A Security Perspective on the Web3 Paradigm

NIST Internal Report (NIST IR 8475)

By Dylan Yaga & Peter Mell

February 2025 | Read the full publication (Doi link)

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

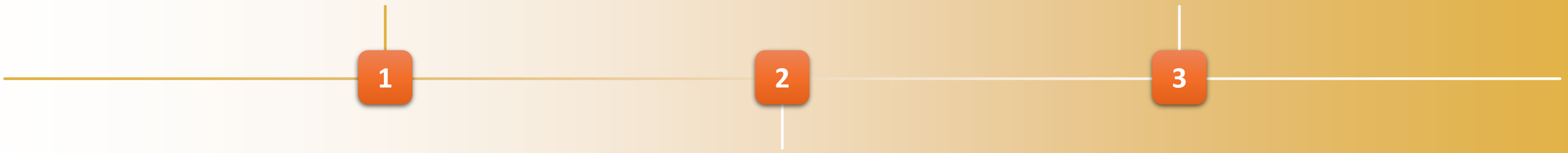
The Web's Evolution: From Static to Decentralized

Web 1.0: The Nascent Web

Late 1980s–Early 2000s. The "static" or "read-only" web, primarily text, images, and hyperlinks. Minimal user interaction.

Web3: The Proposed Future

A user-centric restructuring emphasizing decentralized data, user ownership, and web-native currencies.



Web 2.0: The Current Web

Early 2000s–Present. The "interactive" and "social" web. Massive growth in user data collection, social media, and platform lock-in.

Note: Web3 is distinct from the "Semantic Web" (Web 3.0), which focuses on making data more machine-readable via metadata.

The Web3 Vision: User-Centric Restructuring

Web3 is a goal for restructuring the internet to be more user-centric, shifting ownership and operation into the hands of users themselves.

Data Ownership

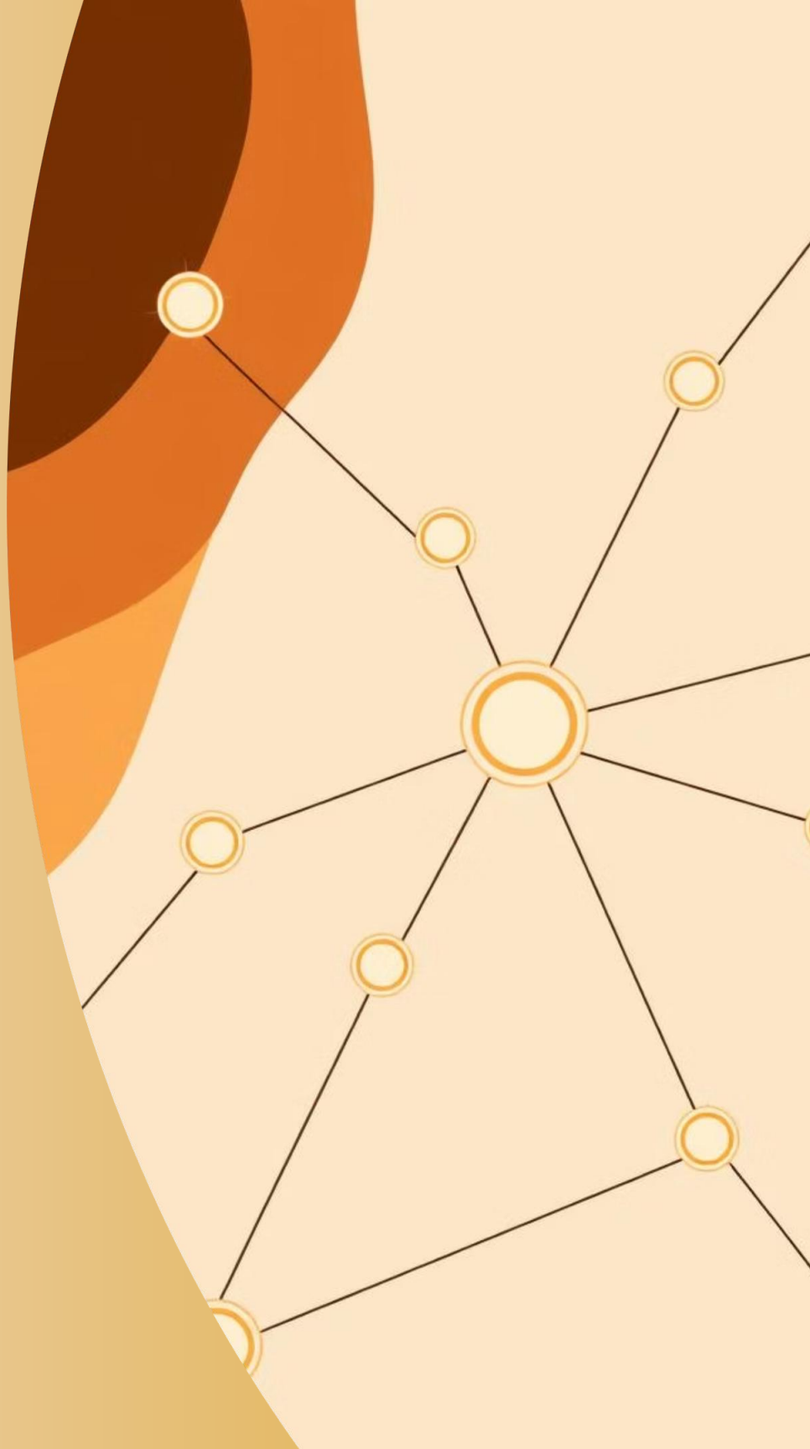
Users own, manage, and secure their personal data, acting as gatekeepers for applications.

