SAMPLE

Building the Web3 of Tomorrow

A Practical Guide to the Technology Decentralizing the Internet

Aiman JoeHanz

Free sample: Introduction & Chapter 1

putrabooks.github.io

Buy the full book:

Carousell carousell.sg/p/building-the-web3-of-tomorrow-ebook-pdf-1465658911

Gumroad

Ko-fi

ElevenReader

Payhip

Contents

Introduction

Chapter 1: The Current State of Web3

Chapter 2: Today's Web3: Limitations and Failure Modes

Chapter 3: Common Mistakes in Web3 Projects

Chapter 4: Foundational Principles of Web3 Design

Chapter 5: Building Web3 Applications, Step by Step

Chapter 6: Implementation Strategies for Production Web3 Systems

Chapter 7: Technology Deep Dive: Smart Contracts, Consensus, and Cryptography

Chapter 8: Case Studies: Real-World Web3 Deployments

Chapter 9: Evaluating and Testing Web3 Systems

Chapter 10: The Future of Web3

Chapter 11: Action Plan: Building Your Web3 Practice

Chapter 12: Advanced Topics: Privacy, MEV, and Cross-Chain Architecture

Chapter 13: Building a Web3-Ready Organization

Frequently Asked Questions

Glossary

Bibliography

This free sample contains the Introduction and Chapter 1. The complete book contains the full contents above.

Introduction

Web3 is the vision of a decentralized internet built on blockchain technology, smart contracts, and token-based economics. It promises to shift power from centralized platforms to individual users — giving people ownership of their data, their digital assets, and their online identities. It is, depending on who you ask, either the future of the internet or a solution looking for a problem.

The excitement around Web3 is real. Decentralized finance (DeFi) protocols process billions of dollars in transactions without banks. Non-fungible tokens (NFTs) have created new markets for digital art and collectibles. Decentralized autonomous organizations (DAOs) govern protocols with billions in assets.

Layer-2 scaling solutions have reduced transaction costs by orders of magnitude. Cross-chain bridges connect previously isolated ecosystems. Zero-knowledge proofs enable private transactions on public blockchains.

But the skepticism is also real. Most Web3 applications have far fewer users than their Web2 counterparts. Transaction costs, while improved, can still be prohibitive. The user experience of most Web3 applications is clunky and confusing. Regulatory uncertainty looms over every project. Scams, hacks, and exploits have cost users billions of dollars. The environmental impact of proof-of-work blockchains has drawn fierce criticism. And the question of whether decentralization is actually what users want remains open.

This book is for people who need to understand Web3 as a technology and build with it practically. Whether you are a developer considering building on blockchain, a product manager evaluating Web3 features, an executive deciding whether to invest, or a curious observer trying to separate signal from noise, this book will give you the technical foundation and practical guidance you need.

We will cover the current state of Web3 technology, its limitations and failure modes, the common mistakes that derail Web3 projects, the foundational principles of Web3 design, a step-by-step guide to building Web3 applications, implementation strategies for production systems, a deep dive into the underlying technology, real-world case studies, evaluation and testing approaches, the future of the technology, an action plan for building your Web3 practice, advanced topics, and how to build a Web3-ready organization.

This is not a book about crypto speculation or investment advice. It is a practical, engineering-focused guide to the technology behind Web3 — how it works, where it fails, and how to build with it effectively.

Chapter 1: The Current State of Web3

Web3 refers to a set of technologies and principles that aim to decentralize the internet:

- Blockchain networks: Distributed ledgers that record transactions without a central authority. Bitcoin, Ethereum, Solana, and others provide the foundational infrastructure. - Smart contracts: Self-executing programs that run on blockchain networks. They encode rules and automatically execute when conditions are met, without intermediaries. - Token-based economics: Digital tokens (fungible and non-fungible) that represent ownership, governance rights, access, or utility within a network. - Decentralized storage: Systems like IPFS and Arweave that store data across distributed networks rather than centralized servers. - Decentralized identity: Systems that let users control their own digital identity without relying on a central provider. - Self-sovereign data: The principle that users own and control their data, sharing it selectively rather than surrendering it to platforms.

