Trollip's Degen Almanack

Justin Trollip

2024-12-09

Table of contents

Welcome

This Almanack represents an attempt to document cryptocurrency and Web3 knowledge without the conflicts of interest that plague our industry. Just as Henry Varnum Poor created his Manual of Railroads to bring transparency to America's railroad boom, this Almanack aims to bring clarity to the cryptocurrency revolution.

Why This Almanack Exists

The cryptocurrency industry suffers from a unique problem: those with the deepest knowledge often have the strongest financial incentives to mislead others. Protocol developers promote their own chains, influencers pump their own holdings, and "researchers" serve those who pay them. Meanwhile, crucial information remains locked behind paywalls and exclusive groups.

This Almanack breaks that pattern by providing:

- Comprehensive knowledge from basic concepts to advanced strategies
- Independent analysis free from token-holder influence
- Technical depth that doesn't sacrifice accessibility
- Practical guidance for both users and developers

How to Use This Almanack

Whether you're seeking financial sovereignty or building the future, this Almanack offers multiple paths:

For Those Seeking Independence
Start with "Regular Person's Path to Independence" to understand how to safely participate in the cryptocurrency ecosystem without falling prey to scams or losing your funds.

For Technical Minds
The "Technical" section provides deep dives into cryptography, blockchain architecture, and protocol design patterns. Consider starting with "Web3 Essentials" to establish a common vocabulary.

For Market Participants
The “Financial” section offers frameworks for analyzing digital assets, understanding market structures, and evaluating protocols.

Living Document

This Almanack is version controlled through Git and continuously updated by community contributions. Every technical claim is justified, every strategy explained, and every risk clearly stated. You’re reading an early draft, dated December 2024.

Contributing

Knowledge critical to digital independence should be freely accessible. This work is licensed under Creative Commons Attribution-ShareAlike 4.0, ensuring it remains open while preventing commercial exploitation. Learn more in our “Contributing” section.

Begin your journey with the topics listed in the navigation menu, or proceed systematically through each section. Welcome to your guide to digital independence.

Part I

Introduction

Copyright Notice

Motivation

Knowledge critical to achieving financial sovereignty should never be locked behind paywalls or restrictions. The crypto industry already suffers from enough artificial barriers - gated Discord servers, exclusive research groups, and insider knowledge networks that perpetuate inequality.

This Almanack exists to break down these barriers. Just as Bitcoin enables permissionless financial transactions, this work aims to enable permissionless learning. However, we must also prevent others from creating new barriers around this knowledge.

This is why we've chosen the Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0). This copyleft license ensures that:

1. Anyone can freely access, share, and build upon this work
2. Any derivative works must maintain the same freedoms
3. Commercial use is permitted, but cannot restrict access
4. Attribution protects the community's contributions
5. The viral nature of ShareAlike prevents future enclosure

Think of it like a smart contract for knowledge: immutable rules that protect freedom while enabling innovation.

Legal Text

Version Control

This work is version controlled through Git. Each version represents a distinct iteration of the Almanack, identified by commit hashes and release tags. While the content may evolve, this license remains constant across all versions.

You can find the complete version history and contribute to future versions at: https://github.com/HariSeldon23/ almanack

Attribution Example

When sharing or building upon this work, please provide attribution in the following format:

“This work is based on Trollip’s Degen Almanack © 2024 Justin Trollip, used under CC BY-SA 4.0. [Your modifications, if any]”

Contact

For questions about usage or licensing, contact: jtrollip@protonmail.com

---

The above represents the formal terms under which this Almanack is shared. In the spirit of transparency and accessibility that cryptocurrency enables, we've chosen these terms to ensure this knowledge remains as free as the protocols it describes.

Dedication

For my two skebangas. Huxley & Morrissey

Epigraph

“Arise, you have nothing to lose but your barbed wire fences!”
— Timothy C. May (1988)

Preface

The cryptocurrency revolution has created unprecedented opportunities for financial independence, but it has also spawned an industry rife with exploitation. As someone deeply embedded in this world, I face a moral dilemma: I can either participate in a system that profits from obscuring knowledge, or I can work to make that knowledge freely accessible to all.

This Almanack represents my choice of the latter path. Just as the cypherpunks believed privacy and freedom of information could coexist, I believe we can build a more equitable crypto ecosystem without compromising its innovative potential. The fundamental act of friendship among cryptocurrency enthusiasts – what I call "degens" – should be the sharing of knowledge, not the hoarding of it.

The technical complexity of cryptocurrency has created a particularly insidious form of gatekeeping. Essential market data and analysis hide behind expensive paywalls. Crucial insights remain locked in exclusive chat groups and private networks. This artificial scarcity of knowledge directly contradicts the core ethos of Web3: permissionless access and decentralized power.

This Almanack aims to break down these barriers. It will serve as a comprehensive, freely accessible resource covering everything from basic concepts to advanced trading strategies. More importantly, it will evolve through community contributions, ensuring it stays relevant and accurate as the industry develops.

Some might question why I would freely share knowledge that others sell at a premium. My answer is simple: the long-term health of our ecosystem depends on educated participants making informed decisions. When knowledge is concentrated in the hands of a few, it creates the very centralization of power that cryptocurrency was meant to disrupt.

Looking ahead, I envision this Almanack becoming a living document that adapts to the rapid changes in our industry. I'm exploring sustainable open-source funding models, potentially through platforms like Mirror that allow for anonymous contributions. This would ensure the Almanack can continue growing while maintaining its independence from traditional financial incentives.

This is just the beginning. The path to truly democratized crypto knowledge will require continuous effort and collaboration. If you share this vision, I invite you to contribute your expertise, suggest improvements, or simply help spread the word. Together, we can build something that honors the original promise of cryptocurrency: financial sovereignty for all.

The work begins now.

1 Introduction

The crypto industry suffers from a unique paradox: those with the deepest knowledge often have the strongest incentives to obscure rather than illuminate. This troubling reality became clear to me during a technical debate I witnessed on Twitter. Both participants made valid points, yet instead of building understanding, they resorted to personal attacks. What struck me wasn't just the hostility, but the absence of a shared framework for discussion – a common language that could bridge their perspectives.

This observation rekindled an idea I'd been considering for years: creating a comprehensive blockchain taxonomy. But as I began mapping out the technical architecture of various networks, I realized the scope needed to be much broader. The same knowledge gaps that hindered technical discussions were even more pronounced in everyday conversations about cryptocurrency investment and usage.

I thought about the countless conversations I've had with friends and family seeking crypto advice. These weren't developers or traders – they were curious individuals trying to understand a complex new technology. Despite years of experience in the industry, I struggled to give them guidance that was both accessible and comprehensive. The existing resources either oversimplified to the point of uselessness or drowned readers in technical jargon.

This Almanack aims to bridge that gap. Drawing inspiration from Henry Varnum Poor's Manual of Railroads, which brought transparency to America's railway boom, we're creating a resource that serves both technical and non-technical audiences. Just as Poor's manual helped investors understand the revolutionary technology of his time, this Almanack aims to demystify the crypto revolution for everyone.

The name "Trollip's Degen Almanack" might seem unusual. Initially, I considered calling it a blockchain taxonomy or a Web3 guide. But these terms felt too limiting. The word "degen" – short for degenerate – carries special meaning in crypto culture. While often used ironically to describe risk-taking traders, being a degen also implies deep engagement with the technology and markets. It's through this engaged experimentation that true understanding emerges.

What sets this Almanack apart is its commitment to intellectual honesty and practical utility. We're building it as an open-source, community-reviewed resource that will evolve alongside the technology it describes. The documentation uses version control through Git, allowing readers to track how understanding changes over time. As the industry matures, we plan to integrate real-time data sources, transforming this from a static document into a dynamic tool for decision-making.

The Almanack is organized into distinct paths catering to different needs:

- The Path to Independence guides those seeking financial sovereignty
- The Technologist's Path provides deep technical understanding
- The Financial sections offer frameworks for analysis and investment

Each section builds upon the others, creating a comprehensive resource that grows with your understanding. Whether you're a developer looking to understand economic implications, an investor studying technical fundamentals, or someone simply seeking financial independence, you'll find your path forward here.

This is an ambitious undertaking, and like any first edition, it will contain errors and omissions. But by maintaining rigorous standards for evidence, encouraging community contributions, and staying true to the open-source ethos, we aim to create something valuable: a trusted guide through the often confusing world of cryptocurrency and Web3.

The journey begins here. Welcome to your guide to digital independence.

2 How to Use This Almanack

This almanack serves multiple audiences with different needs and backgrounds. Whether you're seeking financial independence, building decentralized systems, or analyzing crypto markets, this guide will help you navigate the content effectively.

2.1 Understanding the Structure

The almanack is organized into progressive sections that build upon each other while remaining independently accessible. Think of it like a city with different districts - you can start in any area that interests you, but the main roads connect everything in a logical way.

2.1.1 For Those Seeking Financial Independence

If your primary goal is achieving financial sovereignty through cryptocurrency, begin with:

1. Start with the "Foundations" section to understand basic tools and security
2. Move to "Path to Independence" which provides step-by-step guidance
3. Reference the "Financial Systems" section as you advance
4. Explore other sections based on your growing interests and needs

2.1.2 For Technical Minds

If you're approaching from a technical perspective, particularly as a builder or developer:

1. Begin with "Technical Architecture" to understand fundamental concepts
2. Explore "Applications & Use Cases" for implementation patterns
3. Study "Financial Systems" to understand the economic aspects
4. Reference "Governance & Social Coordination" for broader ecosystem context

2.1.3 For Market Participants

If you're focused on trading, investing, or market analysis:

1. Start with "Financial Systems" for core concepts
2. Explore "Technical Architecture" to understand underlying technology
3. Study "Governance & Social Coordination" for market-moving factors
4. Reference other sections as needed for comprehensive understanding

2.2 Using the Rating Systems

This almanack includes several rating frameworks to help you evaluate:

- Digital assets and protocols
- Security considerations
- Market opportunities
- Technical architectures

When using these ratings:

- Consider them starting points rather than absolute truth
- Look at the underlying metrics and methodology
- Understand how different factors are weighted
- Apply the frameworks to your own analysis

2.3 Working with Technical Content

Technical sections include:

- Code examples
- Architecture diagrams
- Mathematical formulas
- Protocol specifications

These are designed to be both rigorous and accessible:

- Begin with conceptual overviews
- Study detailed explanations
- Experiment with provided examples
- Reference external resources when needed

2.4 Understanding Risk

Throughout the almanack, risk is treated as a fundamental concept:

- Security risks are covered in technical sections
- Market risks are detailed in financial sections
- Social risks are explored in governance sections
- Operational risks are discussed in implementation guides

Always consider risk factors before implementing any strategy or system described here.

2.5 Contributing and Staying Updated

This is a living document that improves through community contribution:

- Check version numbers and update dates
- Review the contribution guidelines
- Submit improvements or corrections
- Join related discussions

2.6 Making the Most of Examples

The almanack includes numerous examples:

- Case studies of successful and failed projects
- Code implementations
- Market analyses
- Governance scenarios

Use these to:

- Understand theoretical concepts in practice
- Learn from others' experiences
- Identify patterns and anti-patterns
- Develop your own analytical frameworks

2.7 Following the Learning Paths

While sections can be read independently, certain learning paths are recommended:

2.7.1 Beginner Path

1. Basic terminology and concepts
2. Setting up essential tools
3. Security fundamentals
4. First interactions with crypto

2.7.2 Intermediate Path

1. Understanding market dynamics
2. Technical architecture basics
3. Risk management principles
4. Advanced tools and strategies

2.7.3 Advanced Path

1. Complex technical concepts
2. Advanced market analysis
3. Protocol design patterns
4. Governance mechanisms

2.8 Getting Help

If you encounter difficulties:

- Review prerequisite sections
- Check the glossary for unfamiliar terms
- Reference external resources
- Engage with the community
- Submit questions through appropriate channels

Remember that this almanack is designed to grow with you. As your understanding deepens, previously complex sections will become more accessible, and new layers of insight will emerge from familiar content.

3 Web3 Terminology

3.1 Introduction

Understanding Web3 requires familiarity with a unique vocabulary that spans multiple disciplines: cryptography, economics, computer science, and social coordination. This guide organizes these terms into logical categories and provides clear explanations with relevant examples.

3.2 Evolution of the Web

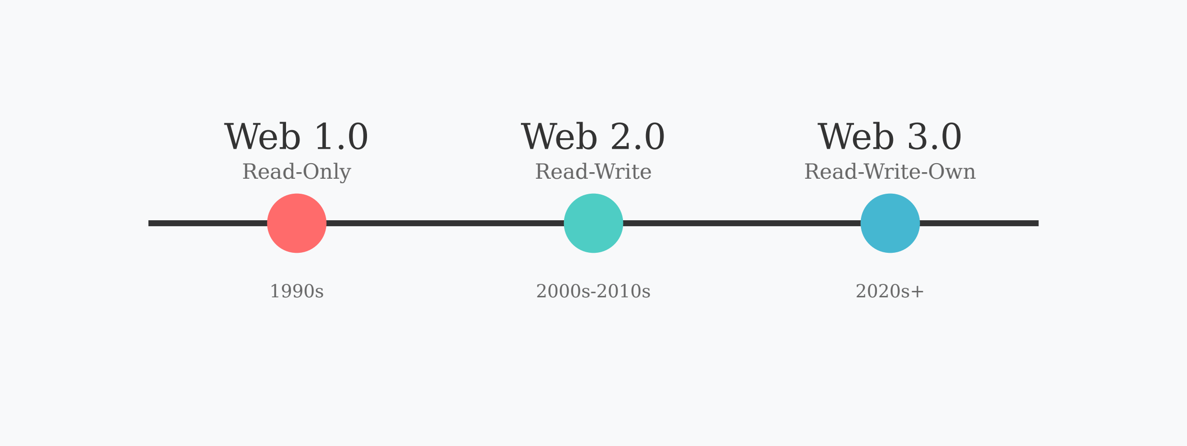

Figure 3.1: Evolution of the Web

3.2.1 Web 1.0 (1990-2004)

The first iteration of the worldwide web consisted primarily of static websites that users could only read. Information flowed in one direction - from website owners to visitors. Think of early news websites or company homepages that rarely changed and offered no interaction.

3.2.2 Web 2.0 (2004-2020)

The social web emerged, characterized by user-generated content, social networks, and interactive platforms. Users could both read and write content, but platforms owned and controlled the data. Facebook, Twitter, and YouTube exemplify Web 2.0 platforms where users create content but don't truly own or control it.

3.2.3 Web3 (2020-Present)

The ownership web represents a fundamental shift where users can read, write, and own their digital assets and data. Instead of trusting platforms to manage our digital lives, Web3 uses cryptographic protocols and economic incentives to enable direct ownership and peer-to-peer interactions.