Decentralization

Systems are decentralized and distributed, built on blockchain technology, allowing direct user participation.

Tokenization & Assets

Digital tokens represent assets, and web-native currencies (cryptocurrency) are used for payments and incentives.



Web3 Data Model: A Fundamental Shift

The proposed Web3 model fundamentally changes how data is owned, stored, and accessed compared to the current web.

Data Ownership	Mostly owned by organizations; limited user rights; data is easily copied.	Mostly owned by users; proven via digital signatures; data can be tokenized for transfer and provenance.
Data Location	Stored by organizations in proprietary databases; redundant copies across applications.	Public data/credentials on blockchain; large data on decentralized storage; private data in secure external hubs.
Data Access	Accessed, modified, or sold by organizations without user knowledge.	Requires explicit user authorization, managed at a granular level, and can be revoked.

Key Web3 Technology Components

Web3 integrates existing and new technologies to achieve its goals, focusing on identity, decentralization, and secure transactions.

Mobile Technology

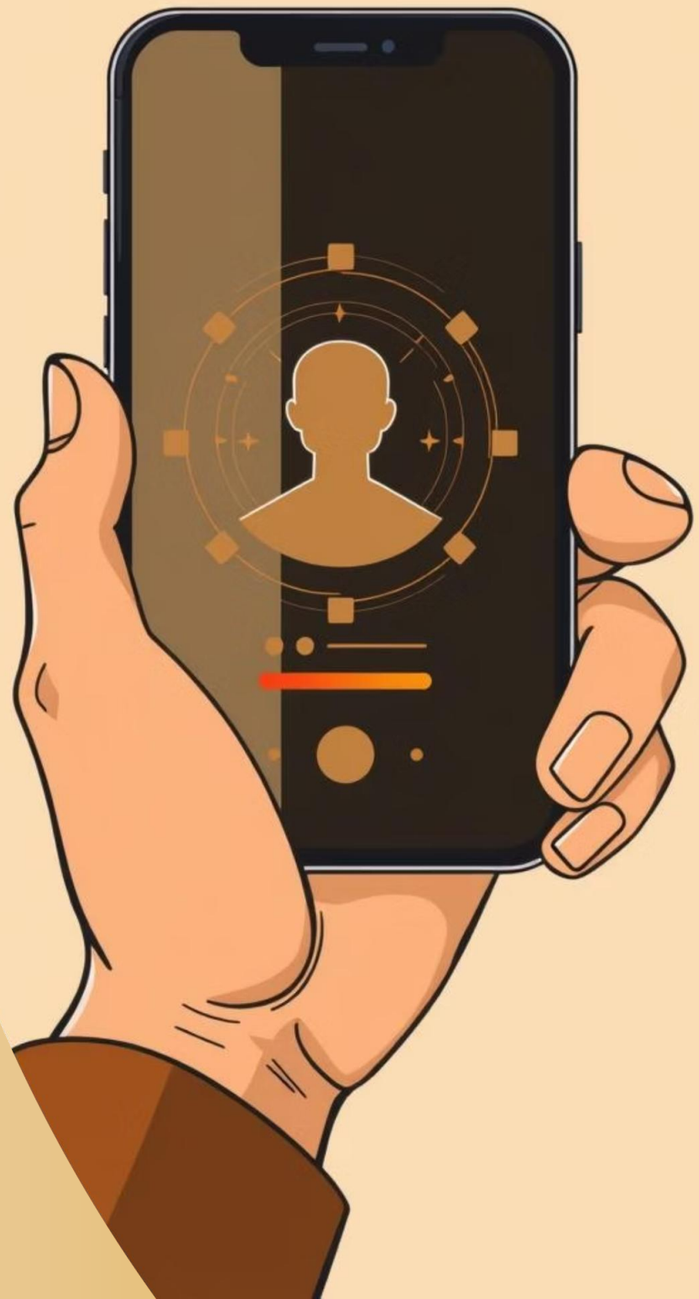
Mobile devices are ideal portals due to their personal nature and modern security features (e.g., hardware security modules).