Web3 is not a single technology but an ecosystem of interconnected protocols, applications, and principles. It is built on the idea that the internet should be more open, permissionless, and user-controlled.

The blockchain landscape has evolved significantly since Bitcoin's launch in 2009:

Ethereum remains the dominant smart contract platform, with the largest ecosystem of developers, applications, and total value locked. Its transition to proof-of-stake in 2022 (The Merge) reduced energy consumption by 99.95%. The rollout of EIP-4844 (proto-danksharding) in 2024 dramatically reduced Layer-2 transaction costs.

Solana has emerged as the primary high-performance alternative, processing thousands of transactions per second with sub-second finality. Its monolithic architecture trades some decentralization for throughput.

Layer-2 networks (Optimism, Arbitrum, Base, zkSync, Starknet) have become the primary venue for user-facing applications. They inherit Ethereum's security while offering dramatically lower costs and higher throughput.

App-chains (applications with their own blockchain) have gained traction for high-value protocols that need custom economics or governance. The Cosmos SDK and Polkadot provide frameworks for building application-specific chains.

Modular blockchains (Celestia, EigenLayer) separate the functions of a blockchain — execution, settlement, consensus, and data availability — into

specialized layers. This modularity enables more efficient scaling.

Web3 applications span several categories:

Decentralized Finance (DeFi): Protocols for lending, borrowing, trading, and earning yield without traditional financial intermediaries. Major protocols include Uniswap (decentralized exchange), Aave (lending), MakerDAO (stablecoin), and Lido (liquid staking). Total value locked in DeFi protocols has ranged from $40B to $180B.

NFTs and Digital Ownership: Non-fungible tokens represent ownership of unique digital assets. Use cases include digital art, gaming items, event tickets, domain names, and membership passes. The NFT market has gone through boom and bust cycles but continues to evolve.

DAOs (Decentralized Autonomous Organizations): Member-owned communities governed by smart contracts and token-based voting. DAOs manage treasuries, make protocol decisions, and coordinate collective action. Notable DAOs include MakerDAO, Uniswap DAO, and Arbitrum DAO.

Decentralized Social: Platforms that give users ownership of their social graph and content. Farcaster and Lens Protocol enable portable social identities that users control.

Decentralized Identity: Systems like ENS (Ethereum Name Service) and World ID provide user-controlled identity that works across applications without central providers.

Web3 Infrastructure: Protocols for decentralized storage (IPFS, Arweave), compute (Akash), oracles (Chainlink), and indexing (The Graph) that provide the building blocks for Web3 applications.

The Web3 competitive landscape differs from traditional technology:

- Open-source by default: Most Web3 protocols are open-source, with code that anyone can audit, fork, or build upon. This creates a fundamentally different competitive dynamic. - Composability: Protocols can be combined like Lego blocks. A lending protocol can integrate a price oracle, which integrates a data provider, creating "money Legos." - Network effects through liquidity: DeFi protocols compete on liquidity depth, not just features. The protocol with the most liquidity attracts the most users, which attracts more liquidity. - Multi-chain reality: Users and applications span multiple chains. Bridges and cross-chain protocols connect these ecosystems. - Token incentives: Protocols use token rewards to bootstrap network effects. This can accelerate growth but also creates misaligned incentives if poorly designed.

The Web3 developer ecosystem has matured significantly:

- Solidity remains the primary smart contract language for Ethereum and EVM-compatible chains. Tooling has improved dramatically with frameworks like Foundry and Hardhat. - Rust is used for Solana and some other chains, offering performance and safety. - Development frameworks (Foundry, Hardhat, Anchor) provide testing, deployment, and debugging tools. - Indexing and data (The Graph, Dune, Token Terminal) make on-chain data accessible for analysis and application building. - Wallet and account abstraction (MetaMask, WalletConnect, account abstraction via EIP-4337) are improving the user experience.

