1

Web3 Concepts and General Introduction

1.1	Basic Web3 Concepts and Definitions	5
1.2	Web3 Is the Convergence of Convergence	23
1.3	Web3 from a User Experience Regulation, and Investment Perspectives	33
1.4	Chapter Summary	37
1.5	Chapter Questions	38
References		39

Web3 is the latest stage in the evolution of the web, following the earlier stages of Web1 and Web2. Each stage represents a significant advancement in the capabilities and functionalities of the Internet.

Web1, the first generation of the web, emerged in the early days of the Internet when websites were predominantly static and text based. It was primarily used for sharing information and ideas, serving as a platform for personal and academic purposes. Websites during this time were created using HyperText Markup Language (HTML), a markup language that structures and formats web pages. However, they lacked the interactive features commonly found on modern websites.

Web2, the second generation of the web, marked a significant shift toward dynamic and interactive websites. It introduced advanced technologies that enabled users to have more engaging experiences. Web2 applications incorporated elements such as mobile technology, social networking, location-based services, user-generated content, and cloud computing. This led to the rise of mobile apps, social media platforms, e-commerce websites, content-sharing platforms, and other online services that offered a wide range of features and capabilities to users.

Now, with Web3, we are witnessing the next stage in the evolutionary progression of the web. Web3 builds upon the advancements of Web1 and Web2 while introducing new technologies and concepts to make the web more intelligent, interactive, and decentralized.

Web3 utilizes artificial intelligence (AI) to enhance the user experience by providing personalized and tailored interactions. Algorithms powered by AI analyze user data to offer recommendations, predictions, and customized services. This intelligence empowers users to have more meaningful and relevant interactions with web applications.

The integration of the Internet of Things (IoT) is another key aspect of Web3. It expands the connectivity of devices to the web, enabling a more seamless and integrated digital experience. Users can interact with a broader range of connected devices, gathering and sharing information across multiple platforms.

However, one of the most transformative elements of Web3 is the adoption of blockchain technology. Blockchain allows for the creation of decentralized networks and applications, ensuring data transparency, security, and user ownership. Users can have greater control over their data and identities through decentralized identity systems, granting them the ability to manage and authenticate their online presence.

Web3 represents the ongoing transformation and development of internet technologies and applications. Unlike the current centralized model, Web3 focuses on providing a self-sovereign and decentralized Internet, where users have ownership of their data and are not reliant on BigIT platforms. BigIT companies like Facebook and Google have centralized massive amounts of user data into their systems, giving them unprecedented control over people's information. With vast troves of data concentrated under their control, BigIT wields immense power to analyze, monetize, and leverage consumer data across their digital platforms and services.

A core aspect of Web3 is the emphasis on decentralized applications (dApps). Built on blockchain and other decentralized technologies, dApps are open, peer-to-peer (P2P), transparent, and secure. They offer users greater control over their data and online activities than traditional Web2 applications, unlocking new possibilities for interactions and services beyond the capabilities of the current web.

The potential value that Web3 can create is evident in various applications. Decentralized Finance (DeFi) (more details in Chapter 7) enables P2P access to financial services, reducing costs, and improving inclusivity. Supply chain management benefits from blockchain's real-time tracking and verification capabilities, enhancing transparency and reducing risks.

CAMBRIDGE
Cambridge University Press & Assessment
978-1-009-37567-2 — Web3
Ken Huang , Youwei Yang , Fan Zhang , Xi Chen , Feng Zhu
Excerpt
More Information

Non-fungible tokens (NFTs) provide unique digital assets, allowing businesses to monetize digital collectibles and virtual items, expanding revenue streams and global reach (Raptopoulos and Kelly 2022). The concept of a Metaverse, a virtual shared space, offers new platforms for commerce, entertainment, and social interactions, opening up new business opportunities.

