# SAMPLE

## Building the Blockchain of Tomorrow

A Practical Guide to the Technology Reshaping Trust, Finance, and Digital Infrastructure

Aiman JoeHanz

Free sample: Introduction & Chapter 1

putrabooks.github.io

**Buy the full book:**

Carousell carousell.sg/p/building-the-blockchain-of-tomorrow-ebook-pdf-1465142323

Gumroad

Ko-fi

ElevenReader

Payhip

# Contents

Introduction

Chapter 1: The Current State of Blockchain Technology

Chapter 2: Limitations and Failure Modes of Today's Blockchain

Chapter 3: Common Mistakes in Blockchain Projects

Chapter 4: Foundational Principles of Blockchain Design

Chapter 5: The Step-by-Step Guide to Building Blockchain Applications

Chapter 6: Implementation Strategies for Production Blockchain Systems

Chapter 7: Technology Deep Dive: Consensus, Smart Contracts, and Layer-2

Chapter 8: Case Studies: Real-World Blockchain Deployments

Chapter 9: Evaluating and Testing Blockchain Systems

Chapter 10: The Future of Blockchain

Chapter 11: Action Plan: Building Your Blockchain Practice

Chapter 12: Advanced Topics: Security, Privacy, and Regulatory Compliance

Chapter 13: Building a Blockchain-Ready Organization

Frequently Asked Questions

Glossary

Bibliography

Appendix A: Deep Dive into Smart Contract Vulnerabilities

Appendix B: Token Economics Design

Appendix C: Deployment and Operations Checklist

Appendix D: Platform Comparison

Appendix E: Smart Contract Development Best Practices

Appendix F: Regulatory Reference

Appendix G: Case Study: A Complete DeFi Protocol

Appendix H: Glossary of Attack Vectors

Appendix I: Blockchain Integration Patterns

Appendix J: Frequently Misunderstood Concepts

Appendix K: Development Environment Setup

Appendix L: Key Metrics for Evaluating Blockchain Platforms

Appendix M: Blockchain Development Resources

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

# Introduction

Blockchain is one of the most misunderstood technologies of our era. It has been simultaneously overhyped as the solution to every problem and dismissed as a solution in search of a problem. The reality, as usual, is somewhere in between. The technology has genuine applications where it solves real coordination and trust problems, but it is not a universal replacement for existing infrastructure. Understanding where blockchain adds value and where it does not is the difference between a successful project and an expensive failure.

At its core, blockchain is a distributed ledger technology that enables multiple parties to agree on a shared state without requiring a central authority. This capability—trustless consensus—has applications far beyond cryptocurrency, though cryptocurrency remains the most prominent use case. The fundamental insight is that blockchain enables parties who do not trust each other to transact and collaborate without requiring a trusted intermediary. This is a genuinely new capability that did not exist before Bitcoin introduced it in 2009.

This book is for people who need to understand blockchain as a technology, not as an investment thesis. Software engineers evaluating blockchain for their applications. Product managers considering blockchain-based features. Business leaders deciding whether blockchain is relevant to their industry. Students learning about distributed systems. Anyone who wants to move beyond the hype and understand what blockchain actually does, how it works, and where it is going. The book assumes a basic understanding of software systems but does not require prior blockchain knowledge.

This book covers blockchain as an engineering discipline. It treats blockchain as a distributed system technology with specific capabilities, limitations, and trade-offs. It covers the current state of blockchain technology, including the platforms, protocols, and applications in use today. It covers the limitations and failure modes of current blockchain approaches. It provides a step-by-step guide to building blockchain applications. It covers implementation strategies for production systems. It explores the technology landscape, from consensus algorithms to smart contracts to layer-2 scaling. It presents case studies of real-world deployments. And it looks at the future of blockchain, including the emerging applications and the evolving regulatory landscape.

The book deliberately avoids speculation about cryptocurrency prices, token investment advice, or predictions about which blockchain will dominate. Instead, it focuses on the technology, the engineering decisions, and the

practical considerations of building blockchain systems. The goal is to give you the knowledge to evaluate blockchain for your use case and, if appropriate, to build it.