Despite this progress, the developer experience still lags behind Web2. Setting up a development environment, testing smart contracts, and deploying to production requires specialized knowledge.

Institutions have moved steadily into Web3:

- ETF approvals: Regulated investment vehicles arrived in the US with the approval of Bitcoin and Ethereum ETFs. - Corporate adoption: Stripe, PayPal, and Visa have all wired crypto payment rails into their products.- Regulatory clarity (partial): Some jurisdictions (EU with MiCA, Singapore with MAS) have provided regulatory frameworks, while others remain uncertain. - Institutional infrastructure: Custody solutions (Fireblocks, Anchorage), trading platforms (Coinbase Institutional), and data providers (Chainalysis) serve institutional needs.

Inside Web3, tokens do several jobs at once:

- Utility tokens: Unlock a protocol's services (paying for computation on a decentralized compute network, for instance) - Governance tokens: Carry votes on protocol decisions - Stablecoins: Hold a fiat peg (USDC, USDT, DAI) for payments and DeFi - NFTs: Stand for unique digital assets - Security tokens: Stand for regulated financial instruments

Few parts of Web3 are harder than token design. Tokenomics done badly produces death spirals, governance capture, or regulatory trouble.

Web3 infrastructure has evolved beyond basic blockchain:

- RPC providers (Alchemy, Infura, QuickNode) provide API access to blockchain networks - Indexing protocols (The Graph) organize and query blockchain data - Oracle networks (Chainlink, Pyth) bring off-chain data to smart contracts - Bridge protocols (LayerZero, Wormhole) connect different blockchain networks - Storage networks (IPFS, Arweave, Filecoin) provide decentralized file storage - Compute networks (Akash, Render) provide decentralized computing

resources

User experience remains the biggest barrier to mainstream adoption:

- Wallet management: Users must manage seed phrases, understand gas fees, and navigate transaction signing - Onboarding: Converting fiat to crypto and back remains friction-heavy - Transaction complexity: Users must understand concepts like gas, nonces, and confirmation times - Error messages: Smart contract errors are often cryptic and unhelpful - Recovery: Lost keys mean lost funds — there is no "forgot password" button

Account abstraction (EIP-4337) and smart contract wallets are addressing these issues, enabling features like social recovery, gasless transactions, and session keys. But widespread adoption of these improvements is still in early stages.

PRACTICAL INSIGHT The biggest barrier to Web3 adoption is not technology — it is user experience. A Web3 application that requires a user to install a wallet, buy crypto, transfer it, and pay gas fees will lose 99% of potential users at each step. The applications that succeed are those that abstract away as much of this friction as possible. Account abstraction, gas sponsorship, and social login are not optional features — they are requirements for mainstream adoption.

KEY TAKEAWAYS

- Web3 is an ecosystem of blockchain-based technologies aiming to decentralize the internet — not a single technology - Ethereum remains dominant but faces competition from Solana, Layer-2s, and app-chains - DeFi, NFTs, and DAOs are the primary application categories, but infrastructure and identity are growing - Open-source composability creates unique competitive dynamics — protocols are built to be combined - User experience is the biggest barrier to mainstream adoption — technical improvements must be paired with UX improvements

Stablecoins have become the connective tissue between traditional finance and Web3:

- Fiat-backed stablecoins (USDC, USDT) are pegged to the US dollar through reserves held by the issuer.

They dominate trading pairs and serve as the primary medium of exchange in DeFi. - Crypto-backed stablecoins (DAI) are pegged through over-collateralization with crypto assets. They are fully decentralized but capital-inefficient. - Algorithmic stablecoins attempt to maintain pegs through algorithmic mechanisms. The collapse of Terra's UST in 2022 demonstrated the

fragility of this approach — $40B in value evaporated in days. - Stablecoin volume now exceeds that of many traditional payment networks. The infrastructure for issuing, transferring, and settling stablecoins has matured significantly.