This chapter provides a foundational understanding of Web3, covering its definitions, technological advancements, data ownership, user experience, regulatory considerations, and scalability challenges. It highlights the convergence of technologies, data, interactions, business models, identity, and organizational structures within the Web3 ecosystem. By exploring these dimensions, readers gain insights into the transformative potential of Web3 and its impact on the future of the Internet.

1.1 Basic Web3 Concepts and Definitions

At its core, Web3 represents a paradigm shift toward decentralization, aiming to redistribute power and control over digital interactions to users through innovative technologies such as blockchain, smart contracts, and dApps. Critical innovations such as zero-knowledge proofs (ZKPs) and new governance models allow Web3 to enhance privacy and democratic participation while maintaining verifiability and consensus. Programmable tokens serve as the incentive layer fueling collaborative ecosystems, while advances in interoperability stitch together the fabric of this connected yet decentralized network. However, Web3 also faces complex scalability, security, regulation, and adoption challenges. Understanding foundational concepts like decentralization, governance, cryptography, and token economics is key to appreciating both the transformative potential and current limitations of Web3. This constellation of technologies and ideas represents the building blocks for an envisioned Internet of the future that promises to be more open, user-centric, and privacy-preserving.

Here is a quick rundown of the main concepts covered in this section:

Decentralization – The core principle of Web3. Aims to distribute power and control away from centralized entities. Enabled by blockchain and P2P networks.

Blockchain – Distributed ledger technology that enables decentralization, transparency, and immutability. Provides the backbone for many Web3 applications.

Smart Contracts – Self-executing programs on the blockchain that automate agreements and processes. Enable the creation of dApps.

dApps – Decentralized applications built on blockchain that give users more control over data and interactions.

Interoperability – Ability for different blockchains and dApps to communicate and interact seamlessly. Critical for connecting the decentralized Web3 ecosystem.

Web3 Wallets – Gateways for managing identities, assets, and interactions in Web3. Enable key management, transactions, and dApp access.

Privacy/Security – Web3 aims to give users more control over data privacy via encryption, decentralized storage, ZKPs, and so forth. But it also faces new threats.

Governance/Consensus – Web3 networks use decentralized, participatory governance models such as decentralized autonomous organizations (DAOs) and consensus mechanisms such as proof of stake (PoS).

Tokens/Tokenization – Programmable digital assets on blockchain that power incentives, transactions, and governance in Web3 networks and dApps.

Scalability – Decentralized systems can be slower and limited in transaction capacity compared to centralized systems. Ongoing research into solutions.

1.1.1 Decentralization

Decentralization lies at the core of Web3. Unlike the traditional Web2 model, which relies on centralized authorities and intermediaries, Web3 seeks to distribute power and authority among participants in the network. Decentralization finds its primary implementation in blockchain technology (described in Section 1.1.2), a distributed ledger system that records immutable transactions across multiple computers, negating the need for centralized control. Further supporting decentralization, P2P networks enable direct transactions between participants, thereby eliminating the requirement for a central authority.

The promise of decentralization underpins many of the proposed benefits of Web3, including transparency, resilience, accessibility, and user empowerment.

However, decentralization exists on a spectrum. Understanding the different degrees and forms of decentralization, and their inherent trade-offs, provides important clarity on the realities and limitations of achieving a fully decentralized web.

Protocols and platforms in Web3 can be categorized across a spectrum of weak to strong decentralization. Weakly decentralized systems still have centralized points of control and failure but open participation. For example, Solana is an open blockchain network but relies on a small number of nodes run by the Solana Foundation to validate transactions. This makes it fast in transaction process but also more centralized. Strongly decentralized systems such as Bitcoin have no central authority and allow open participation in validating and governing the network. Bitcoin is a decentralized digital currency that uses cryptography and a public ledger called the blockchain to verify and record transactions. It was created in 2009 by an unknown person or group under the pseudonym Satoshi Nakamoto (Kaur 2023).