The book is organized as a progression from diagnosis to prescription. Chapters 1-3 map the current state of blockchain practice: what works, what stalls, and where teams go wrong. Chapters 4-11 deliver the solutions — design principles, step-by-step implementation guides, strategy, technology deep dives, case studies, evaluation methods, and the road ahead. Chapters 12-13 close with advanced topics and how to build an organization that is genuinely blockchain-ready.

Each chapter builds on the previous ones, but the book is also designed to be used as a reference. If you need to understand consensus mechanisms, go to Chapter 7. If you need to evaluate whether blockchain is right for your project, go to Chapter 5. If you need to understand the regulatory landscape, go to Chapter 12. The practical insights and key takeaways at the end of each chapter summarize the most important points for quick reference.

# Chapter 1: The Current State of Blockchain Technology

Blockchain is a distributed ledger that records transactions in blocks, where each block is cryptographically linked to the previous block, creating a chain that is resistant to modification. The key innovation is not the data structure—linked lists have existed for decades—but the combination of cryptographic linking, distributed consensus, and economic incentives that enable multiple parties who do not trust each other to agree on a shared state.

The essential properties of blockchain are: - Immutability: Once data is recorded, it is extremely difficult to change. Each block contains a cryptographic hash of the previous block, so modifying any block requires modifying all subsequent blocks, which requires controlling the majority of the network's computing power (in PoW) or stake (in PoS). - Transparency: All participants can verify the recorded data. On public blockchains, every transaction is visible to anyone. On private blockchains, visibility is restricted to authorized participants, but all authorized participants see the same data. - Decentralization: No single party controls the ledger. Transactions are validated by a distributed network of nodes, and no single node can unilaterally modify the ledger. This is the key differentiator from traditional databases. - Consensus: Participants agree on the state through a defined protocol. Consensus mechanisms (PoW, PoS, PBFT) ensure that all honest participants eventually agree on the same state, even if some participants are malicious.

Understanding these properties is essential because they define both the capabilities and the limitations of blockchain. Immutability provides security but makes bug fixes difficult. Transparency provides auditability but creates privacy challenges. Decentralization removes single points of failure but adds complexity. Consensus enables trustless agreement but limits throughput. Every blockchain design decision involves trade-offs among these properties.

Blockchain has evolved through several distinct phases, each driven by a key innovation:

Phase 1 (2009-2013): Bitcoin and the proof of concept. Blockchain was synonymous with cryptocurrency, and the technology was primarily of interest to cryptographers and libertarians. Bitcoin demonstrated that a decentralized digital currency was possible without a central authority. The blockchain in this phase was simple—a ledger of transactions—but it proved the fundamental concept.

Phase 2 (2014-2017): Ethereum and smart contracts. The realization that blockchain could host programmable logic, not just currency, expanded the technology's potential applications. Ethereum introduced the concept of a virtual machine that could execute arbitrary code on a blockchain, enabling decentralized applications. Initial coin offerings (ICOs) drove significant investment and experimentation, though many projects failed.

Phase 3 (2018-2021): Enterprise blockchain and DeFi. Companies explored private and consortium blockchains for supply chain, identity, and financial applications. Hyperledger Fabric, Quorum, and Corda emerged as enterprise platforms. Simultaneously, the decentralized finance movement built financial applications on public blockchains—lending, trading, derivatives —without traditional intermediaries. Decentralized exchanges, automated market makers, and flash loans were invented.

Phase 4 (2022-present): Maturation and specialization. The focus shifted from "blockchain for everything" to specific use cases where blockchain provides genuine value: settlement, tokenization, supply chain tracking, and identity. Layer-2 scaling solutions became mainstream, reducing transaction costs by orders of magnitude. Major financial institutions began exploring tokenization and CBDCs. The technology matured from speculative experimentation to production deployment.

Today's blockchain ecosystem is diverse and specialized:

Public blockchains (Bitcoin, Ethereum, Solana, Avalanche, Polygon) are open networks where anyone can participate. They use economic incentives (cryptocurrency) to secure the network and achieve consensus. Public blockchains are the most decentralized and censorship-resistant, but they are also the most expensive and slowest. Bitcoin remains focused on store of value and payment. Ethereum is the dominant platform for smart contracts and decentralized applications. Solana prioritizes throughput and low costs. Avalanche offers customizable subnet architecture.