3.3 Core Concepts

3.3.1 Decentralization

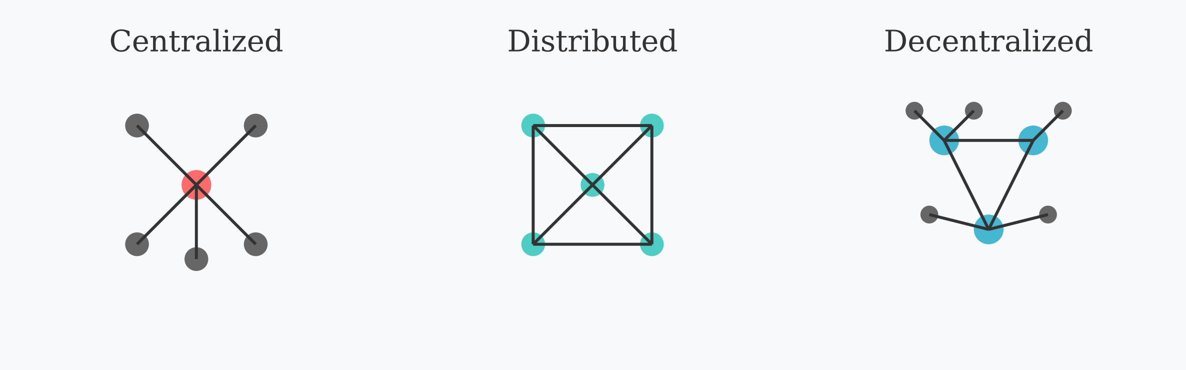

Figure 3.2: Decentralization

Decentralization refers to the distribution of power, control, and decision-making across a network rather than concentration in a single entity. It exists on a spectrum:

1. **Architectural Decentralization**: How many physical computers comprise the system?
2. **Political Decentralization**: How many individuals or organizations control those computers?
3. **Logical Decentralization**: Does the interface and data structures appear more like a single monolithic object, or an amorphous swarm?

Examples help illustrate these distinctions:

- Bitcoin is architecturally and politically decentralized but logically centralized (one shared ledger)
- Email is architecturally decentralized but politically centralized (few major providers) and logically centralized (standardized protocol)
- Language is decentralized across all three dimensions

3.3.2 Blockchain

A blockchain is a distributed database that maintains a continuously growing list of records (blocks) that are cryptographically linked to previous records. Key characteristics include:

1. **Immutability**: Once data is recorded, it cannot be altered without changing all subsequent blocks
2. **Transparency**: All transactions are public and verifiable
3. **Consensus**: Network participants agree on the state of the system without trusting each other

The term “blockchain” has become somewhat limiting - many modern systems use different data structures while maintaining similar properties. This is why some prefer broader terms like “distributed ledger technology” or “decentralized incentive networks.”

3.4 Account Types

3.4.1 Simple Accounts

Simple accounts represent the most basic way to interact with blockchain networks. They have:

- A public key (like an email address)
- A private key (like a password)
- The ability to hold and transfer native network tokens
- No additional programmable logic

3.4.2 Smart Accounts

Smart accounts extend simple accounts with programmable functionality:

- Custom validation logic
- Multi-signature requirements

- Automated actions
- Integration with smart contracts

For example, a smart account might require two out of three designated signatures to approve transactions or automatically split incoming payments between multiple recipients.

3.5 Digital Assets

3.5.1 Native Coins

Native coins (sometimes called protocol tokens) are the primary digital assets of blockchain networks. They serve several purposes:

- Pay for transaction fees (gas)
- Secure the network through staking or mining
- Participate in governance
- Transfer value

Examples include:

- Bitcoin (BTC) on the Bitcoin network
- Ether (ETH) on Ethereum
- SOL on Solana

3.5.2 Tokens

Tokens are digital assets created on top of blockchain platforms. They differ from native coins because they don't secure the underlying network. Major categories include:

3.5.2.1 Fungible Tokens

Interchangeable tokens where each unit is identical to every other unit. Think of them like traditional currency - any dollar bill can be exchanged for any other dollar bill. Categories include:

- Stablecoins (USDC, DAI)
- Governance tokens (UNI, AAVE)
- Security tokens
- Utility tokens

3.5.2.2 Non-Fungible Tokens (NFTs)

Unique digital assets where each token has distinct properties. Common uses include:

- Digital art and collectibles
- Gaming items
- Domain names
- Membership passes
- Real estate titles

3.6 Financial Concepts

3.6.1 Decentralized Finance (DeFi)

Financial services built on blockchain networks that operate without traditional intermediaries. Key components include:

3.6.1.1 Automated Market Makers (AMMs)

Smart contracts that create liquidity pools allowing users to trade tokens without traditional order books. Instead of matching buyers with sellers, users trade against a pool of tokens with prices determined by mathematical formulas.

3.6.1.2 Yield Farming

The practice of providing liquidity or assets to DeFi protocols in exchange for rewards, typically in the form of governance tokens or trading fees.

3.6.1.3 Impermanent Loss

A unique risk in liquidity provision where the value of assets deposited in an AMM pool can decrease relative to simply holding those assets, due to price movements and the AMM's constant product formula.

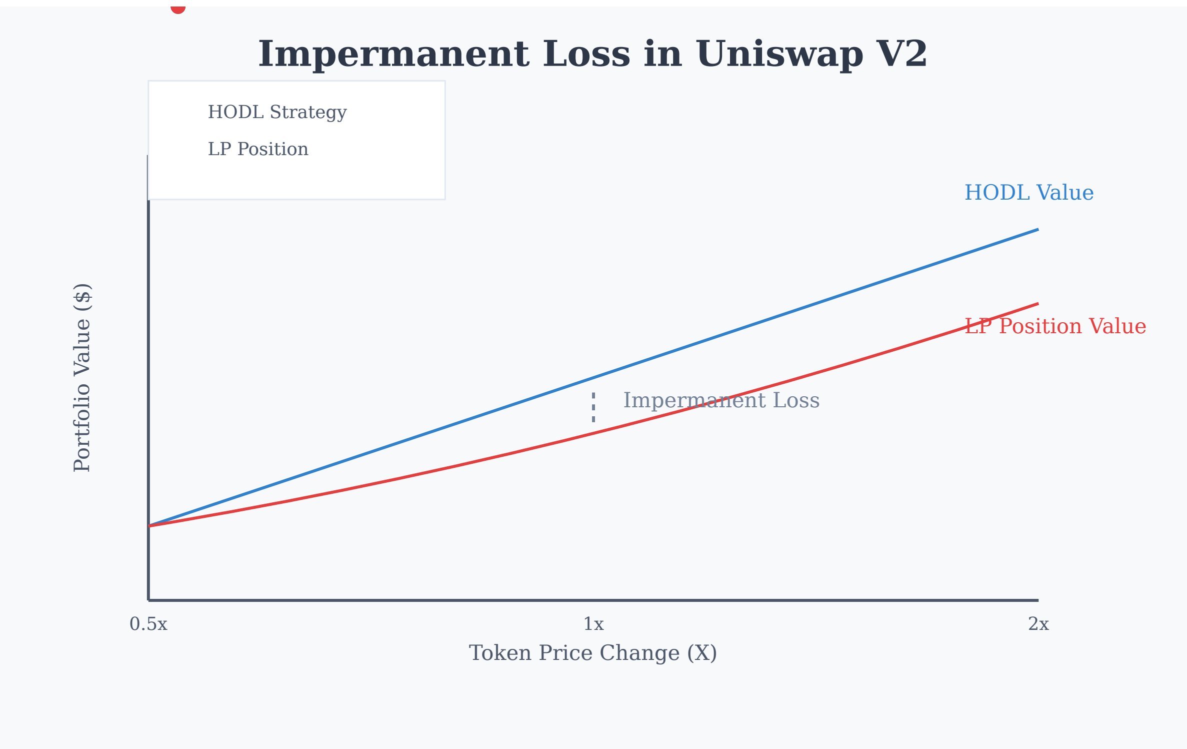

Figure 3.3: Impermanent Loss

3.7 Cultural Terms

3.7.1 HODL

Originally a misspelling of "hold" that became crypto slang for maintaining long-term positions regardless of market conditions. The term evolved to mean "Hold On for Dear Life" and represents a conviction-based investment strategy.

3.7.2 Degen

Short for "degenerate," this term began as criticism of high-risk trading behavior but has been reclaimed by the community to describe sophisticated traders who:

- Take calculated risks
- Deeply understand protocol mechanics
- Stay ahead of market trends
- Actively participate in new protocols

3.7.3 Gas

Transaction fees paid to network validators, typically priced in the network's native token. Gas prices fluctuate based on network demand, with higher prices during periods of congestion.

3.7.4 Gwei

A denomination of ETH, specifically 10^-9 ETH. Commonly used to express gas prices on Ethereum and EVM-compatible networks.

3.8 Security Concepts

3.8.1 Seed Phrase

A sequence of 12-24 words that serves as a backup for private keys. Also called a mnemonic phrase or recovery phrase. The words are selected from a standardized list of 2048 words and must be stored securely, as anyone with access to the seed phrase can control the associated accounts.

3.8.2 Smart Contract

Self-executing programs stored on a blockchain that automatically enforce and execute agreements between parties. Key characteristics:

- Immutable once deployed
- Transparent and verifiable
- Execute exactly as programmed
- No downtime or censorship

Part II

Foundations

4 Digital Independence

The story of digital independence begins not with blockchains or cryptocurrencies, but with a profound recognition: the tools that brought unprecedented convenience to our lives have also created unprecedented control over them.

Consider your daily financial life. Your morning coffee purchase creates a data point. Your salary arrives through systems you don't control. Your savings exist primarily as numbers in someone else's database. This convenience comes with hidden costs - your transactions can be blocked, your accounts frozen, your privacy compromised. Each small sacrifice of control seemed reasonable in isolation, but together they've created golden handcuffs of financial dependence.

This isn't accidental. The post-industrial financial system runs on centralization because it's efficient. Banks can process thousands of transactions per second. Credit cards work seamlessly across borders. Mobile payments happen with a fingerprint. But this efficiency masks a fundamental truth - you're asking permission to use your own money.

The early cypherpunks understood this tradeoff. In 1993, Eric Hughes wrote in the Cypherpunk Manifesto:

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

They saw that digital privacy would become inseparable from freedom. Without privacy in our transactions and communications, true independence would be impossible. But they also understood that simply criticizing the system wasn't enough - they needed to build alternatives.

This brings us to public key cryptography, the foundation of digital independence. Imagine having a special lock that anyone can use to send you messages or money, but only you can open. No permission needed, no middlemen required, no central authority to approve or deny. This isn't just technical theory - it's a practical tool for independence.

Bitcoin emerged from this foundation, but it would be a mistake to see it as just digital money. It proved that we could create systems where trust comes from mathematics and consensus rather than institutions. Where rules are enforced by code rather than policy. Where participation is permissionless rather than granted.

The path to digital independence isn't about rejecting modern convenience - it's about reclaiming control while preserving it. We'll learn to:

- Hold assets that can't be frozen or seized
- Communicate without surveillance
- Trade without gatekeepers
- Build systems that resist control

But this power comes with responsibility. In traditional systems, mistakes can often be reversed. Passwords can be reset. Transactions can be disputed. In truly independent systems, you alone are responsible for your security. Your privacy. Your choices.

This Almanack exists because that responsibility requires knowledge. Not just technical knowledge, though that's important, but practical wisdom. Understanding not just how these systems work, but why they matter. Learning not just to use tools, but to think independently about digital freedom.

The journey of digital independence is both personal and collective. Each person who takes control of their digital life strengthens the network for everyone. Each developer who builds privacy-preserving tools expands what's possible. We're not just users of a new system - we're participants in its evolution.

In the coming chapters, we'll explore both the philosophical foundations and practical tools of digital independence. Whether you're a developer looking to build these systems or someone seeking to use them, understanding these foundations is essential. Because digital independence isn't given - it's learned, practiced, and ultimately, earned.

5 The Path to Digital Money

From Ciphers to Smart Contracts

The story of cryptocurrency begins long before Bitcoin. It starts with a simple question that has challenged mathematicians and philosophers for millennia: How can we share secrets safely?

Ancient Rome used the Caesar cipher to protect military communications. Medieval merchants developed complex codes to secure trade routes. During World War II, the breaking of the Enigma machine's encryption changed the course of history. Each advance in cryptography came from the need to communicate privately in an unsafe world.

But the true revolution began in the 1970s with two breakthroughs that would eventually make digital money possible: public key cryptography and the development of secure network protocols.

In 1976, Whitfield Diffie and Martin Hellman solved a problem that had seemed impossible: how could two people who had never met establish a shared secret over an insecure channel? Their solution, known as public key cryptography, created the foundation for secure digital communications. A few years later, Ron Rivest, Adi Shamir, and Leonard Adleman developed the RSA algorithm, making these theoretical ideas practical.

The 1980s saw the birth of the Cypherpunk movement. These technologists and privacy advocates believed that cryptography could protect individual liberty in the digital age. They weren't just mathematicians – they were philosophers who saw privacy as essential to human dignity and freedom.

David Chaum, a pioneer in cryptographic privacy, proposed the first digital cash system in 1983. His DigiCash company later implemented these ideas, but ultimately failed – partly because it remained centralized, requiring trust in a single company.

The 1990s brought both advances and setbacks. Phil Zimmermann released PGP (Pretty Good Privacy), bringing strong encryption to everyday users. The U.S. government, viewing strong cryptography as a national security threat, tried to mandate backdoors through the Clipper Chip. The resulting "Crypto Wars" ended with cryptography being classified as protected speech.

Through these battles, the Cypherpunks refined their vision. In 1993, Eric Hughes published "A Cypherpunk's Manifesto," declaring that "privacy is necessary for an open society in the electronic age." The movement explored various approaches to digital money: Nick Szabo's bit gold, Wei Dai's b-money, and Adam Back's Hashcash all contributed crucial ideas.

Then came 2008. As the global financial system teetered on the brink of collapse, an anonymous figure calling themselves Satoshi Nakamoto published a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin solved a problem that had stymied previous attempts at digital money: how to achieve consensus about ownership without trusting any central authority.

Bitcoin's genius lay in combining existing technologies in a novel way. It used public key cryptography for identity, cryptographic hash functions for mining, and a distributed ledger to record transactions. Most importantly, it created an economic incentive structure that made the system self-sustaining.

The early Bitcoin years were marked by experimentation and growing pains. The first known commercial transaction occurred in 2010 when Laszlo Hanyecz paid 10,000 BTC for two pizzas – bitcoins that would later be worth hundreds of millions of dollars. Mt. Gox, the largest Bitcoin exchange, collapsed in 2014, teaching harsh lessons about the risks of centralized custody.

By 2013, a young programmer named Vitalik Buterin saw both Bitcoin's potential and its limitations. Bitcoin's simple scripting language was intentionally restricted to prevent complex computations that could slow the network. Buterin proposed Ethereum, a platform that would add a complete programming language to blockchain technology.