The stablecoin market continues to grow as it provides the reliable unit of account that crypto-native applications need.

Institutional adoption has accelerated across multiple vectors:

- Asset managers like BlackRock and Fidelity have launched crypto funds and ETFs, providing regulated exposure to digital assets. - Banks are exploring tokenization of traditional assets (bonds, money market funds) on blockchain networks. - Payment companies (Stripe, PayPal, Visa, Mastercard) have integrated crypto payment rails. - Trading firms like Jump Trading and Wintermute provide liquidity across DeFi and CeFi venues. - Custody providers (Coinbase Custody, Anchorage, Fireblocks) offer institutional-grade custody solutions.

This institutional infrastructure reduces the risk for traditional finance participants to engage with Web3, creating a bridge between the two ecosystems.

The Layer-2 ecosystem has exploded since 2024:

- Arbitrum leads in TVL with over $15B locked, hosting major DeFi protocols and gaming applications. - Optimism has evolved into the OP Stack — a modular framework that powers Base, Worldcoin, and other chains. - Base (built by Coinbase on the OP Stack) has rapidly become one of the most active L2s, with strong consumer onboarding through Coinbase's user base. - zkSync and Starknet lead the ZK rollup space, offering faster finality but with a less mature developer ecosystem. - Scroll and Linea provide EVM-equivalent ZK rollups, maintaining full compatibility with Ethereum tooling. - Blast and Mantle offer native yield for deposited assets, creating a new L2 category.

The L2 ecosystem has fundamentally changed how users interact with Ethereum — most user-facing applications now live on L2s, with Ethereum L1 serving as the settlement layer.

Developer tooling has improved dramatically:

- Foundry has become the preferred development toolkit, offering fast testing, fuzzing, and deployment in Rust. - Hardhat remains popular, especially for teams with JavaScript expertise. - Halmos and Hevm provide formal verification and symbolic execution for smart contracts. - Slither and Mythril provide static analysis to catch common vulnerabilities. - Tenderly offers

simulation, debugging, and monitoring for production contracts. - OpenZeppelin Defender provides a platform for managing, monitoring, and securing smart contracts.

Despite improvements, the developer experience still lags behind Web2. The learning curve for Web3 development remains steep, and the tooling ecosystem is fragmented across multiple chains and standards.

Institutions are building a compliant DeFi stack:

- Permissioned pools: DeFi pools that require whitelisted addresses, enabling institutions to participate while maintaining compliance. - KYC'd NFTs: NFTs that serve as KYC credentials, granting access to compliant DeFi protocols. - Custodial DeFi: Custodians like Fireblocks enable institutions to interact with

DeFi through their custody infrastructure, without exposing private keys. - Regulated bridges: Bridges that perform KYC/AML checks on cross-chain transfers, enabling compliant cross-chain operations. - On-chain reporting: Tools for generating compliance reports, audit trails, and tax documentation from on-chain activity.

NFTs have evolved beyond digital art:

- Utility NFTs: NFTs that provide access to products, services, or communities. Examples include event tickets, membership passes, and loyalty programs. - Dynamic NFTs: NFTs whose metadata and appearance can change based on on-chain or off-chain events. Examples include evolving game characters and NFTs that update with real-world data. - NFT financialization: Protocols that enable lending against NFTs, fractionalizing NFTs, and trading NFT indices. - Soulbound tokens: Non-transferable NFTs that represent identity, credentials, or reputation. Proposed by Vitalik Buterin, these enable on-chain credentials.

One of the most significant technical challenges in Web3 is interoperability — the ability for different blockchain networks to communicate, share data, and transfer value. The early assumption that a single blockchain would dominate has given way to a multi-chain reality where users and assets flow across dozens of networks.