Private and consortium blockchains (Hyperledger Fabric, Quorum, Corda) are permissioned networks where participation is restricted to known parties. They trade decentralization for efficiency and are used in enterprise settings where the participants are known but do not fully trust each other. These platforms can process transactions much faster than public blockchains because they do not need economic incentives or Byzantine fault tolerance at the same scale.

Layer-2 networks (Lightning Network, Optimism, Arbitrum, zkSync) are built on top of public blockchains to improve scalability and reduce costs while inheriting the security of the underlying chain. Layer-2s process transactions

off-chain and settle periodically on the base chain. They have become the primary way to build blockchain applications that need both security and affordability. Transaction costs on layer-2s are typically 10-100x lower than on the base chain.

Application-specific blockchains (appchains) are custom blockchains designed for specific applications, offering optimized performance and customization. Rather than sharing a general-purpose chain with other applications, an appchain dedicates its throughput to a single application. This approach is used by gaming projects, DeFi protocols, and enterprise applications that need predictable performance.

Consensus mechanisms are how blockchain networks agree on the state of the ledger. The choice of consensus mechanism determines the network's security, speed, cost, and energy consumption. The major approaches are:

Proof of Work (PoW): Participants (miners) solve cryptographic puzzles to propose blocks. The first miner to find a valid solution adds the block and receives a reward. PoW is secure but energy-intensive—Bitcoin's network consumes more electricity than some countries. PoW's security comes from the cost of mining: an attacker must control more hash power than the rest of the network to rewrite history, which is prohibitively expensive for established networks.

Proof of Stake (PoS): Participants (validators) stake cryptocurrency to propose blocks. Validators are selected to propose blocks based on their stake

(or randomly among stakers). If a validator acts maliciously—by proposing invalid blocks or going offline—their stake is slashed. PoS is more energy-efficient than PoW by orders of magnitude. Ethereum transitioned from PoW to PoS in 2022, reducing its energy consumption by 99.95%. PoS security comes from the value at risk: an attacker must acquire and risk a large amount of the native token.

Delegated Proof of Stake (DPoS): Stakeholders elect delegates to validate transactions. DPoS is faster but more centralized than standard PoS because only a small number of delegates produce blocks. EOS and Tron use DPoS. The trade-off is throughput versus decentralization—DPoS can process thousands of transactions per second but relies on a small group of delegates.

Practical Byzantine Fault Tolerance (PBFT): A consensus algorithm where validators vote on blocks. PBFT is fast and provides deterministic finality (a confirmed block is immediately final, unlike PoW's probabilistic finality), but requires known validators and does not scale well beyond dozens of participants. Used in Hyperledger Fabric and Tendermint. PBFT is well-suited

for consortium blockchains where the participants are known and relatively few.

Smart contracts are programs that run on a blockchain. They execute automatically when predefined conditions are met, without requiring intermediaries. Smart contracts are the key innovation that distinguishes Ethereum from Bitcoin—they make blockchain a programmable platform, not just a ledger.

Smart contracts enable: - Programmable money: Automatic payments, escrow services, conditional transfers. A smart contract can hold funds and release them only when specific conditions are verified, enabling trustless escrow without a third party. - Tokenized assets: Digital representations of real-world assets. Smart contracts can create and manage tokens that represent anything from currencies to real estate to digital art. - Decentralized applications (dApps): Applications that run on blockchain infrastructure rather than centralized servers. A dApp's backend logic lives in smart contracts, and its frontend is a standard web application that interacts with the blockchain. - Automated governance: Voting, proposal execution, and fund management. Smart contracts can enforce governance rules automatically, ensuring that decisions are executed exactly as voted.

Smart contracts are written in programming languages like Solidity (Ethereum), Rust (Solana), and Move (Aptos, Sui), and are compiled to bytecode that runs on the blockchain's virtual machine. The EVM (Ethereum Virtual Machine) is the most widely used smart contract execution environment. Smart contracts are immutable once deployed (unless upgrade patterns are used), which means bugs are permanent and security is paramount.