Ethereum launched in 2015, introducing the concept of smart contracts – self-executing programs stored on the blockchain. This opened up entirely new possibilities. Instead of just transferring value, users could create complex financial instruments, digital organizations, and decentralized applications.

The next major innovation came in 2018 with the launch of Uniswap, which introduced automated market makers (AMMs) to crypto. Traditional order book exchanges require active market makers to provide liquidity. AMMs used smart contracts to create passive, algorithm-driven markets that could operate 24/7 without human intervention.

This sparked the DeFi (Decentralized Finance) revolution. Compound introduced algorithmic lending markets. Aave pioneered flash loans. Curve optimized stable asset trading. Each innovation built on previous ones, creating increasingly sophisticated financial infrastructure.

But Ethereum's success brought scaling challenges. High transaction fees during peak usage made smaller transactions impractical. This spurred development of alternative approaches. Solana launched in 2020, using a proof-of-history mechanism to achieve higher throughput. The Move programming language, first developed for Facebook's Libra project, influenced platforms like Aptos and Sui that prioritized safer smart contract development.

Layer 2 scaling solutions emerged as another approach. Optimistic rollups like Arbitrum and Optimism, and zero-knowledge rollups like zkSync and StarkNet, aimed to increase Ethereum's capacity while inheriting its security. Each made different tradeoffs between speed, cost, and decentralization.

This brings us to today. We've moved from simple ciphers to programmable money, from centralized experiments to decentralized networks. Each step built on previous innovations while solving new challenges. Understanding this history helps us appreciate both how far we've come and the challenges that still lie ahead.

The cypherpunks believed privacy tools could reshape society. They were right, but perhaps not in the way they expected. Cryptocurrency has indeed changed how we think about money, but its greatest impact may be in showing that alternative financial systems are possible. As we look to the future, we carry forward their core insight: mathematical tools, properly designed, can create new forms of human coordination and freedom.

6 The Search for Alternatives

Promise and Compromise

When you deposit money in a bank, you're making a trade. You gain convenience but surrender control. Your money becomes an entry in someone else's database. Your privacy becomes a policy in someone else's rulebook. Your financial freedom becomes subject to someone else's discretion.

For decades, we accepted this trade because we had no alternative. But different groups have increasingly questioned whether this bargain serves their interests. Their reasons reveal both the promise of decentralized systems and the challenges they face.

6.1 Regular People's Motivations

For many people, the search for alternatives begins with personal experience. Perhaps it's a Venezuelan family watching inflation devour their savings, or a Nigerian entrepreneur unable to receive international payments. Maybe it's an American discovering their bank account has been frozen without explanation, or a privacy-conscious individual uncomfortable with every purchase being tracked.

These experiences share a common thread: the realization that traditional financial systems grant enormous power to intermediaries while offering users surprisingly few protections. Consider these common scenarios:

- A bank can freeze your accounts without warning or immediate recourse
- Payment processors can refuse to serve legal but "high-risk" businesses
- Governments can impose capital controls during economic crises
- Financial surveillance tracks nearly every transaction you make
- Inflation can steadily erode purchasing power
- International transfers incur high fees and lengthy delays

Each of these represents a failure of centralized systems to serve basic human needs: the need to save without fear of confiscation, to transact without excessive surveillance, to maintain privacy without sacrificing convenience.

6.2 Technologists' Motivations

For technologists, the appeal of decentralized systems often starts with recognizing their elegant solutions to complex problems. How do you create digital scarcity without central control? How do you achieve consensus among untrusting parties? How do you build systems that remain secure even when some participants are malicious?

But deeper motivations often emerge:

- The desire to build systems that can't be corrupted by concentrated power
- The technical challenge of creating truly trustless protocols
- The vision of enabling new forms of human coordination
- The goal of making financial services universally accessible
- The drive to reduce society's dependence on trusted intermediaries

6.3 Core Principles

These diverse motivations converge around several core principles:

- **Self-Sovereignty**: The idea that individuals should have direct control over their assets and data. This means holding private keys rather than trusting custodians, controlling your own identity rather than relying on centralized providers, and maintaining ownership of your data rather than surrendering it to platforms.

- **Censorship Resistance**: The ability to transact and communicate without permission from authorities. This doesn't just mean resistance to government censorship – it includes resistance to corporate policies, payment processor restrictions, and other forms of private sector control.

- **Trustless Systems**: Protocols that work through mathematical guarantees rather than institutional trust. Instead of having to trust that a bank will honor its obligations, users can verify the system's operation directly through code and cryptography.

6.4 The Compromise of Success

Yet crypto's growing success has brought compromise. The same industry that began as a rebellion against financial intermediaries now builds new forms of intermediation. Venture capital firms that once missed the internet boom now rush to stake their claims. Wall Street, initially dismissive, now sees opportunities for familiar forms of financial engineering.

This transformation is evident in several trends:

- The rise of centralized exchanges that function much like traditional brokerages
- The push toward regulatory compliance that recreates existing financial structures
- The focus on token prices over technological advancement
- The concentration of wealth and influence among early investors
- The emphasis on speculation over actual utility

Some compromises were perhaps inevitable. Mass adoption requires user-friendly interfaces, institutional investment needs regulatory clarity, and complex systems benefit from specialized service providers. But other changes represent a more fundamental drift from crypto's founding principles.

Consider how: - "Not your keys, not your coins" became "Trust our custody solution" - "Censorship resistant" became "Compliant with all regulations" - "Trustless" became "Trust our proprietary trading engine" - "Decentralized" became "Controlled by a small group of token holders"

6.5 Finding Balance

Yet this story isn't simply one of ideals corrupted by commerce. The reality is more nuanced. While some projects have abandoned core principles in pursuit of profit, others maintain a careful balance. True decentralization coexists with user-friendly interfaces. Privacy-preserving protocols operate alongside regulated exchanges.

The challenge ahead lies in preserving crypto's essential promise – financial sovereignty, censorship resistance, and trustless operation – while making these benefits accessible to ordinary users. This might mean:

- Building better self-custody solutions that match centralized convenience
- Creating privacy-preserving compliance mechanisms
- Developing truly decentralized governance systems
- Focusing on real-world utility over speculation
- Maintaining open protocols alongside commercial services

The original vision of cryptocurrency remains powerful: a world where financial freedom doesn't require anyone's permission, where privacy is protected by mathematics rather than policies, and where trust comes from transparent code rather than opaque institutions. Realizing this vision means neither rejecting all compromise nor accepting every dilution of principle, but rather finding ways to make radical ideas practical.

For both regular people and technologists seeking alternatives to centralized systems, the core question remains: How do we build systems that preserve freedom while serving human needs? The answer may lie not in choosing between idealism and practicality, but in finding ways to achieve both.

7 Tools

7.1 Introduction

The Web3 ecosystem requires specialized tools for interacting with blockchains, managing digital assets, and analyzing on-chain data. This guide provides a detailed overview of essential tools across different categories, helping users understand when and how to use each one effectively.

7.2 Wallets

Wallets serve as your primary interface with blockchain networks. Understanding the different types and their security implications is crucial for safely participating in Web3.

7.2.1 Hardware Wallets

Hardware wallets store private keys in secure hardware devices, providing the highest level of security for long-term storage.

7.2.1.1 Ledger

- Supports multiple application models (Account, UTXO, Resource, Actor)
- Available on desktop and mobile
- Proprietary secure element chip
- Regular firmware updates
- Supports 5000+ cryptocurrencies

Key features:

- Clear signing screen for transaction verification
- Secure element certification
- Desktop and mobile companion apps
- DApp integration capabilities

7.2.1.2 Trezor

- Open-source hardware and firmware
- Supports Account (EVM) and UTXO models
- Browser-based interface
- Shamir backup feature
- Focuses on Bitcoin and EVM chains

7.2.2 Software Wallets

Software wallets offer greater convenience but with increased security risks compared to hardware solutions.

7.2.2.1 MetaMask

- Primary gateway to EVM networks
- Browser extension and mobile app
- Built-in token swap feature
- Custom network support
- Extensive DApp integration

Best practices:

- Never share seed phrase
- Use with hardware wallet for large amounts
- Regularly check token approvals
- Keep browser extension updated

7.2.2.2 Phantom

- Multi-chain support (Solana, EVM, Bitcoin)
- Mobile and browser extension
- Built-in NFT support
- SOL staking integration
- Token swap functionality

7.2.2.3 Safe (formerly Gnosis Safe)

- Multi-signature wallet platform
- Advanced security features
- Treasury management tools
- Transaction batching
- Custom access controls

7.3 Centralized Exchanges (CEXs)

While centralized exchanges present counterparty risks, they remain crucial infrastructure for entering and exiting the crypto ecosystem.

7.3.1 Key Considerations for CEX Selection

1. Security Track Record

- Historical hacks or breaches
- Insurance coverage
- Cold storage policies
- Security certifications

2. Liquidity Depth

- Trading volume verification
- Order book depth
- Market maker relationships
- Wash trading detection

3. Regulatory Compliance

- Licensing status
- Jurisdictional restrictions
- KYC/AML procedures
- Asset segregation

4. Feature Set

- Supported cryptocurrencies
- Trading pair availability
- Fiat on/off ramps
- Advanced trading features

7.3.2 Notable Exchange Failures and Lessons

1. Mt. Gox (2014)

- Loss: 850,000 BTC
- Lesson: Importance of proof of reserves

2. FTX (2022)

- Loss: $8-10 billion
- Lesson: Dangers of commingled funds

3. Celsius Network (2022)

- Loss: $4.7 billion
- Lesson: Risks of CeFi lending platforms

7.4 Analysis Tools

7.4.1 On-Chain Analysis Platforms

7.4.1.1 Block Explorers

Block explorers provide detailed information about transactions, addresses, and smart contracts on specific networks.

1. Etherscan (Ethereum)

- Transaction tracking
- Contract verification
- Gas tracker
- Token approvals
- API access

2. Solana Explorer

- Program interaction tracking
- Account management
- Stake delegation monitoring
- Vote account tracking

7.4.1.2 Portfolio Trackers

7.4.1.2.1 DeBank

- Comprehensive DeFi position tracking
- Cross-chain support
- Real-time updates
- Historical performance
- Risk monitoring

Best for:

- Active DeFi users
- Multi-chain portfolios
- Yield farming tracking

7.4.1.2.2 Zapper

- NFT integration
- Bridge tracking
- Portfolio history
- DeFi dashboard
- Cross-chain support

Ideal for:

- NFT collectors
- DeFi participants
- Multi-chain users

7.4.2 Professional Analysis Tools

7.4.2.1 Data Query Platforms

1. Dune Analytics

- SQL-based queries
- Custom dashboard creation
- Community-driven insights
- Historical data access
- Real-time analytics

2. Nansen

- Wallet labeling
- Smart money tracking
- Token flow analysis
- NFT market insights
- Investment signals

7.5 Security Tools

7.5.1 Smart Contract Analysis

7.5.1.1 OpenZeppelin

- Security auditing tools
- Contract templates
- Upgrade management
- Access control
- Gas optimization

Best practices:

- Regular security reviews
- Automated testing
- Upgrade planning
- Access control management

7.6 Privacy Tools

Privacy tools help protect user identity and transaction privacy while interacting with Web3 platforms.

7.6.1 VPN Services

When selecting a VPN for Web3:

- Look for no-log policies
- Check jurisdiction
- Verify cryptocurrency payment support
- Test connection stability
- Evaluate server locations

Recommended Services:

- Mullvad VPN (accepts Bitcoin, focused on privacy)
- ProtonVPN (cryptocurrency support, Swiss jurisdiction)

7.6.2 TOR Network

- Provides network-level privacy
- Multiple relay encryption
- Bridge support for censorship resistance
- Integration with privacy-focused tools

8 Protecting Your Assets

The decentralized nature of cryptocurrency creates unique security challenges. While traditional finance offers safety nets like fraud protection and account recovery, crypto operates on the principle of absolute ownership - which means absolute responsibility. This guide will help you understand and protect against the major ways people lose their crypto assets.

8.1 Understanding Private Key Security

Your private key is like the master key to a vault - anyone who has it can access everything inside. Unlike a physical key, it can't be copied by someone who briefly sees it, but it also can't be replaced if lost. This creates two opposing risks we must balance: the risk of loss and the risk of theft.

8.1.1 Securing Your Private Key

Think of your private key (usually represented as a seed phrase) as the most sensitive information you own. Good security practices include:

1. Physical Security
   - Write your seed phrase on durable materials (steel or titanium for long-term storage)
   - Store copies in multiple secure locations
   - Consider dividing the phrase into parts stored separately
   - Never store digitally or take photos
2. Access Planning
   - Create a clear inheritance plan
   - Document recovery procedures for family members
   - Consider multi-signature setups for large holdings
   - Test recovery procedures periodically

8.1.2 Common Private Key Mistakes

Many losses occur through simple oversights:

- Taking photos of seed phrases
- Storing phrases in cloud services or password managers
- Using phrases generated by others
- Entering phrases on suspicious websites
- Sharing phrases with "support staff"

8.2 Understanding Technical Risks

Technical risks often arise from misunderstanding how blockchain systems work. Let's examine the most common technical failures and how to prevent them.

8.2.1 Network Selection Errors

Blockchain networks are separate universes - sending assets to the wrong network often means permanent loss. Protection requires:

1. Always verify the network before transactions
2. Start with small test transactions
3. Use address book features in wallets
4. Understand bridge mechanisms between networks

8.2.2 Gas and Transaction Mechanics

Transaction failures often come from misunderstanding gas (transaction fees):

1. Low Gas Issues

    - Transactions can get stuck
    - Some tokens can become temporarily locked
    - Emergency cancellation may require high fees

2. High Gas Mistakes

    - Overpaying during network congestion
    - Not understanding fee calculations
    - Falling for gas token scams

8.2.3 Smart Contract Interactions

Smart contracts introduce complex risks:

1. Token Approvals
   - Never approve unlimited spending
   - Regularly review and revoke approvals
   - Use token allowance checkers
   - Understand the contracts you're interacting with
2. Contract Verification
   - Check contract addresses on block explorers
   - Verify official documentation
   - Be wary of cloned contract names

8.3 Understanding Social Engineering

Social engineering attacks exploit human psychology rather than technical vulnerabilities. These attacks are particularly dangerous because they bypass security measures by tricking you into taking harmful actions.

8.3.1 Common Attack Patterns

1. Authority Exploitation
   - Fake customer support
   - Impersonated team members
   - False urgency messages
   - Regulatory compliance scams
2. FOMO (Fear of Missing Out) Manipulation
   - Limited time offers
   - Exclusive access promises
   - Artificial scarcity
   - Pump and dump schemes
3. Trust Exploitation
   - Fake testimonials
   - Manufactured social proof

- Community infiltration
- Long-term relationship building

8.3.2 Protection Strategies

1. Verification Procedures

   - Always use official channels
   - Verify team member identities
   - Check multiple sources
   - Never act under time pressure

2. Communication Hygiene

   - Ignore direct messages about crypto
   - Never share private information
   - Be skeptical of unsolicited offers
   - Verify URLs carefully

8.4 Smart Contract Vulnerabilities

Smart contract risks require special attention because they can affect many users simultaneously and often can't be fixed once discovered.