Token bridges have emerged as the primary mechanism for cross-chain asset transfers. These protocols lock assets on one chain and mint representative tokens on another, creating a bridge between otherwise isolated ecosystems. However, bridges have also been the most exploited category of Web3 infrastructure. The Wormhole bridge hack in 2022 resulted in $326 million in losses. The Nomad bridge exploit in the same year saw $190 million drained due to a faulty initialization bug. The Ronin bridge attack cost $625 million.

These incidents highlight a fundamental tension: bridges concentrate value and create attractive targets for attackers.

LayerZero and CCIP (Cross-Chain Interoperability Protocol) represent a newer generation of cross-chain protocols that attempt to address these security concerns through multi-party verification and decentralized oracle networks. Rather than relying on a single validator set, these protocols use multiple independent parties to verify cross-chain messages, reducing the risk of a single point of failure.

The Inter-Blockchain Communication (IBC) protocol, developed within the Cosmos ecosystem, takes a different approach. IBC enables native communication between chains built with the Cosmos SDK, creating a network of interoperable blockchains that can transfer tokens and data without bridges. Over 90 chains currently support IBC, including Cosmos Hub, Osmosis, and Celestia.

Axelar provides a complementary layer that connects EVM chains to the Cosmos ecosystem via IBC, extending cross-chain communication beyond a single framework.

The Ethereum ecosystem is pursuing its own interoperability through shared sequencing and shared settlement. Layer-2 networks that share the same sequencer or settlement layer can communicate more efficiently, reducing the need for external bridges. Optimism's Superchain vision and Polygon's AggLayer are built on this principle — a network of chains that share infrastructure and can communicate natively.

Despite these advances, cross-chain communication remains one of the most technically complex and risky areas of Web3 development. Projects building cross-chain functionality must carefully evaluate the security models of the protocols they use, have contingency plans for bridge failures, and consider whether the complexity is justified by the benefits.

Account abstraction, formalized in EIP-4337, represents one of the most significant improvements to the Web3 user experience. Traditional Ethereum accounts are controlled by private keys — lose the key and you lose access to everything. There is no password recovery, no multi-factor authentication, no spending limits. This "key loss equals total loss" model has been a major barrier to adoption.

Account abstraction changes this by separating the concept of an account from a private key. Smart contract wallets can implement arbitrary logic for transaction validation, enabling features that traditional externally owned accounts cannot support:

Social recovery allows users to designate trusted contacts or devices that can collectively recover access to a wallet if the primary key is lost. This mirrors the account recovery flows that users expect from conventional web applications. Guardian-based recovery systems, pioneered by Safe (formerly Gnosis Safe), let users set up a quorum of addresses that can rotate keys without compromising the wallet.

Sponsored transactions enable applications to pay gas fees on behalf of users. This removes one of the most confusing aspects of Web3 onboarding — the need to acquire tokens before a user can do anything. A new user can be onboarded with zero tokens and the application covers the cost of their first transactions. This is particularly important for mass adoption, as the mental model of "I need to buy crypto to use this app" is a significant friction point.

Session keys allow users to grant limited, time-bound permissions to applications. Instead of approving every transaction individually, a user could grant a gaming application the right to execute specific in-game transactions for a limited time, without giving the app full control of their wallet. This reduces transaction fatigue while maintaining security boundaries.

Batch transactions let users combine multiple operations into a single transaction. Instead of separately approving a token transfer, a swap, and a withdrawal, a user can batch all three into one action. This reduces both gas costs and the number of approvals a user must navigate.

Major wallet providers including Coinbase Wallet, Polygon, and Binance have integrated account abstraction features. The ERC-4337 rollup saw millions of user operations in its first year of deployment, with bundlers processing transactions across multiple networks. While adoption is still early, account abstraction is fundamentally changing what is possible in Web3 user experience design.