Blockchain networks have economic layers that incentivize participation and secure the network. The economic layer is not optional—it is fundamental to how blockchains work. Without economic incentives, there is no reason for participants to maintain the network honestly.

The key economic components are: - Tokens represent value, governance rights, or utility within the network. The native token (e.g., ETH for Ethereum, SOL for Solana) is used to pay for transactions and participate in consensus.

Application tokens may represent governance rights, access to services, or ownership stakes. - Gas fees compensate validators for processing transactions. Gas is a measure of computational work—more complex transactions cost more gas. Gas prices fluctuate based on demand, creating a market for block space. During high-demand periods, gas prices can spike

dramatically. - Staking locks up tokens to secure the network and earn rewards. Validators must stake tokens to participate in consensus, and their stake is at risk if they misbehave. Staking aligns validator incentives with network health—the more they stake, the more they have to lose from misbehavior. - Governance allows token holders to vote on protocol changes. On-chain governance enables decentralized decision- making, though in practice, governance participation is often low and large holders have disproportionate influence.

Blockchain networks process millions of transactions per day. Ethereum processes approximately 1 million transactions per day. Bitcoin processes approximately 400,000. Layer-2 networks like Polygon process millions more. The total value locked in decentralized finance protocols exceeds $50 billion. Cryptocurrency markets trade hundreds of billions of dollars per day. Stablecoins process trillions of dollars in annual transaction volume, rivaling major payment networks.

Despite this scale, blockchain is still far from replacing traditional infrastructure for most applications. The technology faces significant challenges in scalability (blockchains process 15-30 transactions per second at the base layer, while Visa processes 24,000), usability (managing private keys and understanding gas fees is beyond most users), regulation (the regulatory landscape is fragmented and evolving), and energy consumption (though PoS has largely addressed this for new networks).

A common misconception is that blockchain is a replacement for traditional databases. It is not. Blockchain is significantly slower, more expensive, and less flexible than a traditional database. A modern database can process millions of transactions per second with full ACID guarantees. A blockchain processes 15-30 transactions per second at the base layer, with each transaction costing money.

What blockchain provides that databases do not is trustless consensus: the ability for parties who do not trust each other to agree on a shared state without a central authority. This is a capability that no database can replicate. If your application does not need trustless consensus, a database is almost always the better choice—it is faster, cheaper, more flexible, and better supported.

The test is simple: if your application has a trusted operator who controls the data, use a database. If your application involves multiple parties who need to share data but do not trust a single operator to maintain it, blockchain may be appropriate. Supply chain tracking across multiple companies, cross-border payments between different banks, and decentralized lending between

strangers are genuine trust problems. Internal record-keeping, content management, and user analytics are not.

Tokenization—the representation of real-world assets as blockchain tokens—is one of the most significant current trends. Tokenized assets include: - Stablecoins (USDC, USDT): Cryptocurrencies pegged to fiat currencies, providing the stability of fiat with the transferability of crypto. Stablecoins are the most successful tokenized asset, with a combined market capitalization exceeding $150 billion. - Tokenized securities: Digital representations of stocks, bonds, and other financial instruments. Tokenized securities enable faster settlement (minutes instead of days), fractional ownership, and programmable compliance. - Tokenized real estate: Fractional ownership of properties, reducing investment minimums from hundreds of thousands to tens of dollars.

Tokenized real estate enables 24/7 trading and global access to local markets. - Tokenized commodities: Digital representations of gold, oil, and other commodities. Tokenized commodities provide a convenient way to hold exposure to physical assets without the logistics of physical storage. - NFTs: Non-fungible tokens representing unique digital or physical assets. While NFTs are best known for digital art, their broader application is representing ownership of unique items—from event tickets to domain names to in-game assets.

Tokenization enables fractional ownership, faster settlement, and 24/7 trading. However, it also introduces regulatory complexity (tokenized securities may be subject to securities regulation), custody challenges (who holds the physical asset?), and the need for reliable price oracles (how does the blockchain know the real-world price?).