Digital Identity & Credentials

Uses Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to prove information without revealing underlying data.

Decentralized Systems

Blockchains provide decentralization and ownership. Smart contracts automate procedures and record complex transactions.



Security Challenge: Increased User Responsibility

The shift to user-centric data ownership greatly increases the burden on individuals for security, privacy, and access recovery.

Access Recovery is Critical

Losing private keys means permanent loss of access. Users must proactively set up robust backup and recovery schemes.

Security Complexity

Non-technical users may struggle with complex security and privacy options. Software must be designed for usability and security.

Targeted Attacks

Malicious actors must target individuals, making attacks less significant for the system but potentially devastating for the user.

Security Challenge: Trust and Scams

In a decentralized ecosystem, determining the legitimacy of applications and organizations is difficult, making users highly vulnerable to scams.

Phishing and Private Keys

Users may be tricked into giving away private keys, granting malicious actors full access to all their data and digital assets.

Fraudulent Assets

Scammers use "look-alike" accounts to sell worthless tokens (fungible and non-fungible) or entice users to approve fraudulent smart contracts.

Excessive Permissions

Compromised or fraudulent applications may request excessive system or smart contract privileges, leading to data theft or asset transfer.

Data Permanence and Removal Difficulty

Data posted to a blockchain are almost certain to remain, making removal effectively impossible and creating significant challenges.

Irreversible Data

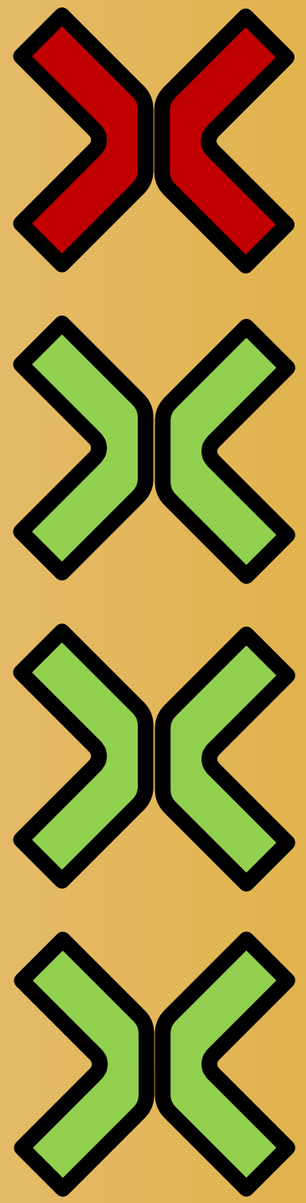
Users must refrain from posting sensitive information directly to a blockchain, as there are no formalized procedures for removal.

Costly Rollbacks

Removing data via a rollback (reorg) is computationally expensive, especially for proof-of-work systems, and requires redoing all subsequent work.

Chain Splits

Controversial data removal can lead to a chain split, where the original data persists on a copy of the blockchain.



The Impact of Chain Splits on Web3

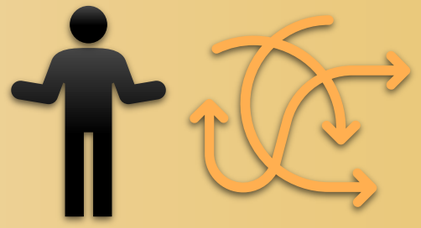
A chain split (hard fork) duplicates everything up to the split point, including smart contracts and NFTs, leading to potential confusion and security issues.

Duplicated Assets

NFTs and smart contracts exist on all resulting chains. Developers must decide which chain to support, potentially abandoning users on others.

Investor Confusion

The duplication of assets like NFTs can confuse users and investors regarding the true value and longevity of their digital items.



Future Considerations for Web3 Development

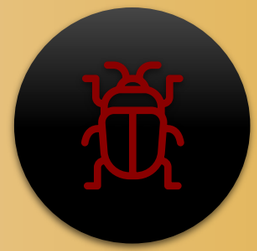
As Web3 evolves, developers must address core challenges related to regulation, availability, and security best practices.

Regulatory Conflict

Privacy regulations (e.g., GDPR) conflict with blockchain permanence. Developers must determine technical feasibility and jurisdiction.

Availability & DoS

Scaling solutions are needed to prevent execution cost increases and long wait times. Cross-chain bridge vulnerabilities remain a key risk.



Errors and Bugs

Security must be integrated early. Developers must monitor all technology layers (blockchain, smart contracts, wallets) for vulnerabilities.

Security should be integrated into the design instead of being added later to a built solution.

Thank you for your time!

Do you have any Questions?

Reference:

Yaga D, Mell PM (2025) A Security Perspective on the Web3 Paradigm. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8475. https://doi.org/10.6028/NIST.IR.8475

Group # 4 (ADP CS 5th Semester)