Zero-knowledge proofs (ZKPs) have moved from theoretical cryptography to practical deployment in Web3 systems. A zero-knowledge proof lets one side demonstrate a statement's truth while disclosing nothing about the information behind it. Within Web3 that unlocks private transactions, scalable verification, and trustless computation. ZK rollups use zero-knowledge proofs to batch thousands of transactions off-chain and submit a single cryptographic proof to the base layer. This dramatically increases throughput while maintaining the security guarantees of the underlying blockchain. zkSync Era, Starknet, Polygon zkEVM, and Linea are production ZK rollups that process real user transactions. The cost of generating proofs has decreased significantly with hardware acceleration and algorithmic improvements, making ZK rollups increasingly competitive with optimistic rollups.

Private transactions use ZKPs to shield transaction details from public view. Tornado Cash (before its sanctioning) used zero-knowledge proofs to enable private Ethereum transactions. Zcash uses ZKPs natively for shielded transactions. Aztec Protocol is building encrypted smart contracts that use ZKPs to keep transaction data private while still being verifiable.

Identity verification is another growing use case. Protocols like World ID use ZKPs to prove that a user is a unique human without revealing which human they are. This enables one-person-one-vote governance, sybil resistance for airdrops, and verification without doxxing. The proof verifies personhood without linking the proof to a specific identity.

The computational cost of generating proofs remains a challenge. Proof generation for complex computations can take minutes to hours, requiring specialized hardware. However, the field is advancing rapidly. New proof systems like PLONK, Halo2, and STARKs have reduced proving times, and the development of application-specific integrated circuits for proof generation promises further cost reductions.

Decentralized storage is a critical layer of Web3 infrastructure that is often overlooked in favor of more glamorous applications. Web3 applications need to store data — metadata for NFTs, content for decentralized social media, documents for DAOs — and centralized storage providers (AWS, Google Cloud) reintroduce the centralization that Web3 aims to eliminate.

IPFS (InterPlanetary File System) is the most widely used decentralized storage protocol. It uses content-addressed storage, where files are identified by their cryptographic hash rather than their location. This means that the same file will always have the same identifier, regardless of which node serves it. IPFS is used by NFT marketplaces to store metadata and images, by DApps to host their frontend, and by protocols to store documentation.

Arweave provides permanent storage. Files stored on Arweave are replicated across the network and designed to persist for approximately 200 years, with the cost of storage paid upfront through an endowment model. The protocol's novel consensus mechanism, SPoRA (Succinct Proofs of Random Access), incentivizes miners to store data by requiring them to prove they have access to historical data blocks.

Filecoin is a decentralized storage marketplace built on top of IPFS. Clients pay storage providers to store their data, with the network verifying that the providers are actually storing what they claim. This creates a market for storage where prices adjust based on supply and demand. Filecoin's integration with IPFS makes it practical for applications that need reliable,

incentivized storage.

Data availability is the other side of the storage coin. For Layer-2 networks to function, the data needed to reconstruct their state must be available — either on Ethereum (as calldata) or on a dedicated data availability layer. Celestia is the first purpose-built data availability layer, using a technology called data availability sampling that allows nodes to verify that data is available without downloading it all. EigenDA, Avail, and the EigenLayer ecosystem are building complementary data availability solutions.

The modularity enabled by data availability layers is transformative. A rollup can post its data to Celestia, settle on Ethereum, and execute on its own chain — using each layer for what it does best. This separation of concerns reduces costs, improves scalability, and creates a more flexible architecture for building Web3 applications.

End of free sample. The full book is available at putrabooks.github.io

ABOUT THE AUTHOR

Aiman JoeHanz writes about the technologies that are quietly reshaping the world. His Building of Tomorrow series examines the infrastructure behind artificial intelligence -- from blockchain and cloud computing to agentic systems and token optimization -- and asks how these technologies will evolve over the coming decade.

His books are built on technical research and engineering documentation, written for readers who want to understand systems rather than trends. He covers what is being built today and what it will take to build what comes next.

He believes that understanding infrastructure is the difference between watching the future happen and helping to create it.