The regulatory landscape for blockchain is evolving rapidly and varies significantly by jurisdiction. This fragmentation creates compliance challenges for projects that operate globally: - United States: The SEC has taken enforcement actions against several token issuers and DeFi protocols, arguing that many tokens are unregistered securities. The CFTC oversees commodity transactions, including Bitcoin and Ether. The ongoing debate about which tokens are securities and which are commodities creates significant uncertainty for token issuers. - European Union: The Markets in Crypto- Assets (MiCA) regulation provides a comprehensive framework for crypto assets, including licensing requirements for crypto service providers, rules for stablecoin issuers, and consumer protection provisions.

MiCA is the most comprehensive crypto regulation enacted by a major economy. - Singapore: The Monetary Authority of Singapore (MAS) operates a licensing regime for digital payment token services. Singapore has positioned

itself as a blockchain-friendly jurisdiction with clear rules, attracting many crypto businesses. - El Salvador: Adopted Bitcoin as legal tender in 2021, making it the first country to do so. The government holds Bitcoin reserves and promotes Bitcoin adoption. - China: Banned cryptocurrency trading and mining in 2021, but actively develops blockchain technology through the Blockchain Service Network (BSN) and the digital yuan CBDC.

Regulatory uncertainty is one of the biggest risks for blockchain projects. Projects must navigate multiple jurisdictions, comply with evolving rules, and plan for regulatory changes. The best approach is to design for compliance flexibility, engage with regulators, and build compliance into the architecture from the start rather than retrofitting it later.

The blockchain developer ecosystem has matured significantly. Development tools have improved, documentation has expanded, and best practices have been established. Key components of the ecosystem include:

- Development frameworks: Hardhat, Foundry, and Brownie provide tools for compiling, testing, and deploying smart contracts. These frameworks include testing environments, debugging tools, and deployment scripts. - Libraries: Web3.js, Ethers.js, and viem provide JavaScript/TypeScript libraries for interacting with blockchains from frontend applications. These libraries handle wallet connections, transaction signing, and contract interactions. - Indexing: The Graph protocol enables efficient querying of blockchain data. Indexers process blockchain events and make them queryable through

GraphQL APIs. - Security tools: Slither, Mythril, and Echidna provide static analysis, symbolic execution, and fuzz testing for smart contracts. These tools help identify vulnerabilities before deployment. - Oracles: Chainlink, Pyth, and API3 provide oracle services that feed real-world data to smart contracts. Oracles are essential for any smart contract that needs external data (prices, weather, sports results).

Enterprise adoption of blockchain follows a consistent pattern. Companies typically begin with a proof of concept to validate the technology, then move to a pilot with a limited scope, and finally to production if the pilot succeeds. The key factors for successful enterprise adoption are:

- Clear use case: Enterprises that succeed with blockchain identify a specific trust problem in their operations—such as supply chain visibility, cross-border payments, or identity verification—and evaluate whether blockchain solves it better than alternatives. - Consortium approach: Many enterprise use cases involve multiple organizations that need to share data. Consortium blockchains, where each organization runs a node, provide the trustless

properties without the transparency of public blockchains. - Integration with existing systems: Enterprise blockchain applications must integrate with existing IT systems—databases, APIs, ERP systems, and identity providers. The integration work is often more complex than the blockchain component itself. - Regulatory compliance: Enterprises must comply with existing regulations, which may constrain how they use blockchain. KYC/AML requirements, data privacy laws, and financial regulations all affect blockchain design.

The gap between blockchain's promise and its current reality is significant. Many promised use cases have not materialized at scale. Supply chain tracking has been piloted extensively but deployed in production by few companies. Tokenized securities have been demonstrated but face regulatory barriers to widespread adoption. Blockchain-based voting has been piloted but faces security concerns that prevent adoption for high-stakes elections.

The gap exists because blockchain's value proposition—trustless consensus—is only valuable in specific contexts. Most business processes already have trusted intermediaries, and replacing them with blockchain adds cost and complexity without adding value. The successful use cases are those where the trust problem is genuine and significant: cross-border payments (no single trusted intermediary), supply chain finance (multiple parties who do not trust each other), and decentralized lending (strangers lending without a bank).

Blockchain's energy consumption, particularly PoW-based blockchains like Bitcoin, has been a significant criticism. Bitcoin's network consumes an estimated 100-150 terawatt-hours per year—comparable to a medium-sized country. This energy consumption is a direct result of PoW's design: security comes from computational cost.