Most Web3 systems exist on a spectrum between these poles. Even strongly decentralized blockchains require some central coordination outside the protocol to fund development. Decentralized autonomous organizations enable community-driven decision-making but often delegate authority to smaller working groups for efficiency (see Chapter 9).

Pure decentralization rarely exists in practice. There are always trade-offs between decentralization and other properties like efficiency, utility, user experience, and regulatory compliance. For example, decentralized storage networks struggle to match the ease of use of centralized cloud storage services. Decentralized stablecoins wrestle with efficient minting and redemption mechanisms.

The dream of a permissionless, autonomous, and anonymous web enabled by pure decentralization remains elusive (Dale 2020). Web3 reflects incremental steps toward dispersing control and participation, not eliminating centralization entirely. As with most complex technologies, success lies in navigating decentralization trade-offs rather than absolutism.

The degrees and dimensions of decentralization should be examined critically in each Web3 context. Blind adherence to decentralization as an end in itself risks curtailing functionality, usability, and commercial viability. However, prudent application of decentralization principles offers a path to harness its benefits while balancing real-world demands.

As Web3 continues maturing from its ideological origins, nuance around decentralization remains vital. Users should scrutinize claims of “complete” decentralization and assess systems based on their unique blend of centralization and distribution. Only through this lens can Web3’s potential be realized.

1.1.2 Blockchain

As a foundational element of Web3, blockchain technology serves as more than just a ledger for recording transactions; it’s the backbone that enables the kind of decentralization and security that sets Web3 apart from Web2. The architecture of blockchain is inherently designed to democratize control and establish trust among participants, which is why it's often referred to as a "trustless" system. This does not mean it's devoid of trust; rather, it signifies that the system is structured in such a way that trust is built in, eliminating the need for centralized intermediaries.

It's crucial to recognize that transactions in the blockchain context are not limited to just financial exchanges. In the realm of Web3, a transaction can encapsulate various types of interaction, including data sharing, contract execution, and even governance decisions. Each of these transactions is verified through a rigorous consensus algorithm, such as proof of work (PoW) or PoS, which ensures that no single entity can unilaterally alter the state of the blockchain. This is a departure from centralized models, where a single entity often has the final say on the validity of transactions.

The term "immutable chain" is not merely a figurative expression. The cryptographic linking of blocks ensures that once data is added to the blockchain, altering it would require an unrealistic amount of computational power. This immutability is a critical feature that brings a new level of security and trust to digital interactions. It's a deterrent against fraud, data tampering, and many forms of cyberattacks, making blockchain technology an attractive solution for not just financial systems but also supply chains, identity management, and even voting systems.

Transparency is another core attribute of blockchain technology, but it's important to understand its nuanced application in Web3. While it's true that blockchain ledgers are typically transparent, meaning that any participant can verify transactions and blocks, there are implementations such as private or consortium blockchains where transparency is selectively applied. Even in public blockchains, advancements in ZKP and other cryptographic techniques are making it possible to maintain privacy without compromising on the integrity and verifiability of transactions (Section 1.1.12).

Security in the blockchain context is multidimensional. While the architecture itself is robust against certain types of cyber threats, it's not an invincible system. The surrounding ecosystem, including smart contracts (Section 1.1.3), dApps (Section 1.1.4), and even the user interfaces to the blockchain, can introduce vulnerabilities. For this reason, a holistic approach to security that encompasses not just the blockchain but also its interacting components is essential in Web3. Chapter 3 will give a more detailed description of blockchain technology.

Blockchain transactions can be slow and resource-intensive due to the fact that the decentralized and distributed nature of blockchains requires consensus and validation across the network before transactions can be added to the blockchain. This process of reaching consensus through mechanisms like PoW mining or PoS voting takes time. The more transactions that need to be validated, the longer it takes. This can lead to delays in transaction approval. Additionally, some blockchains are restricted in how many transactions they can process at one time. For example, Bitcoin is currently limited to around seven transactions per second. So during times of high traffic, transactions get backlogged. The computational power required for the cryptographic hash functions and other validation steps also makes blockchain transactions relatively resource-heavy compared to traditional payment networks. All the nodes in the network have to do redundant work verifying each transaction (See References section).