8.4.1 Risk Categories

1. Implementation Flaws

   - Logic errors
   - Mathematical errors
   - Access control issues
   - Race conditions

2. Economic Vulnerabilities

   - Flash loan attacks
   - Price manipulation
   - Liquidity attacks
   - Governance attacks

3. External Dependencies

- Oracle failures
- Bridge compromises
- Network congestion
- Protocol interactions

8.4.2 Protection Measures

1. Due Diligence

   - Check audit reports
   - Review attack history
   - Understand dependencies
   - Monitor protocol metrics

2. Risk Management

   - Start with small amounts
   - Diversify across protocols
   - Monitor security alerts
   - Maintain exit strategies

8.5 Building Security Habits

Security in crypto requires developing consistent habits:

1. Regular Security Reviews

   - Check wallet connections
   - Review token approvals
   - Update security software
   - Test backup procedures

2. Transaction Hygiene

   - Verify all details multiple times
   - Use test transactions for new operations
   - Maintain separate wallets for different purposes
   - Keep detailed records

3. Continuous Learning

   - Study new attack vectors
   - Update security practices

- Share knowledge with others
- Learn from others' mistakes

Remember: In crypto, security isn't a destination - it's a continuous process of learning, adapting, and staying vigilant. The best security measures are the ones you actually use consistently.

Part III

Path to Independence

9 Starting Your Web3 Journey

9.1 Phase 1: Understanding the Basics

Before touching any money or creating accounts, let's build your foundation of knowledge. Think of this like learning to recognize road signs before driving a car.

9.1.1 Essential Terms

Start by familiarizing yourself with the fundamental vocabulary in Chapter "Terms". Key concepts you need to understand first include:

- Web3 and decentralization
- Blockchain basics
- Public and private keys
- Gas fees and transaction costs
- Smart contracts

9.1.2 Cultural Context

The Web3 community has its own culture, largely expressed through memes. Review Chapter "Memes" to understand:

- "Not your keys, not your coins" - why self-custody matters
- "HODL" - the philosophy of long-term holding
- The evolution of different crypto communities
- Common scam warnings and red flags

9.1.3 Required Tools

You'll need specific tools to interact with Web3. Reference Chapter "Tools" for details on:

- Wallets (MetaMask, hardware wallets)
- Block explorers
- Portfolio trackers

- Security tools

9.2 Phase 2: Security First

Before handling any real money, we need to establish secure practices. Security isn't optional - it's the foundation everything else builds upon.

9.2.1 Protecting Your Assets

From the Chapter "Don't Lose Your Money":

1. Private Key Management
   - Never share your seed phrase
   - Secure storage methods
   - Backup procedures
   - Emergency access plans
2. Creating Safe Wallets
   - Setting up MetaMask securely
   - Creating a "burner" wallet for testing
   - Understanding hardware wallet benefits
   - Using multiple wallets for different purposes
3. Privacy Considerations
   - The Tornado Cash situation
   - Legal implications of privacy tools
   - Alternative privacy methods
   - Balance between privacy and compliance

9.3 Phase 3: Getting Started

Now that you understand the basics and security fundamentals, it's time to enter the ecosystem.

9.3.1 Your First Crypto Purchase

Following the Chapter “First Steps”:

1. Start Small
   - Buy your first $10 of Bitcoin
   - Understand exchange basics
   - Learn about order types
   - Practice secure withdrawals
2. Understanding Fees
   - Different fee markets (overview with links to Technical section)
   - How gas prices work
   - Choosing the right time to transact
   - Estimating transaction costs

9.3.2 Creating Your Web3 Identity

1. Setting Up MetaMask
   - Proper installation and security
   - Network configuration
   - Backup procedures
   - Test transactions
2. Creating Clean Wallets
   - Understanding wallet separation
   - Privacy tool options
   - Legal considerations
   - Operational security

9.4 Phase 4: Basic Operations

Now you’re ready to start using Web3 services while maintaining security.

9.4.1 Essential Skills

1. Using DEXes (Decentralized Exchanges)
    - Trading on Uniswap
    - Understanding liquidity pools
    - Managing slippage
    - Avoiding common pitfalls
2. Bridging Between Networks
    - Understanding bridge risks
    - Choosing reliable bridges
    - Managing cross-chain assets
    - Minimizing bridge costs

9.4.2 DeFi Fundamentals

1. Lending Markets
    - How lending protocols work
    - Borrowing against your Bitcoin
    - Managing collateral ratios
    - Understanding liquidation risks
2. Yield Strategies
    - Basic yield farming
    - Risk assessment
    - Sustainable practices
    - Tax considerations

9.5 Phase 5: Advanced Operations

Once comfortable with basics, you can explore more sophisticated strategies.

9.5.1 Sustainable Practices

1. Cash Flow Management
   - Using lending markets effectively
   - Managing borrowed positions
   - Creating sustainable yield
   - Emergency procedures
2. Off-ramping Strategies
   - Converting crypto to fiat
   - Tax compliance
   - Banking relationships
   - Local regulations

10 Your First Steps

10.1 Introduction

Taking your first steps into Web3 can feel like learning to walk in a new world. The concepts may be unfamiliar, and the stakes feel high since real money is involved. This chapter will guide you through your initial journey, ensuring you start with strong fundamentals while maintaining security at every step.

10.2 Your First Cryptocurrency Purchase

10.2.1 Choosing Your Entry Point

Your first cryptocurrency purchase represents more than just buying digital assets—it's about learning to navigate a new financial system. We'll start small, with just $10 worth of BTC (Bitcoin). This amount is chosen carefully: it's enough to learn the mechanics but small enough that mistakes won't be devastating.

10.2.2 Selecting an Exchange

For your first purchase, we'll use a regulated cryptocurrency exchange. While decentralized options exist, centralized exchanges offer important advantages for beginners:

- Familiar payment methods (bank transfers, credit cards)
- Customer support for common issues
- Regulated entities with clear legal obligations
- Simple user interfaces

Popular options include:

- Coinbase: Known for ease of use (recommended for this guide)
- Kraken: Strong security history
- Gemini: Regulatory compliance focus

10.2.3 Step-by-Step Purchase Process

1. Registration

   - Use a strong, unique password
   - Enable two-factor authentication **immediately**
   - Complete identity verification (KYC)
   - Secure your recovery options

2. Funding Your Account

   - Start with a small test deposit
   - Document all transaction details
   - Understand processing timeframes
   - Verify fees before proceeding

3. Making Your First Purchase

   - Navigate to the Bitcoin trading page
   - Select “Buy” or “Market Buy”
   - Enter $10 USD (or local equivalent)
   - Review the quoted price and fees
   - Confirm the transaction

4. Understanding Order Types

   - Market Orders: Instant execution at current price
   - Limit Orders: Set your desired price
   - Stop Orders: Automated triggers for buying/selling
   - Pros and cons of each approach

10.2.4 After Your Purchase

Immediately after buying, familiarize yourself with:

- Transaction history viewing
- Price alerts setting
- Account statements
- Tax reporting requirements

10.3 Creating Your Web3 Identity

10.3.1 The Importance of Self-Custody

While keeping your first Bitcoin purchase on the exchange is acceptable temporarily, true participation in Web3 requires self-custody through wallets you control. This begins with setting up Phantom.

10.3.2 Phantom Setup Guide

1. Installation
    - Use official sources only
    - Chrome/Firefox/Brave supported
    - Mobile options available
    - Verify extension authenticity
2. Initial Configuration
    - Create new wallet
    - Record seed phrase properly
    - Set strong password
    - Understand recovery options
3. Security Best Practices
    - Never share seed phrase
    - Use hardware wallet for large amounts
    - Regularly check connected sites
    - Update extension promptly
4. Network Configuration
    - Understanding Bitcoin Mainnet
    - Recognizing test networks
    - Managing network switching

10.3.3 Creating Clean Wallets

As you progress in Web3, wallet separation becomes crucial. Think of wallets like different bank accounts—each serving a specific purpose.

1. Wallet Types
    - Main Wallet: Your primary identity
    - Trading Wallet: For DeFi interactions
    - Gaming Wallet: For Web3 games
    - Test Wallet: For trying new protocols
2. Privacy Considerations
    - Transaction history is public
    - Address clustering risks
    - Block explorer visibility
    - Network analysis implications
3. Operational Security
    - Different devices for different wallets
    - Clean transaction patterns
    - Cross-chain considerations
    - Interaction compartmentalization
4. Legal and Privacy Tools
    - VPN usage pros and cons
    - Mixer considerations
    - Jurisdiction awareness
    - Compliance documentation

10.4 Your First Transactions

10.4.1 Understanding Network Fees

Before making your first transaction, understand that every blockchain action has a cost:

1. Fee Components
    - Base network fees
    - Priority fees (tips)
    - Contract interaction costs

    - Failed transaction fees

2. Timing Considerations

    - Network congestion patterns
    - Gas price variations
    - Weekend vs weekday differences
    - Time zone impacts

10.4.2 Practice Transactions

Start with small test transactions to build confidence:

1. Send a minimal amount between your own wallets
2. Interact with a simple smart contract
3. Add/remove liquidity from a DEX
4. Try a cross-chain bridge

10.4.3 Common Pitfalls to Avoid

1. Technical Mistakes

    - Insufficient gas allocation
    - Wrong network selection
    - Incorrect address input
    - Contract approval limits

2. Security Risks

    - Phishing websites
    - Fake tokens
    - Malicious smart contracts
    - Social engineering attempts

10.5 Next Steps

After completing these initial steps, you'll be ready to:

- Explore DeFi protocols
- Participate in DAOs
- Trade on DEXs
- Investigate yield opportunities

Remember: The goal of these first steps isn't to make money—it's to build a strong foundation for your Web3 journey. Take your time, double-check everything, and don't rush into complex interactions until you're completely comfortable with the basics.

10.6 Emergency Procedures

Keep this information readily available:

- How to revoke contract approvals
- Emergency contact information for exchanges
- Local crypto-friendly legal resources
- Asset recovery procedures

Stay curious, but always prioritize security and understanding over speed and potential profits.

11 DeFi Fundamentals

11.1 Introduction

Decentralized Finance (DeFi) represents a fundamental reimagining of financial services. While traditional finance relies on banks, brokers, and other intermediaries, DeFi uses smart contracts – self-executing computer programs – to enable direct peer-to-peer financial activities. This shift removes gatekeepers and creates opportunities for anyone with an internet connection to access sophisticated financial services.

While Ethereum pioneered DeFi, its high transaction costs can make learning expensive, with fees sometimes exceeding $50 per transaction. This is why we'll start our journey on Base, a Layer 2 network built on top of Ethereum. Base offers the same capabilities but with dramatically lower fees, typically under $1 per transaction. This makes it perfect for learning DeFi without fear of expensive mistakes.

11.2 Getting Your First ETH on Base

Now that you have Bitcoin in your Phantom wallet from following our earlier steps, we need to get some ETH on Base to begin exploring DeFi. We'll use Coinbase for this process since they built Base and offer direct deposits.

11.2.1 Direct Purchase Method

The most straightforward approach is:

1. On Coinbase Exchange:
   - Purchase $50-100 worth of ETH
   - Select "Withdraw"
   - Choose "Send to Base"
   - Send to your Phantom wallet's Base address

This method is optimal because: - Coinbase handles the bridge transaction for you - You avoid paying Ethereum mainnet gas fees - The process is simpler than manual bridging - Base transaction fees are much lower

11.2.2 Understanding Base vs Ethereum

Base maintains a special relationship with Ethereum: - It inherits Ethereum's security - Uses the same wallet addresses - Runs the same smart contracts - Costs much less to use

Think of Base like an express lane on a highway - it's faster and cheaper while still getting you to the same destination safely.

11.3 Your First DeFi Steps

Before diving into trading and lending, let's verify everything is working:

1. Initial Setup Check
    - Confirm ETH appears in your Phantom wallet on Base
    - Ensure you've selected Base network
    - Have your Phantom wallet connected to Base
    - Keep transaction records for taxes
2. Test Transaction
    - Send a tiny amount of ETH ($1 worth) between your own addresses
    - Notice how the gas fees are much lower than Ethereum
    - Get comfortable with Base network mechanics
    - Understand transaction confirmation times

11.4 Trading Fundamentals

When it comes to trading tokens on Base, using a DEX aggregator provides significant advantages over using any single decentralized exchange. Let's understand why and how to trade effectively.

11.4.1 Understanding DEX Aggregators

DEX aggregators are like smart shopping assistants that find the best prices across multiple exchanges. We recommend ParaSwap for several reasons:

1. Gas Efficiency
    - Optimizes routes to minimize gas costs
    - Particularly effective on Base's already low-fee environment
    - Helps make small trades viable

2. User Experience
    - Clean, intuitive interface
    - Clear transaction previews
    - Easy-to-understand settings
3. Price Optimization
    - Splits orders across multiple DEXs when beneficial
    - Protects against price impact
    - Finds efficient trading paths

11.4.2 Your First Trade Using ParaSwap

Let's walk through converting some ETH to USDC:

1. Preparation
    - Visit ParaSwap's official website (always verify the URL)
    - Connect your Phantom wallet
    - Verify you're on Base network
    - Ensure sufficient ETH for both trade and gas
2. Making the Trade
    - Select ETH as your "from" token
    - Choose USDC as your "to" token
    - Enter a small test amount ($10 worth)
    - Review the quoted price and gas fees
    - Understand the suggested route
    - Confirm the transaction

11.4.3 Understanding Slippage and Price Impact

When trading on Base, it's crucial to understand how trade size affects price:

1. Slippage
    - The difference between expected and executed price
    - Larger trades typically experience more slippage
    - ParaSwap helps minimize this through smart routing
2. Price Impact
    - How your trade affects market price
    - Depends on available liquidity
    - Visible before trade execution

11.5 Understanding Gas on Base

While Base uses the same gas system as Ethereum, the costs are much lower:

1. Typical Base Costs

   - Simple transfers: $0.01-0.05
   - Token swaps: $0.10-0.30
   - Complex DeFi operations: $0.20-0.50 Compare this to Ethereum's fees which can be 50-100x higher!

2. Gas Management

   - Keep $5-10 worth of ETH for gas
   - Monitor network conditions
   - Understand peak usage times
   - Plan non-urgent transactions

11.6 Lending Markets with Aave on Base

Now that you're comfortable with basic transactions and trading, let's explore lending markets. Aave is one of DeFi's most battle-tested lending protocols and has deployed on Base.