The transition to PoS has largely addressed this concern for new blockchains. Ethereum's transition to PoS reduced its energy consumption by 99.95%. PoS-based blockchains consume negligible energy compared to PoW. However, Bitcoin remains on PoW and is likely to stay there, as changing Bitcoin's consensus mechanism would require consensus among stakeholders who disagree on the change.

The energy debate also involves nuance: much of Bitcoin's mining uses renewable energy (hydroelectric, geothermal, solar) that would otherwise be wasted. Mining operations often locate near excess energy sources. However, this does not eliminate the environmental impact, and the debate continues.

Blockchain does not exist in isolation. It is part of a broader technology landscape and interacts with other technologies:

- Cloud computing: Blockchain applications rely on cloud infrastructure for off-

chain components (indexers, APIs, frontend hosting). Cloud providers offer managed blockchain services (AWS Managed Blockchain, Azure Blockchain Service). - AI: Blockchain and AI are complementary—blockchain provides audit trails for AI decisions, and AI can optimize blockchain operations (gas optimization, anomaly detection). - IoT: IoT devices can record sensor data directly to a blockchain, providing tamper-proof provenance for physical-world data. Supply chain tracking often combines IoT sensors with blockchain ledgers. - Cryptography: Blockchain is fundamentally a cryptographic technology. Advances in cryptography (zero-knowledge proofs, homomorphic encryption, multi-party computation) directly enable new blockchain capabilities.

Blockchain has the potential to address financial inclusion by providing access to financial services for the unbanked population. Over 1.7 billion people lack access to traditional banking. Blockchain-based financial services can provide digital wallets without bank accounts, cross-border remittances at lower cost, access to lending and borrowing, micro-investments through fractional ownership, and identity verification for financial access.

The impact has been most visible in cross-border remittances. Traditional remittances cost an average of 6-8% of the transfer amount. Blockchain-based remittances can reduce this to 1-2%, saving billions of dollars for families in developing countries. Stablecoins have become particularly important in countries with high inflation or unstable currencies—people in Argentina, Turkey, and Nigeria increasingly hold stablecoins as a store of value.

However, the impact has been limited by barriers including smartphone access, internet connectivity, digital literacy, and regulatory restrictions. The potential is real, but the realization requires more than technology—it requires infrastructure, education, and supportive regulation.

Institutional adoption of blockchain and cryptocurrency has accelerated significantly. Major banks offer custody services for digital assets. Bitcoin and Ethereum ETFs have been approved in the United States, providing traditional investors with regulated exposure to cryptocurrencies. Payment companies like PayPal and Square have integrated crypto payments. Investment firms allocate to digital assets as part of diversified portfolios. Central banks worldwide are exploring or piloting CBDCs.

Institutional adoption brings legitimacy, capital, and regulatory clarity. It also brings infrastructure: institutional-grade custody solutions, compliance tools, and trading platforms. However, institutional adoption also brings centralization pressures and conflicts with the decentralized ethos of blockchain. The tension between institutional adoption and decentralization is

a defining dynamic of the current era.

NFTs have been primarily associated with digital art, but their applications extend far beyond creative works. NFTs represent unique digital assets verifiable on a blockchain, and this capability has applications across many domains:

- Digital identity: NFTs representing credentials, memberships, and achievements. A university could issue diplomas as NFTs, enabling instant verification without contacting the university. - Gaming assets: In-game items owned by players, not developers. Players can trade, sell, or carry assets between games, creating real digital ownership. - Domain names: Blockchain-based domain names (ENS, Unstoppable Domains) that are owned rather than rented, with no renewal fees to a centralized registrar. - Event tickets: NFT tickets that prevent fraud and enable secondary market control. Event organizers can set rules for resale prices and earn royalties on secondary sales. - Intellectual property: NFTs representing ownership and licensing rights. Creators can encode licensing terms directly into the NFT, automating royalty payments. - Physical asset provenance: NFTs linked to physical goods for authenticity verification. Luxury goods, art, and collectibles can be tracked from creation to current owner.