1.1.3 Smart Contracts

Smart contracts are self-executing agreements coded on the blockchain. They automatically execute predefined conditions once those conditions are met. Smart contracts eliminate the need for intermediaries, providing a trustless environment for conducting transactions and enforcing agreements. They enable the creation of dApps, facilitating a wide range of functionalities such as token issuance, DeFi, and governance mechanisms.

Indeed, smart contracts are one of the most revolutionary innovations brought forth by blockchain technology, serving as the automation and logic layer of the Web3 ecosystem. While blockchain provides the foundational layer of decentralized trust, smart contracts build on this by adding programmable logic to digital agreements. This not only automates the execution of contracts but also extends the utility of blockchain from a passive ledger to an active participant in various types of transactions and interactions.

In a Web3 context, smart contracts serve multiple purposes that go beyond simple transactions. They become the building blocks of more complex dApps, which can range from DeFi platforms to DAOs. Smart contracts can encode complex business logic, governance protocols, and even interactive user interfaces, all while ensuring the benefits of transparency, security, and immutability that come with blockchain technology.

The term “trustless” in the context of smart contracts is particularly noteworthy. As we discussed in Section 1.1.2, this does not imply a lack of trust but rather the obviation of the need for trust. In traditional contractual agreements, trust is often established through legal frameworks, third-party audits, or centralized authorities. Smart contracts, however, make these mechanisms redundant by encoding trust in the form of cryptographic guarantees. Once a smart contract is deployed on the blockchain, its code is visible for anyone to audit, and its execution is guaranteed as long as the network itself remains secure.

The automation provided by smart contracts has profound implications for various sectors. In finance, they enable the creation of complex financial instruments without the need for intermediaries like banks or brokers. In supply chain management, smart contracts can automatically verify and execute steps in the supply chain, providing real-time, immutable tracking data. They also hold potential in legal frameworks, where they can automate the enforcement of contractual clauses, potentially reducing the cost and complexity of legal processes.

However, it’s essential to note that smart contracts are not without their challenges and limitations. The immutability that makes them secure also makes them inflexible. Once deployed, a smart contract’s code cannot be easily altered, which means that any bugs or vulnerabilities are there to stay unless specific upgrade patterns have been implemented. This has led to well-publicized security incidents, highlighting the need for rigorous testing and auditing practices in smart contract development.

Furthermore, while smart contracts can enforce the execution of agreements, they rely on the data they are fed. This raises the issue of “oracle problems,” where the trustworthiness of external data sources becomes a bottleneck in the otherwise trustless environment. Numerous solutions, such as decentralized oracles and data verification layers, are being developed to address these challenges.

Chapter 5 will provide an in-depth examination of smart contracts, dissecting their inner workings, potential applications, and the challenges they pose. As smart contracts continue to evolve and find new applications, their role as the automation and logic layer of Web3 will only become more crucial. Understanding their capabilities, limitations, and the security implications inherent in their use is vital for anyone engaged in the Web3 ecosystem.

1.1.4 dApps

In traditional applications, the centralized architecture often places the user in a dependent position. You entrust your data to the service provider, who stores it on their central servers. This arrangement creates a significant power imbalance because the service provider has unilateral control over the application’s functionality, the user’s data, and even the user’s access to the service itself. In stark contrast, dApps return control to the users. Decentralized applications are built on decentralized technologies such as blockchain. Since data is stored either locally or on the blockchain, the user retains full ownership and control over their information. This does not just offer more privacy and autonomy; it fundamentally reshapes the user's relationship with digital platforms.

Unlike traditional applications that rely on a central server, dApps operate on a P2P network, leveraging the power of distributed consensus. They also ensure transparency, as all transactions and operations are recorded on the blockchain, and are accessible to all participants.