11.6.1 How Aave Works

Think of Aave like a decentralized bank where you can both lend and borrow crypto assets:

1. Lending Assets When you lend on Aave:

   - You receive aTokens representing your deposit
   - Interest accrues automatically in your wallet
   - You can withdraw anytime (subject to liquidity)
   - Your deposit can serve as collateral for borrowing

2. Understanding Collateral and Borrowing Aave uses an overcollateralized lending model:

   - You must maintain a minimum health factor
   - Different assets have varying collateral factors
   - Monitor your position's health regularly
   - Understand liquidation risks

3. Safety First

   - Always maintain a health factor above 1.5
   - Set up notifications for position health

- Keep some ETH for emergency transactions
- Know how to repay loans quickly

[Continue with Yield Strategies, Portfolio Building, Emergency Procedures sections as before...]

11.7 Monitoring Your DeFi Activity

Stay informed about your DeFi positions:

1. Essential Tools
   - DeFiLlama for protocol TVL and health
   - Base block explorer for transactions
   - Aave dashboard for loan positions
   - ParaSwap analytics for trading data
2. Regular Checks
   - Monitor lending positions daily
   - Review transaction history weekly
   - Track portfolio performance
   - Stay updated on protocol changes

Remember: While Base's low transaction costs make DeFi more accessible, never invest more than you can afford to lose. Start small, learn the mechanics, and scale up gradually as you gain confidence and understanding.

12 DeFi Fundamentals

12.1 Introduction

While Ethereum created DeFi and remains its foundational layer, starting your DeFi journey directly on Ethereum can be expensive due to high transaction fees (sometimes $50+ per transaction). Fortunately, Base, a layer 2 network built on top of Ethereum, offers the same fundamental DeFi capabilities but with dramatically lower fees (often less than $1 per transaction). This makes it an ideal starting point for learning DeFi.

12.2 Getting Your First ETH on Base

Now that you have Bitcoin in your Phantom wallet, let's get some ETH on Base to start exploring DeFi. We'll use Coinbase for this process since they built Base and offer direct deposits.

12.2.1 Direct Purchase Method

The most straightforward approach is:

1. On Coinbase Exchange:
    - Purchase $50-100 worth of ETH
    - Select "Withdraw"
    - Choose "Send to Base"
    - Send to your Phantom wallet's Base address

This method is optimal because:

- Coinbase handles the bridge transaction for you
- You avoid paying Ethereum mainnet gas fees
- The process is simpler than manual bridging
- Base transaction fees are much lower

12.2.2 Understanding Base vs Ethereum

Base maintains a special relationship with Ethereum:

- It inherits Ethereum's security
- Uses the same wallet addresses
- Runs the same smart contracts
- Costs much less to use

Think of Base like a express lane on a highway - it's faster and cheaper while still getting you to the same destination safely.

12.3 Your First DeFi Steps on Base

Let's verify everything is working before diving deeper:

1. Check Your Setup
    - Confirm ETH appears in your Phantom wallet on Base
    - Make sure you've selected Base network
    - Have your Phantom wallet connected to Base
    - Keep transaction records for taxes
2. Test Transaction
    - Send a tiny amount of ETH (like $1 worth) between your own addresses
    - Notice how the gas fees are much lower than Ethereum
    - Get comfortable with Base network mechanics
    - Understand transaction confirmation times

12.4 Essential DEX Skills on Base

Base hosts many of the same DeFi protocols as Ethereum. Let's start with decentralized exchanges, using Base's version of Uniswap.

12.4.1 Your First Swap on Base

Let's walk through a simple ETH to USDC swap:

1. Preparation
    - Connect your Phantom wallet to Base's Uniswap interface

- Ensure you have enough ETH for both the swap and gas (much less than Ethereum!)
- Verify you're on the official Uniswap site
- Check current Base gas prices (typically cents, not dollars)

2. Making the Swap
   - Select ETH as your "from" token
   - Choose USDC as your "to" token
   - Enter a small test amount ($10 worth)
   - Review the quoted price and gas fees
   - Notice how Base's low gas makes small trades viable

12.4.2 Understanding Gas on Base

While Base uses the same gas system as Ethereum, the costs are much lower:

1. Typical Base Costs:
   - Simple transfers: $0.01-0.05
   - Token swaps: $0.10-0.30
   - Complex DeFi operations: $0.20-0.50 Compare this to Ethereum's fees which can be 50-100x higher!
2. Gas Reserve Planning
   - Keep $5-10 worth of ETH for gas on Base
   - Monitor Base network conditions
   - Understand peak usage times
   - Plan non-urgent transactions

12.5 Base DeFi: Lending and Yield Strategies

12.5.1 Understanding Lending Markets on Base

Base has attracted several major lending protocols, each offering unique features and risk profiles. Let's explore how to use them safely and effectively.

12.5.2 Moonwell: Base's Native Lending Protocol

Moonwell represents one of Base's core lending protocols. Think of it like a decentralized bank where you can both lend and borrow crypto assets. Here's how to use it effectively:

1. Lending Assets When you lend on Moonwell, you receive mToken (like mUSDC or mETH) representing your deposit. For example:

- Deposit 100 USDC, receive 100 mUSDC
- Your mUSDC continuously accrues interest
- Interest rates typically range from 2-5% APY for stablecoins
- ETH lending rates usually range from 1-3% APY

2. Borrowing Basics Moonwell uses an overcollateralized lending model:

- You must maintain at least 125% collateral ratio
- Different assets have different collateral factors
- ETH typically has 80% collateral factor
- Stablecoins often have 90% collateral factor

3. Risk Management on Moonwell

- Monitor your health factor constantly
- Set up alerts for approaching liquidation
- Maintain at least 150% collateral ratio for safety
- Understand emergency exit procedures

12.5.3 Compound on Base

Compound has deployed their latest version on Base, offering some unique features:

1. Key Differences from Moonwell

- Different interest rate curves
- Usually lower collateral requirements
- More conservative risk parameters
- Established security track record

2. Strategic Usage

- Compare rates between protocols
- Consider gas costs when switching
- Understand unique features of each
- Maintain positions across both for diversification

12.6 Yield Strategies Tailored for Base

Base offers several unique opportunities for generating yield. Let's explore them from lowest to highest risk.

12.6.1 Strategy 1: Stablecoin Lending

The foundation of any yield strategy should start with stable, reliable returns:

1. USDC Lending Path

- Lend USDC on Moonwell or Compound
- Current base yields: 2-4% APY
- Additional protocol rewards possible
- Minimal impermanent loss risk

2. Risk Mitigation

- Split funds between protocols
- Monitor protocol health
- Keep detailed records
- Understand withdrawal processes

12.6.2 Strategy 2: ETH-Based Yields

Base offers several ways to earn yield on ETH holdings:

1. Liquid Staking

- Deposit ETH via cbETH
- Earn staking rewards
- Maintain liquidity
- Current yields: 3-4% APY

2. Lending Markets

- Provide ETH as collateral
- Borrow stablecoins at low ratios
- Earn lending yields
- Manage liquidation risks

12.6.3 Strategy 3: Liquidity Provision on Base

Base hosts several DEXs where you can provide liquidity:

1. Stable Pair Liquidity (Lowest Risk)

- USDC-USDbC pools
- Typical yields: 3-8% APY

- Minimal impermanent loss
- Regular fee income

2. ETH Pair Liquidity (Medium Risk)

- ETH-USDC pools
- Yields vary widely: 5-20% APY
- Higher impermanent loss risk
- Better for long-term holders

12.6.4 Strategy 4: Yield Aggregation on Base

Several yield aggregators have launched on Base:

1. Yearn-style Vaults

- Automated yield farming
- Protocol reward optimization
- Complex strategies simplified
- Higher gas efficiency

2. Risk Considerations

- Smart contract risk exposure
- Strategy complexity risk
- Reward token price risk
- Exit liquidity risk

12.7 Building a Balanced Base Portfolio

Let's create a sample portfolio strategy for $1000 on Base:

1. Conservative Allocation (40%)

- $300 USDC split between lending protocols
- $100 in stable-stable LP positions
- Expected yield: 3-5% APY
- Focus on capital preservation

2. Moderate Risk (40%)

- $200 ETH in lending markets
- $200 in ETH-USDC liquidity pools

- Expected yield: 5-10% APY
- Balance growth with stability

3. Higher Risk (20%)

- $200 in yield aggregators
- Focus on newer protocols with incentives
- Expected yield: 10-20% APY
- Higher risk for higher returns

12.8 Tax and Record Keeping

Base transactions require careful tracking:

1. Essential Records

- All deposits and withdrawals
- Interest earned
- Trading fees collected
- Protocol rewards received

2. Transaction Management

- Use portfolio tracking tools
- Keep detailed spreadsheets
- Document all wallet addresses
- Save all transaction hashes

12.9 Emergency Procedures

Always maintain emergency plans:

1. Quick Exit Strategy

- Keep enough ETH for exit transactions
- Know fastest withdrawal paths
- Maintain exchange accounts for off-ramps
- Understand bridge withdrawal times

2. Risk Monitoring

- Track protocol TVL
- Monitor social channels

- Set up alerts
- Keep emergency contacts

Remember: Base's lower transaction costs make it easier to actively manage positions and adjust strategies, but never sacrifice security for yield. Start small, learn the mechanics, and scale up gradually as you gain confidence in the protocols and your own abilities.

12.10 Bridge Safety and Ethereum Relationship

While we're starting on Base for cost efficiency, it's important to understand the relationship with Ethereum:

1. Security Model
    - Base derives security from Ethereum
    - Transactions eventually settle on Ethereum
    - Assets can always be bridged back to Ethereum
    - Seven-day withdrawal period for security
2. Bridge Considerations
    - Official Coinbase bridge is safest
    - Understand withdrawal timeframes
    - Keep records of bridge transactions
    - Monitor bridge status

12.11 Moving Beyond Base

As your DeFi experience grows and your transaction sizes increase, the higher security of Ethereum mainnet may justify its higher fees. Consider graduating to Ethereum when:

1. Your portfolio grows significantly
2. You need specific Ethereum-only protocols
3. You're doing large trades where fees matter less
4. You want maximum security for long-term holdings

13 Make some money

13.1 Purchasing your first Crypto

I'd like to respect and adhere to the ethos of the early Cypherpunks. This means that I'd like everyone that follows along to maintain privacy. However the current solutions are overly technical for newcomers. Tornado Cash and Railgun have a high barrier to entry and Payy Network doesn't support moving funds onto other wallets yet.

So please be aware that all your transactions that you perform following along will be non private and easy for someone to trace. If you're an advanced user, then please see how to convert fiat to crypto anonymously.

Important things to note:

- You'll need about 10 US Dollars
- We'll be using a CEX to purchase crypto
- We'll use a Mobile wallet, Phantom

First thing anyone entering Web3 needs to do is to convert Fiat into a Digital Asset

We will use Coinbase as the CEX for this section. You're more than welcome to use your local CEX.

The reason I went with $10 is so that this will work for as many people as possible. See these heart breaking facts:

- The poorest 10% of the world live on less than $2 a day
- About 50% live on less than $7 a day

We'll purchase $10 worth of BTC.

13.2 Creating your first Crypto wallet

We'll follow the mantra of "Not your keys, not your Coins" and as such we need to get our assets off a CEX as soon as is practical. Bitcoin fee's are a bit expensive, so we'll keep them on a CEX until we have enough built up to justify the transaction fee to get them into our own wallet.

Please download or install Phantom. Once you open the wallet it will walk you through creating the wallet and will ask you to store your Seed phrase. For first time users, we recommend storing this on a piece of paper that you laminate and keep somewhere safe. At a later stage, we'll expand this section with a much more comprehensive handling of the pros and cons of various methods to store your seed phrase.

There are countless ways to store your seed phrase...

https://youtu.be/kWp6hZ-5ndc?si=yk6_iFfjv3lw0UQ5&t=70

13.3 Financial Independence

This Almanack is opinionated, because I'm opinionated. It will be wrong on occasion, but it also won't be cowed by crowds into taking safe calls. Where a position is required, we'll take one.

The North Star of this Almanack is financial independence. All strategies will be tailored to help you achieve this.

I'm a firm believer in Compound Interest. While as we progress up the degeneracy scale we'll be trading shit coins like a drunken Goth invading Italy, for now we want to learn some fundamentals, which we can then ignore later at our peril.

> "Compound Interest is the eighth wonder of the world. He who understands it, earns it; he who doesn't, pays it" - Often misattributed, but Author unknown

This isn't a TardFi textbook, so I'm not going too deeply into Compound Interest. I much prefer the Future Value of Money.

> "If you don't know where you are going, you'll end up someplace else." - Yogi Berra

So where are we going? Financial Independence from a Central Authority. That's what I want, and I'm pretty sure if you're reading this, you want it too.

So this book will be tailored to the people living in the third world. So if you live in the first world, just add an extra zero to all the figures and follow along. But for someone living in the third world where they need to live on $7 a day to survive, in order to get financial freedom from a central authority, they'd need to earn enough interest on their money yearly to afford their daily survival. So that's approximately $2,555 US dollars they'd need to earn in interest yearly. This would need to be a relatively stable yield without crazy degen high risks. So something like a US Bond. We'll get into that later.

But let's say we can get 4% yearly. That means we need a principal of $63,875 in order to escape reliance on any authority.

So now we know where we're going.

How do we get there?

In this example, we're going to ignore things like inflation for the time being. Even though inflation is one of the major driving forces behind crypto adoption.