The art use case brought attention, but the broader applications of NFTs as unique digital assets have more lasting value.

Decentralized Autonomous Organizations (DAOs) are organizations governed by smart contracts and token holder votes. DAOs enable collective decision-making without centralized leadership, transparent governance with on-chain voting records, programmable rules for fund management and operations, and global participation without geographic restrictions.

DAOs have been used to manage protocol upgrades (Uniswap DAO), treasury management (BitDAO), investment pools (The LAO), and community projects (Friends with Benefits). Some DAOs manage hundreds of millions of dollars in treasury assets.

However, DAOs face challenges: low voter participation (often below 10% of token holders), plutocratic governance (wealthy token holders dominate decisions), coordination challenges for complex decisions, and legal uncertainty about the status of DAOs as legal entities. The DAO governance model is still experimental, and best practices are still evolving. Innovations like delegation (token holders delegate votes to experts), conviction voting (preference strength increases over time), and quadratic voting (reduces the influence of large holders) are being tried.

Blockchain and cloud computing are complementary technologies. Cloud providers (AWS, Google Cloud, Azure) offer blockchain services, and blockchain applications rely on cloud infrastructure for off-chain components. The integration of blockchain with cloud services enables managed blockchain nodes, blockchain-as-a-service (BaaS), scalable off-chain infrastructure, integration with existing cloud-native applications, and hybrid architectures combining cloud and blockchain.

Cloud providers offer managed blockchain services that handle node operations, upgrades, and scaling. This lowers the barrier to entry for organizations that want to use blockchain without managing infrastructure. However, managed blockchain services introduce a degree of centralization—the cloud provider becomes a trusted party for availability, if not for data integrity.

Stablecoins—cryptocurrencies pegged to stable assets like the US dollar—have become a critical component of the blockchain ecosystem and increasingly of the broader financial system. The three main types of stablecoins are:

Fiat-backed (USDC, USDT): Reserves of fiat currency back each token. The issuer holds dollars in a bank account, and users can redeem tokens for dollars. These are the most widely used and most stable, but they rely on centralized issuers and banking relationships. Transparency of reserves is a key concern—issuers publish regular attestations of their reserves, but the quality of these attestations varies.

Crypto-backed (DAI): Over-collateralized with cryptocurrency reserves. Users lock up crypto collateral (e.g., ETH) in a smart contract and receive stablecoins. The system is decentralized but more complex and potentially volatile during market stress. If the value of the collateral drops too quickly, the system may become undercollateralized.

Algorithmic (formerly UST): Maintain peg through algorithmic mechanisms without full backing. The collapse of Terra/UST in 2022, which destroyed $40 billion in value, demonstrated the fragility of algorithmic stablecoins. This category is now viewed with significant caution by regulators and users alike.

Stablecoins serve as the reserve currency of DeFi, the unit of account for trading, and the bridge between traditional and blockchain-based finance. The total stablecoin market exceeds $150 billion, and stablecoins process trillions of dollars in annual transaction volume. The regulatory scrutiny of stablecoins is intensifying, with proposals for bank-like regulation, reserve requirements, and transparency standards in multiple jurisdictions.

Supply chain finance involves multiple parties—manufacturers, suppliers,

logistics providers, banks, and buyers—who need to coordinate payments, documentation, and goods movement. Traditional supply chain finance is slow, paper-heavy, and opaque. A single international trade transaction can involve over 20 documents, 40 discrete approvals, and up to 40 days to complete.

Blockchain can improve supply chain finance by providing a shared, transparent ledger for all parties, enabling smart contracts that automate payment on delivery, reducing fraud through immutable documentation, improving visibility for financing decisions, and reducing the cost of trade finance documentation. The key insight is that supply chain finance involves a genuine trust problem—no single party trusts the others—making it a natural fit for blockchain.

Several major banks and logistics companies have implemented blockchain-based supply chain finance platforms. TradeLens (Maersk and IBM) and we.trade (consortium of European banks) demonstrated real improvements in speed and transparency, though both have since been discontinued, highlighting that blockchain alone is not sufficient—business model and adoption matter too.