Decentralized applications stand as the real-world manifestation of the theoretical and technological underpinnings of Web3 and blockchain. They are not merely applications that use blockchain as a database; rather, they are holistic applications that function within the decentralized paradigm, embodying its principles from data storage to business logic and user interaction.

The P2P nature of dApps, facilitated by blockchain's distributed consensus mechanisms, adds another layer of robustness and resilience to these applications. By eliminating the need for a central authority or server, dApps are less susceptible to single points of failure. This is not just a theoretical advantage but a practical one that has real-world implications for system uptime, data integrity, and resistance to censorship or external tampering.

Transparency is an intrinsic quality of dApps, stemming from their blockchain foundation. Every transaction, every data change, and every operation is recorded on the blockchain and is publicly verifiable. This level of transparency is unprecedented in traditional digital applications and has significant implications for user trust and system auditability. It also opens up new avenues for community-driven governance models, where changes to the application can be proposed, debated, and implemented in a transparent and democratic way.

However, it's important to note that while dApps offer groundbreaking benefits, they are not a panacea. The same blockchain attributes that offer increased security and transparency can also introduce complexity and potential scalability issues. For example, the computational costs associated with executing smart contracts on a blockchain could become a limiting factor as a dApp grows in popularity and usage. Furthermore, the immutable nature of blockchain data means that any flaws or vulnerabilities in a dApp's smart contract code are permanent unless preemptive measures for upgrades or fixes have been coded in.

The development and deployment of dApps also require a new skill set that goes beyond traditional software development. Understanding the nuances of smart contract programming, the intricacies of decentralized governance, and the complexities of distributed data storage are all integral to building successful dApps. This is where interdisciplinary expertise, combining aspects of software engineering, cryptography, economics, and governance, becomes invaluable.

1.1.5 Interoperability

Interoperability in the context of Web3 is the linchpin that holds the disparate, decentralized systems together in a synergistic relationship. Given that the very essence of Web3 is decentralized and distributed, one can easily envision a scenario where isolated blockchain networks and dApps proliferate, each operating in its own silo. While each of these entities would be powerful in its own right, their true potential can only be fully realized when they can interact and collaborate with one another. This is where interoperability comes into play, serving as the connective tissue that binds these decentralized components into an integrated, functional, and dynamic ecosystem.

The need for interoperability goes beyond mere data exchange; it’s about enabling seamless interactions that can trigger complex operations across multiple blockchains or dApps. For example, a smart contract on one blockchain might need to trigger another smart contract on a different blockchain for a DeFi application to function as intended. This kind of cross-chain interaction would be impossible without robust interoperability protocols.

From a technical standpoint, achieving interoperability is a non-trivial task. It requires sophisticated cryptographic methods, consensus algorithms, and often, dedicated interoperability layers or relayers that act as middlemen between different blockchains. These components must be carefully designed and rigorously tested to ensure they do not introduce vulnerabilities or bottlenecks into the system. The aim is to create a seamless user experience where the complexities of cross-chain interactions are abstracted away, allowing users to enjoy the benefits of a connected Web3 ecosystem without having to navigate its underlying complexities.

From a business perspective, interoperability opens up avenues for new types of collaborations and partnerships between different blockchain projects. It allows for the pooling of liquidity, user bases, and developmental resources, thereby accelerating innovation and adoption. For instance, a DeFi project on one blockchain could tap into a decentralized identity solution on another chain, offering users a more secure and privacy-preserving experience. The synergies created through such collaborations can provide a competitive edge, making interoperability a strategic imperative in the Web3 landscape.

Interoperability also has profound implications for governance and regulatory compliance. As different blockchains may have different governance models or consensus algorithms, interoperable systems need to account for these variations to ensure that cross-chain interactions are not just technically feasible but also governance-compatible. This raises complex questions about jurisdiction, regulatory compliance, and dispute resolution, all of which require thoughtful consideration and, potentially, new legal frameworks.