The formula for future value with periodic payments is: FV = PV × (1 + r)^n + PMT × [((1 + r)^n - 1) / r] Where:

- FV = Future Value
- PV = Present Value (initial investment)
- PMT = Payment (the regular contribution amount)
- r = Interest rate (as a decimal)
- n = Number of time periods

Interactive Financial Independence Calculator

Use the calculator below to experiment with different scenarios and see how they affect your path to financial independence. The chart shows your projected growth over time, with the red dashed line indicating your target amount.

```
// Create input elements with improved formatting
viewof target = Inputs.range(
  [1000, 10000000],
  {value: 63875, step: 100, label: "Target Amount ($)"}
)

viewof initial = Inputs.range(
  [0, 10000],
  {value: 10, step: 1, label: "Initial Investment ($)"}
)

viewof monthly = Inputs.range(
  [0, 1000],
  {value: 10, step: 1, label: "Monthly Contribution ($)"}
)

viewof rate = Inputs.range(
  [0, 1000],
  {value: 77, step: 0.1, label: "Annual Return Rate (%)"}
)

// Enhanced number formatting function
function formatCurrency(value) {
  return new Intl.NumberFormat('en-US', {
    style: 'currency',
    currency: 'USD',
    minimumFractionDigits: 0,
    maximumFractionDigits: 0
  }).format(value);
}

// Display current input values with proper formatting
currentValues = md`
Current Values:
- Target Amount: ${formatCurrency(target)}
- Initial Investment: ${formatCurrency(initial)}
- Monthly Contribution: ${formatCurrency(monthly)}
- Annual Return Rate: ${rate.toFixed(1)}%
`

// Calculation function
function calculateGrowth(initial, monthly, rate, target) {
  const monthlyRate = rate / 100 / 12;
  let amount = initial;
  let data = [{month: 0, amount: amount}];
  let month = 0;

  while (amount < target && month < 1200) {
    amount = amount * (1 + monthlyRate) + monthly;
    month++;
    data.push({month, amount});
  }

  return {
    months: month,
    finalAmount: amount,
    years: Math.floor(month / 12),
    remainingMonths: month % 12,
    isAchievable: month < 1200,
    growthData: data
  };
}

// Calculate results based on inputs
results = calculateGrowth(initial, monthly, rate, target)

// Display formatted results
md`### Results
Time to reach goal: ${results.years} years and ${results.remainingMonths} months

Final amount: ${formatCurrency(results.finalAmount)}

${results.isAchievable ? '' : '  Goal may not be achievable with current parameters'}`

// Create the growth visualization
{
  const svg = d3.create("svg")
    .attr("viewBox", [0, 0, 800, 400])
    .attr("style", "max-width: 100%; height: auto;");

  const x = d3.scaleLinear()
    .domain([0, results.months])
    .range([50, 750]);

  const y = d3.scaleLinear()
    .domain([0, Math.max(target, results.finalAmount)])
    .range([350, 50]);

  // Improved axis formatting for large numbers
  const formatAmount = (value) => {
    if (value >= 1e6) return `$${(value/1e6).toFixed(1)}M`;
    if (value >= 1e3) return `$${(value/1e3).toFixed(1)}K`;
    return `$${value}`;
  };

  svg.append("g")
    .attr("transform", `translate(0,350)`)
    .call(d3.axisBottom(x)
      .ticks(10)
      .tickFormat(d => d + " months"));
```

```
svg.append("g")
  .attr("transform", "translate(50,0)")
  .call(d3.axisLeft(y)
    .ticks(10)
    .tickFormat(formatAmount));

// Grid lines
svg.append("g")
  .attr("class", "grid")
  .attr("transform", `translate(0,350)`)
  .call(d3.axisBottom(x)
    .ticks(10)
    .tickSize(-300)
    .tickFormat(""))
  .style("stroke-opacity", 0.1);

const line = d3.line()
  .x(d => x(d.month))
  .y(d => y(d.amount));

svg.append("path")
  .datum(results.growthData)
  .attr("fill", "none")
  .attr("stroke", "steelblue")
  .attr("stroke-width", 2)
  .attr("d", line);

svg.append("line")
  .attr("x1", 50)
  .attr("x2", 750)
  .attr("y1", y(target))
  .attr("y2", y(target))
  .attr("stroke", "red")
  .attr("stroke-dasharray", "5,5");

svg.append("text")
  .attr("x", 400)
  .attr("y", 390)
  .attr("text-anchor", "middle")
  .text("Time (months)");

svg.append("text")
```

```
    .attr("transform", "rotate(-90)")
    .attr("x", -200)
    .attr("y", 15)
    .attr("text-anchor", "middle")
    .text("Amount ($)");

  return svg.node();
}
```

Important to note that holding BTC for 8 years:

- Starting 2013 (to 2021): ~4,000% return
- Starting 2014 (to 2022): ~2,900% return
- Starting 2015 (to 2023): ~8,500% return
- Starting 2016 (to 2024): ~17,500% return

This clearly means holding BTC is the only logical thing you should do. Everything else is bullshit unless you're mid brain.

The Future Value of Money though assumes that the periodical payments are in a fixed currency like the US Dollar. This is not true though for our approach. We'll revise this in future to take into account the different costs of purchasing BTC throughout the 8 years to make the figures more realistic.

13.4 Your first Degen Strategies

We'll now learn the following strategies:

1. DCA
2. HODL

13.4.1 DCA

An important point in the above section was that we have to have a monthly contribution. This means that every month you'll need to find $10 in Fiat and convert it into BTC. This is what is meant by DCA, or Dollar Cost Averaging. You are averaging the price of the BTC you purchase over 8 years. The beauty of this strategy is that sometimes you'll buy high and sometimes you'll buy low, but by consistently buying every month you'll average it out.

13.4.2 HODL

The ultimate HODL Coin is BTC. Considering we're planning for 8 years, we have a perfect timeline for HODLing.

14 Mid Brain

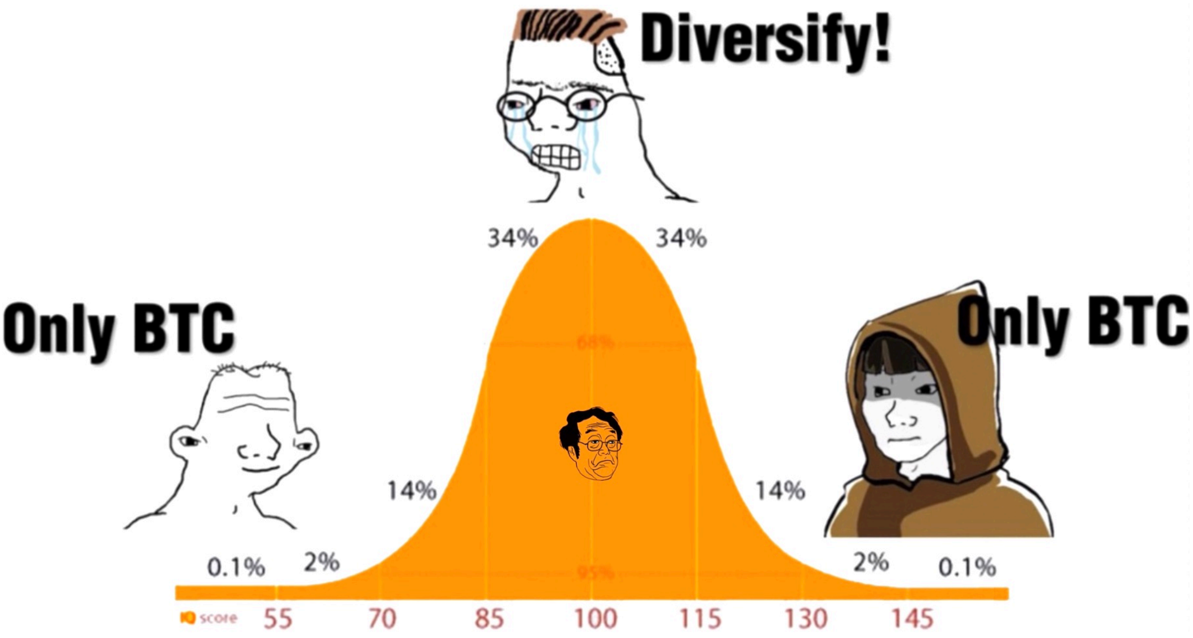

Figure 14.1: You are currently the guy in the middle

While this section will probably be the most fun to write, it will result in unbounded destruction.

Let the fun begin!

14.1 Shit Coins

DeFi truly started on Ethereum in DeFi Summer 2020.

Some pedants will argue it started in 2016, with the launch of EtherDelta and the 2017 ICO boom where it handled about 10% of all Ethereum token trading volume. But degen DeFi started in 2020 with the most degen of crazes. Food tokens and farming.

Meme coins had started in 2013 with Doge. However in the early days even the worst shit coins had to have a network. So even the scammers needed to have enough technical proficiency to create a network to issue a token to scam you. That changed with the advent of the ERC20 token standard on Ethereum in late 2015. Now scammers and purveyors of shit coins could just copy and paste some code and voila, shit coin!

Scammers everywhere rejoiced.

In 2020 when DeFi Summer started kicking off, we got a flood of that special brand of shit coin, the Governance token. We can probably blame MakerDAO for this atrocity, with the introduction of "Liquidity Mining" or "Yield Farming". You see, shit coin creators crave liquidity above all else. Without liquidity, they cannot dump on the market. Without liquidity, you cannot manipulate the market to think your shit coin is worth billions. Traditionally shit coin creators had to go to CEX's to get liquidity. The problem is CEX's are just as, if not more, crooked than shit coin creators. CEX's charge astronomical prices to list. And then they dump on the market before the shit coin creator can. For a great case study see how $GALA shat the bed after getting listed on that dodgiest of the dodge, FTX.

So Yield Farming allowed shit coin creators a new way to gain liquidity and if anything better PsyOps for dumping on mid brains. What you do is, you create your shit coin, with a massive supply, think billions. Then you allocate 10% of this token supply for Yield Farming. Now liquidity on CEX's are provided by mature market makers. Retail is excluded as they're not mature enough or have the resources to provide market making services. So since Uniswap provided an easy way for retail (read marks) to provide liquidity, you could offer these gullible people rewards for providing liquidity. So let's say you put in $10 of liquidity, you'd offer these users $10 a month in Yield Farming rewards for that liquidity. Easy money for the mark. Except that $10 a month is in the shit coin. Shit coin creator gets liquidity so they can dump their allocation into Stables or a blue chip Coin. Farming Yields go to shit. **YOU** get rekt. Unlucky.

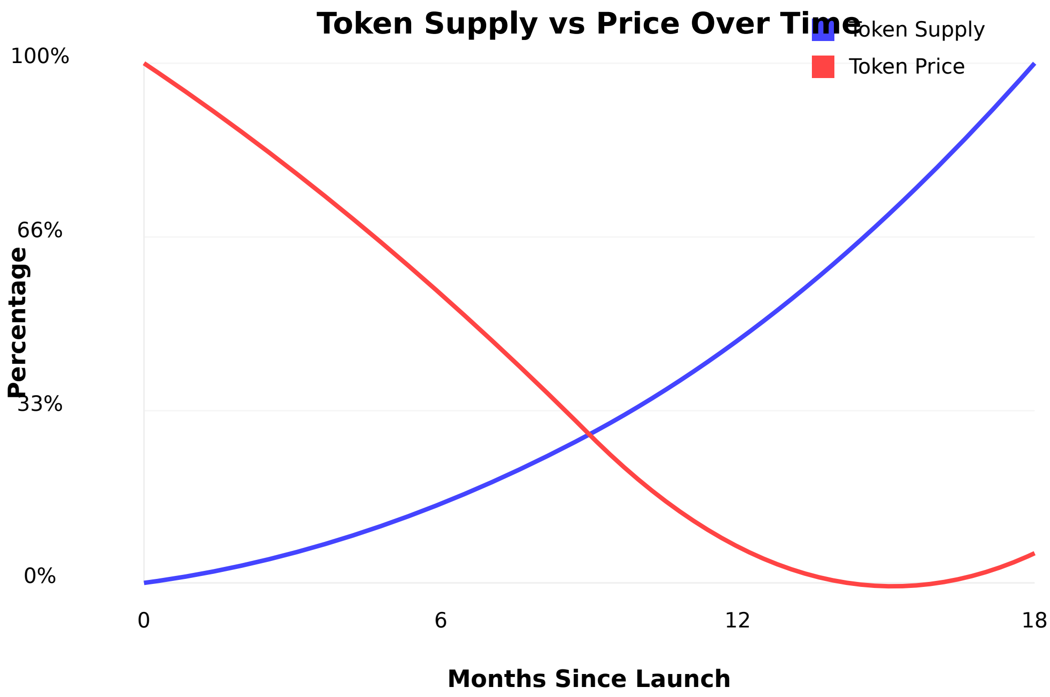

Figure 14.2: Governance Tokens Tokenomics

So now we have all the ingredients for a Yield Farming.

- A plethora of shit coins, masquerading as Governance tokens
- A mature trading environment facilitated by Uniswap's innovation in the AMM space
- An unsuspecting market of victims easily lured by promises of huge profits

Welcome to DeFi Summer 2020.

There were also some cool examples of Vampire Attacks. Or more broadly, a protocol ripping off the source code of a naive project, wrapping a token around their stolen work and trying to unfairly profit. How very James Taggart of them.

So first lesson, we don't deal with shit coins. Or if we're forced to, it's because there's enough zealots around it that the market is being stupendously foolish and we can profit from their idiocy.

> Be fearful when others are greedy, and greedy when others are fearful - Warren Buffet

I really should try categorize shit coins. This is tough to do.

> “I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description [of pornography]; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it, and the motion picture involved in this case is not that.” - Supreme Court Justice Potter Steward’s ruling on Porn

Just like old mate Potter, I don’t think I can define a shit coin, but I know it when I see it. The only way you’ll be able to get that level of maturity is time in the market. Your battle scars will be your wisdom in years to come.

14.2 Notification System

Since we’re going to be playing with the sharks, we’re going to need protection. This is where alerts come into it.

Being good at DeFi is being able to remain emotionless. Being online 24/7 during bull markets is going to make you stupid, strung out and will ensure your strategies are riddled with mistakes. Being a balanced person will make you way more money than some sleep deprived, Twitter obsessed doos. Let the machines work for you.

So we need a good notification system. We can use:

- Tenderly Web3 Actions, or
- OpenZeppelin Defender Sentinels

We’ll use Tenderly’s Web3 actions as they’re more flexible and powerful. Since we’ll be using Ethena’s USDe quite alot through this strategies it’s important that if it shits the bed, we can get out quickly before losing everything. As an example UST on May 10th 2022 from holding it’s dollar peg to losing half it’s value in about 38 hours. So if USDe loses more than 10%, we must assume a death spiral and get our money out.

!UST depeg

So what we want to do is to go to CoinGecko and find the biggest amount of on chain liquidity for USDe. So find USDe and then go to Markets to find the on DEX with the biggest depth. Currently that’s Uniswap V3 with a USDE/USDT pool on Ethereum. https://app.uniswap.org/explore/pools/ethereum/0x435664008F38B0650fBC1C9fc971D0A3Bc2f1e47

So we can set a notification for event emitted in Tenderly through the UI. However this doesn’t give us the exchange rate. So it’s good enough for now, but we’ll eventually revise this to have common notifications that will apply across all our strategies.

14.3 Getting in early

In crypto, if you're not a VC, one of the ways to get the highest multiples on shit coins is by getting in early. Currently the easiest way to see where the most meme coin activity is occuring is by looking at DEX Screener's new pairs. At the time of writing, you can clearly see this is Solana.

Let's analyse the criteria to determine what they all mean

- Price - How much in USD to get 1 of the tokens
- Age - Determines how long the token has been trading. However we actually care about contract deployment date too
- Buys & Sells - Large amount of numbers doesn't necessarily mean much due to the prevalence of bots.
- Volume - Important to see if there is wash trading here. $1 million volume with $100k liquidity may indicate manipulation
- Makers - Some DEX's can act as CLOB's where Makers as a term originate. Makers are trades with a limit order waiting to be filled
- Liquidity - How much liquidity there exists for the token. We can also check to see if the liquidity was burnt
- MarketCap
- Holders - How many wallets hold this token.

15 Big brain

15.1 Converting FIAT into a Cryptocurrency anonymously

This may be the hardest part of being a Degen. A Degen values privacy. Important to distinguish there is a difference between privacy and secrecy. I'd like my cryptocurrency to display the same characteristics as cash. A means of exchange that has been working just fine for centuries. Cash is private by default and people have seemed pretty happy with that arrangement for over 3 centuries.