Digital identity is a growing application of blockchain technology. Current identity systems are fragmented, controlled by centralized entities, and vulnerable to data breaches. Every time you create an account with a new service, you repeat the identity verification process. Every service stores your identity data, creating multiple attack surfaces.

Blockchain-based identity systems provide self-sovereign identity where users control their own identity data, verifiable credentials that are cryptographically provable, privacy-preserving verification (proving attributes without revealing them), portability across services and platforms, and decentralization with no single point of failure.

The W3C has established standards for Decentralized Identifiers (DIDs) and Verifiable Credentials, providing a foundation for interoperable identity systems. Several countries are exploring blockchain-based national identity systems, and enterprise applications are emerging in KYC/AML compliance, where a verified identity on a blockchain can be reused across multiple financial institutions without each one re-verifying from scratch.

Blockchain has been proposed as a solution for secure voting. The potential benefits include transparency (votes can be verified by anyone), immutability (votes cannot be changed once cast), accessibility (remote voting without sacrificing security), and auditability (complete, verifiable audit trail).

However, blockchain voting faces significant challenges. Coercion is

fundamentally unpreventable in remote voting—someone can stand over a voter and watch them vote. Device security is a concern—user devices may be compromised. Privacy is critical—public blockchains may not protect vote privacy adequately. Scale is an issue—national elections have millions of voters. Complexity matters—voters may not understand the system and trust it less as a result.

Several pilots have been conducted, but most security experts remain cautious about blockchain voting for high-stakes elections. The technology may be more suitable for low-stakes governance (DAO votes, organizational elections, shareholder voting) than for national elections where the stakes and attack surface are much higher.

Institutional DeFi—traditional financial institutions using decentralized finance protocols—is a growing trend. Banks, hedge funds, and asset managers are exploring DeFi for yield generation, efficient settlement, and access to new markets. The total value locked in DeFi exceeds $50 billion, and institutional participation is increasing.

However, institutional DeFi faces challenges: regulatory compliance (institutions must comply with KYC/AML, which DeFi protocols typically do not enforce), custody (institutions need qualified custody for digital assets), risk management (DeFi protocols have been hacked, and institutions need to manage this risk), and operational integration (integrating with traditional trading and risk systems). Solutions like permissioned DeFi pools, where only KYC-verified participants can interact, are emerging to bridge this gap.

Trade finance—letters of credit, guarantees, and other instruments that facilitate international trade—is a natural blockchain use case. The process is paper-intensive, involves multiple banks across jurisdictions, and takes weeks to complete. Blockchain can reduce trade finance to days by providing a shared ledger where all parties can verify documents and approvals in real time.

Several trade finance platforms built on blockchain have been deployed: Contour (formerly eTradeConnect) for letter of credit issuance, Marco Polo for trade finance, and Batavia for cross-border trade settlements. These platforms demonstrate real efficiency gains, but adoption has been limited by the need for all parties in a trade transaction to use the same platform. Network effects are essential—trade finance platforms are only valuable if all participants are on them.

Healthcare involves multiple parties (hospitals, doctors, insurers, patients) who need to share sensitive data but do not fully trust each other. Blockchain can

provide a secure, auditable layer for healthcare data exchange: medical records with patient-controlled access, pharmaceutical supply chain tracking (to prevent counterfeit drugs), clinical trial data integrity, insurance claim verification, and consent management.

The sensitivity of healthcare data makes blockchain applications particularly challenging. HIPAA compliance, patient privacy, and the large volume of healthcare data (which cannot be stored on-chain) require careful architecture. Most healthcare blockchain applications store data off-chain (encrypted) and use the blockchain for access control and audit trails.

Governments are exploring blockchain for various applications: land registries (immutable property records), identity systems (national digital identity), voting (as discussed above), tax collection (transparent tax tracking), procurement (auditable government contracts), and CBDCs (digital currency issuance).

Several countries have piloted blockchain-based government services. Estonia has been a pioneer with its e-residency program and blockchain-based health records. Georgia piloted blockchain for land registry. Sweden explored blockchain for land titles. Dubai has a blockchain strategy for government documents. These pilots demonstrate the potential but also the challenges—government blockchain systems must integrate with legacy systems, comply with legal requirements, and serve populations with varying digital literacy.

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.