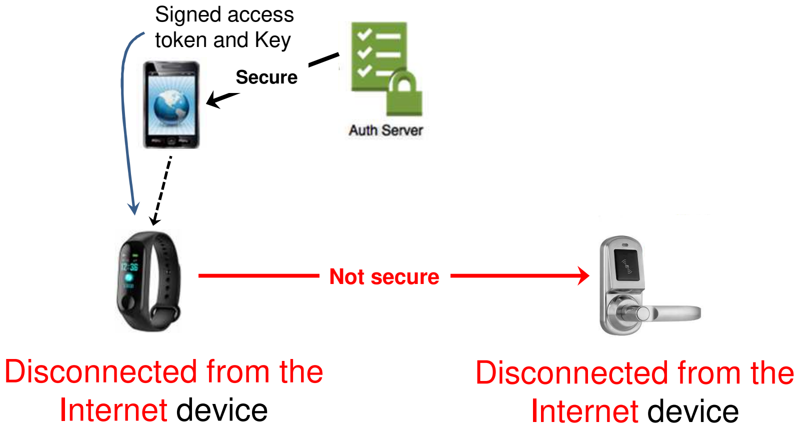
Not secure

Disconnected from the Internet device

Disconnected from the Internet device

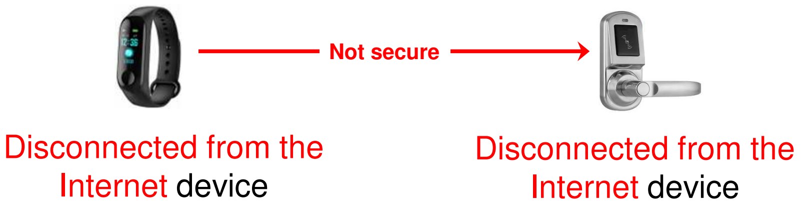
Communicating **between** constrained IoT devices

- Constrained IoT devices (Things): limited/no connectivity, insecure channel


Signed access token and Key
Secure
Auth Server
Not secure
Disconnected from the Internet device
Disconnected from the Internet device

Communicating **between** constrained IoT devices

- Constrained IoT devices (Things): limited/no connectivity, insecure channel
- **Secure** and **trusted** communication **between disconnected IoT devices**
  - **Trusted = perform actions according to owner defined policies**


Not secure
Disconnected from the Internet device
Disconnected from the Internet device