The hardest part of ensuring privacy is making sure that when you create a new wallet there is no trace back to your off chain identity.

The two biggest footprints you can leave are:

1. Funding your wallet to pay for Gas
2. Receiving funds in your wallet from a compromised account

When funding your on chain wallet from a CEX, it becomes very easy to trace your identity. Almost all CEX's require you to KYC. So when you transfer $10 of ETH into your Metamask wallet, anyone will be able to find out that the funding of the wallet came from a CEX and via the CEX will be able to link your identity to your wallet.

So currently the best way to do this is:

- Create two wallets. Compromised and Clean
- Save the Private Keys
- Connect to your VPN
- TOR doesn't support add ons, so we can't install a wallet, but rather need to run a script in order to shield our funds

We can also try Railgun. I'll run through both Tornado and Railgun and eventually Payy wallet and then based upon the results of all those experiments I'll make a recommendation about the best approach to obtain a private by default wallet.

- Purchase USDC or USDT from a CEX
- Transfer the stable coins to the throwaway account
- Download Railgun Client
- Create a Shielded Address

- Transfer it in common increments similar to how Tornado Cash to the clean wallet at random intervals

Part IV

Web3 Essentials

16 Meme Culture

16.1 Introduction

Memes serve as a unique form of cultural communication in the Web3 space, combining humor with important lessons and shared experiences. They often capture complex ideas in accessible formats and help create a sense of community among participants. This guide explores the most significant memes in Web3, their origins, and their deeper meanings.

16.2 Foundational Memes

16.2.1 "Not Your Keys, Not Your Coins"

This fundamental meme emerged from the early Bitcoin community and gained renewed significance after several high-profile exchange collapses. It encapsulates one of the core principles of cryptocurrency: self-custody.

Origin: The phrase likely originated on Bitcoin forums around 2011-2012 but gained prominence after the Mt. Gox collapse in 2014.

Cultural Impact: - Serves as a constant reminder of cryptocurrency's original purpose: financial self-sovereignty - Often shared after exchange hacks or failures - Has evolved into a teaching tool for newcomers - Frequently referenced in discussions about centralized exchanges and custody solutions

Real-world examples that reinforced this meme: - Mt. Gox (2014): 850,000 BTC lost - QuadrigaCX (2019): $190 million lost - FTX (2022): Billions in customer funds lost

16.2.2 HODL

Perhaps the most famous cryptocurrency meme, "HODL" originated from a typo that became a battle cry for long-term investors.

Origin: December 18, 2013, when GameKyuubi posted "I AM HODLING" on the BitcoinTalk forum during a market crash. The poster, admittedly drunk, wrote a passionate defense of holding Bitcoin despite price volatility.

Evolution: 1. Initial phase: Simple misspelling joke 2. Secondary meaning: "Hold On for Dear Life" 3. Modern usage: Philosophical approach to cryptocurrency investment

Cultural significance: - Represents conviction in long-term value over short-term trading - Creates solidarity among investors during market downturns - Differentiates investment approaches (HODLers vs. traders) - Has spawned related terms like "diamond hands"

16.3 Character-Based Memes

16.3.1 Wojak Variations

Wojak (also known as "feels guy") has become the protagonist of countless crypto trading stories, with several important variations:

16.3.1.1 The Crypto Wojak Timeline:

1. Basic Wojak: Represents the average retail trader
2. NPC Wojak: Symbolizes those who follow the crowd without thinking
3. Brainlet: Depicts poor trading decisions
4. Cozy Wojak: Represents comfortable HODLers during market turbulence

16.3.2 The Bogdanoff Twins

A complex meme centered around the late Bogdanoff twins, imagining them as all-powerful market manipulators.

Key elements: - "Dump it": Order given after someone buys - "Pump it": Command issued after someone sells - "He sold?": The setup for market manipulation

Cultural impact: - Reflects the feeling of powerlessness many traders experience - Personifies the seemingly manipulated nature of crypto markets - Creates humor from shared experiences of poor timing

16.4 Educational Memes

16.4.1 The Bell Curve (Midwit) Meme

This meme format illustrates the concept of sophisticated simplicity in cryptocurrency:

Left (Low IQ): Simple but effective approach Middle (Average IQ): Overcomplicated strategies Right (High IQ): Return to simplicity with deep understanding

Examples: - Bitcoin storage: Hardware wallet → Complex multi-sig setup → Hardware wallet with proper backup - Trading: HODL → Complex trading strategies → HODL with occasional rebalancing - Security: Write down seed phrase → Use elaborate encryption → Write down seed phrase and store in safe

16.5 Market Condition Memes

16.5.1 "This is Fine" Dog

A cartoon dog sitting in a burning room, often used during market crashes. The meme represents: - Forced calm during market turbulence - Coping with significant losses - The crypto community's resilience

16.5.2 "When Lambo?"

Origin: 2017 bull run Meaning: Represents the dream of crypto wealth Evolution: 1. Sincere question from newcomers 2. Ironic joke about unrealistic expectations 3. Critique of get-rich-quick mentality

16.6 Community-Specific Memes

16.6.1 Ethereum Memes

- "Vitalik clapping": Celebrating network achievements
- "Ultra sound money": ETH's post-merger monetary policy
- "Merge delayed": Historical references to Ethereum's upgrade timeline

16.6.2 Bitcoin Memes

- "Number go up": Bitcoin's long-term price appreciation
- "Stack sats": Encouraging regular small purchases
- "PayPal of crypto": Mocking misunderstandings of Bitcoin's purpose

16.7 Best Practices for Meme Literacy

Understanding crypto memes helps participants: 1. Navigate community sentiment 2. Identify market cycles 3. Learn from shared experiences 4. Connect with the broader culture

16.8 Modern Usage Guidelines

When engaging with crypto memes: - Understand their historical context - Recognize their educational value - Use them appropriately in discussions - Appreciate their role in community building

16.9 Conclusion

Memes in Web3 are more than just humor - they're a sophisticated form of cultural communication that encodes important lessons, shared experiences, and community values. Understanding these memes helps participants better navigate both the technical and social aspects of the cryptocurrency ecosystem.

As the space evolves, new memes emerge while old ones gain additional layers of meaning. This living document will be updated to reflect these changes and maintain its relevance as a cultural guide to Web3.

Part V

Technologist's Path

17 Overview

- Deep technical fundamentals (cryptography, consensus, networking)
- Protocol design patterns and tradeoffs
- Development frameworks and tools
- Security considerations for builders
- Advanced privacy techniques

18 Cryptography

18.1 Symmetric Cryptography

Shared Keys. AES. But vulnerability is in sharing the Key between parties.

18.2 Asymetric Cryptography

Public Key Cryptography

RSA and elliptic curve cryptography. Slow than symetric cryptography. Enables secure communication over insecure channels

18.2.1 Passkeys

Think of passkeys as a modern, more secure replacement for passwords. Instead of remembering complex strings of characters, your device creates and stores a pair of mathematically linked keys - one public and one private. This system is built on public key cryptography, which has been proven secure over decades of use. Here's how the process works, step by step: When you first set up a passkey with a website or app:

1. Your device generates two mathematical keys: a private key that stays securely stored on your device, and a public key that gets sent to the service you're signing up with. The private key never leaves your device - this is crucial for security.
2. The service stores your public key along with your account information. Think of the public key as a special lock that can only be opened by your private key.

When you later want to sign in:

1. The service sends your device a random mathematical challenge - imagine it as a complex puzzle.
2. Your device uses your private key to solve this puzzle in a way that proves you have the correct private key, without actually revealing the key itself.
3. The service verifies the solution using your stored public key. If it matches, you're granted access.

What makes this particularly clever is the biometric integration. Your device typically requires your fingerprint, face scan, or PIN before it will use the private key. This adds an extra layer of security - even if someone stole your device, they couldn't use your passkeys without your biometric data. The system also handles synchronization elegantly. If you're using an ecosystem like Apple or Google, your encrypted passkeys can sync across your devices. When you want to log in on a new device, your phone can help authenticate you by displaying a QR code that creates a secure connection between devices. To make this more concrete, imagine you're signing into a banking app:

You open the app and enter your username Instead of asking for a password, the app sends a challenge to your phone Your phone asks you to verify with your fingerprint Once verified, your phone uses your private key to respond to the challenge The bank verifies this response and logs you in

All of this happens in seconds, and it's much more secure than traditional passwords because:

The private key never travels across the internet Each login uses a different challenge, so responses can't be reused by attackers Biometric verification adds an extra security layer The cryptographic math behind it is extremely difficult to break

18.3 Hash functions

These are like digital fingerprints

18.4 Zero-Knowledge Proofs

They solve a unique problem: how can you prove you know something without revealing what you know? Imagine proving you're over 21 without showing your actual birthdate.

18.5 Homomorphic Encryption

It allows computations to be performed on encrypted data without decrypting it first. Think of it like being able to ask someone to bake a cake following your secret recipe, but without ever revealing the recipe to them. While still computationally intensive, this technology could revolutionize cloud computing and data privacy.

18.6 Post-Quantum Cryptography

cryptographic systems that can resist attacks from quantum computers. This forward-looking field is essential because many current cryptographic systems (especially asymmetric ones) could be broken by powerful quantum computers.

19 Blockchains

We would prefer to use the term Decentralized Incentive Network instead of blockchain. But we also want to align on common nomenclature within the industry, so we'll stick with Blockchain for now.

The point of blockchains:

- Censorship resistance
- Deterministic State Transition (Mempool creates interesting nuances and complexity here)
- Credible neutrality
- Trustless coordination at scale
- Asset digitization and ownership

Censorship resistance is indeed crucial - it enables truly permissionless systems where no entity can prevent valid transactions. However, there are several other compelling candidates for blockchain's primary purpose:

One strong contender is deterministic state transition. Think about how traditional databases or financial systems might have ambiguity about the exact sequence or timing of transactions, especially across different locations or institutions. Blockchain provides absolute clarity about state changes - there's no ambiguity about which transaction came first or what the exact state was at any given moment. This property enables complex financial systems and smart contracts to operate with complete predictability.

Another fundamental purpose could be creating credible neutrality in computational systems. This goes beyond just censorship resistance - it's about creating systems where the rules are explicit, unchangeable without consensus, and apply equally to all participants. Traditional systems often have hidden biases or special privileges for certain users, while blockchain systems enforce their rules uniformly through code.

We could also argue that the primary purpose is enabling trustless coordination at scale. Before blockchain, coordinating economic activity among untrusting parties required trusted intermediaries like banks or governments. Blockchain enables direct peer-to-peer coordination without these intermediaries, potentially reducing costs and increasing efficiency.

Asset digitization and ownership might be another contender. Blockchain enables digital scarcity and verifiable ownership in ways that weren't possible before. This property enables everything from cryptocurrencies to NFTs to tokenized real-world assets.

We won't be taking any ideological approach to the point of blockchains but rather applying scores to DIN's and then comparing that to how the market values them.

A decentralized incentive network with state consensus

I've tried to simplify our definition as much as possible and even still it's verbose. Read that sentence to 99% of the world and I'll they'll give you a quizzical look and move onto the section about meme coins. There's a lesson there. A lesson the technical luminaries in this space ignore at their peril. Accessibility matters.

Let's break down each component of our definition.

Decentralized. This is how many Nodes participate. Centralized means 1. Therefore anything more than 1 is decentralized.

Network. This loosely means the participants computers/machines communicate via a communication method.

State Consensus. The network will record state and all nodes will agree about the state via consensus.

We don't need to worry too much about consensus yet, but you just need to know that the nodes must agree on the state. For example if Bob sends Alice 10 BTC. Everyone on the network must come to an agreement that Bob did indeed send Alice 10 BTC. Another important characteristic is that even if everyone agrees today, in the future that can't be disputed or changed. This is another important category called censorship resistance. We'll get to it.

Dependent Networks

A sovereign chain can be defined as a network that maintains complete independence in its settlement process, requiring no external chain to validate or guarantee its state transitions. This independence is fundamental to the concept of sovereignty in blockchain networks.

This section should start discussing why the need arose for dependent networks. Specifically Ethereum struggling with scale. Due to the trilemna: decentralization security scalability

Let's talk about scaling strategies monolithic Bigger blocks Faster blocks Higher minimum requirements for nodes Consensus optimizations modular Execution - The current crop of L2's Data availability - Storing and accessing blockchain data Celestia Consensus - Agreeing on the state of the network Settlement - Finalizing transactions and providing security guarantees. Ethereum and Bitcoin in the current Layer craze

19.1 Sovereign Networks

Pure Value Networks Pure value networks stick to the fundamental purpose of moving and storing value, avoiding the additional complexity that comes with being a platform for applications or other services.

What makes these networks "pure value" is what they don't include: They don't support complex smart contracts They don't host decentralized applications They don't provide programmable functionality beyond basic value transfer They don't serve as platforms for other tokens or applications

Application Chains Application Chains represent networks that go beyond pure value transfer to support various types of applications. They're divided into three main categories: Hubs, Specialized, and Generalized chains.

Hub Application Chains serve as central connection points in the blockchain ecosystem.

Specialized Application Chains focus on specific use cases or industries.

Generalized Application Chains aim to support a wide range of applications but differ from hubs in that they're not necessarily trying to be central connection points.

The key distinction between these categories lies in their approach to applications:

- Hubs prioritize becoming central platforms that other networks depend on
- Specialized chains optimize everything for specific use cases
- Generalized chains provide broad functionality but focus on being self-contained ecosystems

19.2 Layer 2's

We break these down into:

- Rollups
  - Optimistic
  - ZK
- Validiums
- Plasma
- Sidechains

So Ethereum has chosen decentralization and security. This means Ethereum is shit at scaling.

So we need to talk about the theory of Layers in Blockchain

That's why L2's became a major part of the roadmap. How does the scalability limitation affect the network. Congestion and high gas fee's. So people don't interact on the chain and it hits a ceiling. So logically we should start any discussion with transaction fee's, as that's the direct result of the scalability failure and the main reason users use L2's. Besides yield opportunities.

So we should first consider the Fee Markets on Ethereum and Bitcoin which are the two major chains looking to scale with L2's. There is a lot of debate and a lot of misinformation around this topic.

Dependent networks can really be divided into chains: External DIN required to validate state transitions External DIN required to guarantee state transitions

We'll define a framework for how we define a Dependent Network. There are few things we look at, in terms of priority:

- censorship resistance. Polygon zkEVM sequencer can censure, but you can go through the contract directly on Ethereum theoretically if censorship occurs. Same thing for Arbitrum. Although this is a very weak guarantee due to the complexity for regular users. For Stacks, it's more censorship resistant that the other two. Also if I were to interact directly with the smart contract on Ethereum, that makes the L2's pointless. Why do I need them if not to deal with congestion and high gas. dispute resolution. I believe all chains need to hard fork. Potentially not Movement due to Move's resource model. None of the chains will automatically hard fork if a dispute is found.
- settlement. So the base chain must validate and guarantee state transitions on the dependent chain. This is kinda stupid. It's guaranteeing the state transitions but makes no attempt to resolve things like censorship resistance.
- finality of settlement. Optimistic 7 days, zk 30 minutes, Stacks 16 hours
- economic security model inheritance - this is actually pointless as it just means the state transitions match the rules. Nothing about censorship resistance.

So my qualification of dependent networks means that they must inherit the censorship resistance of the base chain, settlement must be validated and guaranteed by the base chain, dispute resolution must be automatic and/or decentralized. else the chain can just fork.

Settlement Types In order of strength

- Cryptographically enforced settlement
- Validity proofs
- Fraud proof systems
- Checkpoint systems

19.3 Consensus Mechanisms

Consensus Mechanisms All DIN's have a consensus mechanism we have the consensus mechanisms. These can be divided into the following broad categories:

- Proof based mechanisms. Mainly Proof of Work and Proof of Stake
- Byzantine Fault Tolerance (BFT) Mechanisms. Tendermint
- Voting Based Mechanisms, Ripple and Stellar
- Directed Acrylic Graph based mechanisms
- Hybrid. PoS + BFT is used by Polkadot and Cosmos
- Novel Mechanisms

Need to talk about finality here about probabilistic vs deterministic. Also focus on Single Slot Finality

19.4 Application Models

Each application model represents a fundamental approach to how blockchains manage state, handle parallel execution, represent assets, enable composability, and provide safety guarantees.

We classify Application Models as:

- UTXO also includes Cardano's extened UTXO, Kaspa also falls into this
- Account
  - Pure EVM Ethereum, Polygon, Avalanche, TRON et al
  - Specialized XRP and Stellar
- Sharded account model Near falls into this.
- Object Sui
- Resource model Aptos and Movement
- Capability Solana
- Cell model TON
- Actor Based (ICP and CosmWasm

19.4.1 UTXO

The UTXO model treats the ledger as a set of unspent outputs that can be consumed as inputs to create new outputs. This model inherently supports parallel transaction validation since each UTXO can only be spent once.

Key Characteristics:

- State Management: Stateless, transaction-oriented
- Parallelization: Natural parallel validation
- Asset Representation: Native representation of tokens
- Composability: Limited without extensions
- Safety Guarantees: High through explicit ownership

19.4.2 Account Model

Accounts maintain state directly, with each account having properties like balance and nonce. This model enables rich programmability but can face challenges with parallelization. However if we look at EOA's, they only maintain state of the network token and not ERC20's.

Key Characteristics:

- State Management: Stateful, account-oriented
- Parallelization: Challenging due to state dependencies
- Asset Representation: Contract-based tokens
- Composability: High through contract interactions
- Safety Guarantees: Varies by implementation

19.4.3 Object Model

Objects are owned, independent state elements that can be transferred and modified. This enables parallel execution while maintaining rich programmability.

Key Characteristics:

- State Management: Object-oriented
- Parallelization: Natural through object independence
- Asset Representation: Native objects
- Composability: Through object references
- Safety Guarantees: Object-level ownership

19.4.4 Resource Model

Resources are linear types that cannot be copied or discarded, only moved between accounts. This provides strong safety guarantees for digital assets.

Key Characteristics:

- State Management: Resource-oriented
- Parallelization: Possible through resource independence
- Asset Representation: Native resources

- Composability: Through resource combination
- Safety Guarantees: Very high through linear types

19.4.5 Capability Model

Capability Model Access to resources is controlled through explicit capabilities, enabling fine-grained access control and parallel execution.

Key Characteristics:

- State Management: Capability-based
- Parallelization: High through capability isolation
- Asset Representation: Capability-protected resources
- Composability: Through capability delegation
- Safety Guarantees: High through access control

19.4.6 Cell Model

State is organized into cells that can be independently accessed and modified, enabling high parallelization.

Key Characteristics:

- State Management: Cell-based
- Parallelization: High through cell independence
- Asset Representation: Cell-based
- Composability: Through cell references
- Safety Guarantees: Cell-level isolation

19.4.7 Actor Model

Computation is organized around actors that can independently process messages, enabling natural parallelization.

Key Characteristics:

- State Management: Actor-local state
- Parallelization: Natural through actor independence
- Asset Representation: Actor-managed
- Composability: Through message passing
- Safety Guarantees: Actor isolation

Application Model	Blockchains	Key Features
UTXO	Bitcoin, Cardano (eUTXO), Kaspa, Ergo, Bitcoin Cash, Litecoin, Zcash, Dogecoin, Monero, BEAM	- Natural parallelism- Simple state model- High security
Account (Pure EVM)	Ethereum, Polygon, Avalanche C-Chain, BSC, TRON, Fantom, Arbitrum, Optimism, Mantle, WorldCoin, Gala, Flare	- Rich programmability- High composability- Standard tooling
Account (Specialized)	XRP, Stellar, Algorand, Stacks, Tezos, Hedera, VeChain, Quant, the Sandbox, StarkNet, Neo, BitTorrent	- Custom account models- Specific use-case optimization- Modified state management
Sharded Account	NEAR, Polkadot, Kusama, Elrond (MultiversX), Harmony	- Parallel execution- Cross-shard composition- Scalable state
Object	Sui	- Object-centric- Natural parallelism- Rich ownership model
Resource	Aptos, Movement, Flow, Virtual Protocol	- Linear types- Strong safety- Asset-oriented
Capability	Solana, Injective, SEI, Theta Network	- Fine-grained access- High parallelism- Explicit permissions
Cell	TON, Everscale	- Cell-based storage- High parallelism- Flexible structure
Actor	Internet Computer (ICP), CosmWasm chains (Osmosis, Celestia, Cosmos Hub), Fetch.ai, IOTA	- Message-passing- Natural isolation- Independent processing
Unknown	Filecoin, Arweave, Bittensor, Mantra, Ondo, Kaia, Brett, Jasmycoin	Still researching these

19.5 Communication Protocols

We have

- IBC (Inter-Blockchain Communication) - Cosmos
- XCMP (Cross-Chain Message Passing) - Polkadot
- CCTP (Cross-Chain Transfer Protocol) by Circl
- CCIP (Cross-Chain Interoperability) by Chainlink
- Warp Messaging for Avalanche
- IMP (Interchain Messaging Protocol)

We can then further classify these standard by the following properties: * Security Model * Centralized vs Decentralized * Message Scope (General (IBC,CCIP, Hyperlane) vs Specialized (Circle's CCTP and Warp)) * Open vs Close networks * Message Verification Method

19.6 Fee Markets

We break down fee markets into:

- Block Space Markets
- Resources Markets

19.6.1 Block Space Markets

These are the most fundamental type. Users are paying for space in the next block, regardless of what they're doing with that space. It only considers the price of inclusion while respecting the limits of the network.

19.6.2 Resource Markets

These evolved with the advent of Ethereum as blockchains became more complex. We break these down into:

- Compute
- Data Availability
- Storage
- Hybrid

19.6.2.1 Compute Markets

Transaction fee's sometimes called Gas is what you pay to execute a smart contract on a blockchain. On some networks, like Ethereum, there is an execution limit on how much computational work can be done in a block. This parameter directly impacts the computational resources required to run a node.

Nodes can propose a gas limit

So the attributes for Transactions Fee's are: Tips/Bribes How Transactoin fees are distributed. Burnt or redirected to Miners How fee's are calculated Base Fee Dynamic Fee (based on something like network congestion)

19.6.3 Data Availability

We will compare the mechanisms of the following major DA layers:

- Ethereum
- Celestia
- Eignlayer DA
- Avail

Ethereum uses dynamic blob fees based upon a target amount of blob space per block.

Celestia charges by size. Celestia is designed to scale to handle increase demand with adding more validators

Avail also charges by size but also the type.

EigenDA creates a marketplace for data availability providers

19.6.3.1 Storage

19.6.3.2 Hybrid

19.6.3.3 Congestion Measurement Mechanisms

Ethereum

- Measures block gas utilization vs 15M target
- 12.5% base fee adjustment per block
- Block size can flex up to 30M gas

Stellar

- Uses surge pricing mechanism
- Triggers when ledger capacity exceeds 50%
- Fee increases proportionally to network load

Polkadot

- Uses weight-based system
- Measures block weight against target
- Adjusts fees based on block fullness

Tezos

- Monitors block saturation
- Adjusts fees based on recent block usage
- Uses gas limits per operation type

19.6.4 Data Availability market

Ethereum uses blobs, which are special containers for Layer 2 rollups to post their transaction data. They also disappear after a time.

Blob fee is calculated based on the target blob gas per block.

19.7 Network Change Management

19.7.1 Overview

Network change management in DINs encompasses the processes, mechanisms, and stakeholders involved in proposing, discussing, approving, and implementing network modifications. This framework covers everything from minor parameter adjustments to major protocol upgrades.

TODO Design something that can simulate

19.8 Clients

19.9 Bridges

Classification of Bridges. Need to include Lazy Bridges here https://blog.celestia.org/lazybridging/

- Trusted

  - Custodial
  - Multi Signature
  - Federated

- Trustless Bridges
  - Light Client
  - ZK
    - Lazy Bridge
  - Relay

20 Gas

The Fuel of Web3

20.1 Introduction

Imagine trying to mail a package without paying for postage, or running a car without fuel. In Web3, gas serves a similar fundamental purpose - it's the essential resource that powers all blockchain operations. But unlike postage or gasoline, blockchain gas represents something more complex: it's a dynamic pricing mechanism that manages network resources, incentivizes operators, and helps secure the entire system.

This chapter explores gas from multiple perspectives: as a practical tool users must understand, as a technical mechanism that enables network operation, and as an economic system that shapes Web3's evolution.

20.2 Understanding Gas: First Principles

20.2.1 What is Gas?

At its most basic level, gas represents computational effort. Every operation on a blockchain - from simple token transfers to complex smart contract interactions - requires computational resources from the network. Gas measures these resources and assigns them a cost.

Key characteristics of gas include:

- It measures computational complexity
- It's priced dynamically based on network demand
- It's paid in the network's native token
- Failed transactions still consume gas

20.2.2 Why Gas Exists

Gas serves three essential functions:

1. Resource Management
   - Prevents infinite loops and spam attacks
   - Allocates network capacity fairly
   - Creates predictable operational costs
2. Economic Security
   - Compensates network operators
   - Makes attacks economically expensive
   - Aligns incentives across participants
3. Priority Mechanism
   - Determines transaction ordering
   - Manages network congestion
   - Enables price discovery for blockspace

20.3 Gas Mechanics

20.3.1 Basic Components

Every gas transaction involves several components:

1. Gas Limit
   - Maximum computational units allowed
   - Set by the user
   - Must be sufficient for operation
   - Excess is refunded
2. Gas Price
   - Cost per unit of gas
   - Determined by network demand
   - Usually measured in small denominations (e.g., Gwei)
   - Can change rapidly
3. Total Cost
   - Gas Limit × Gas Price

- Paid upfront
- Maximum possible cost
- Actual cost may be lower

20.3.2 Network-Specific Implementations

Different networks handle gas in distinct ways:

1. Ethereum

    - Base fee + priority fee model
    - EIP-1559 burning mechanism
    - Complex gas calculations for different operations
    - Block gas limits

2. Layer 2 Networks

    - Usually cheaper than Layer 1
    - May have different gas tokens
    - Often bundle L1 and L2 costs
    - Can have unique gas mechanics

3. Alternative Networks

    - May use different resource metrics
    - Often optimize for specific use cases
    - Can have fixed or variable costs
    - Might separate different resource types

20.4 User's Guide to Gas

20.4.1 Practical Gas Management

1. Setting Gas Limits

    - Understanding operation costs
    - Adding safety margins
    - Avoiding out-of-gas errors
    - Estimating complex transactions

2. Choosing Gas Prices

    - Reading gas price oracles

- Understanding urgency tradeoffs
- Timing transactions
- Using gas price alerts

3. Common Pitfalls

    - Insufficient gas limits
    - Overpaying during congestion
    - Failed transaction costs
    - Network-specific quirks

20.4.2 Advanced Gas Strategies

1. Gas Optimization

    - Batching transactions
    - Using gas tokens
    - Timing non-urgent transactions
    - Contract interaction efficiency

2. Cross-Network Considerations

    - Bridge gas costs
    - Network selection
    - Cost comparison tools
    - Gas token economics

20.5 Economic Implications

20.5.1 Fee Markets

Gas creates a market for blockspace with unique characteristics:

1. Supply Mechanics

    - Fixed block space
    - Regular block intervals
    - Network-specific limits
    - Upgrade considerations

2. Demand Factors

    - User activity levels

- Market conditions
- Bot competition
- MEV opportunities

20.5.2 Market Impact

Gas mechanics influence broader market behavior:

1. Layer 2 Adoption
   - Cost comparison driving usage
   - Network effects
   - Migration patterns
   - Protocol competition
2. Protocol Design
   - Gas optimization requirements
   - Economic model constraints
   - User experience trade-offs
   - Scaling solutions

20.6 Future of Gas

20.6.1 Evolving Models

Gas systems continue to develop:

1. Technical Innovations
   - Account abstraction
   - Meta-transactions
   - Gas-less transactions
   - Resource-specific pricing
2. Economic Experiments
   - Alternative fee mechanisms
   - Novel burning models
   - Hybrid systems
   - Cross-chain standardization

20.6.2 Implications for Users

As gas systems evolve, users should:

- Stay informed about changes
- Adapt strategies accordingly
- Understand new opportunities
- Manage changing risks

20.7 Key Takeaways

1. Gas is fundamental to Web3:

    - Essential for network operation
    - Drives economic security
    - Shapes user behavior

2. Understanding gas is crucial for:

    - Effective network usage
    - Cost management
    - Strategy development
    - Risk assessment

3. Gas systems are evolving:

    - New models emerging
    - Greater efficiency possible
    - More complexity likely
    - Continued innovation certain

20.8 Practical Exercises

To reinforce your understanding:

1. Calculate total gas costs for different operations
2. Compare gas prices across networks
3. Optimize a multi-step transaction
4. Analyze historical gas patterns

20.9 Further Reading

- Gas optimization guides
- Network-specific documentation
- Economic analysis papers
- Technical proposals

21 dApps

dApps can be single chain or multichain. However they must exist on a DIN and can't exist independently from a DIN. They don't need to have a token to be included here. If an NFT develops functionality, they they'll be inlcuded here too. They can be DeFi SocialFi GameFi CeDeFi Concepts Concepts Flash loans DeFi Derivatives Basis Trading DEX Lending Utility Yield Pendle 3k in Basis Trading Current dApps Ethena USDX BounceBit

Derivatives Liquid staking Derivatives such as Lido, and EtherFi is the primary element here Lending

SocialFi Meme Coins CeDeFi Circle fits in here GameFi

21.1 DEX's

21.2 Name Services

21.3 Privacy

< lipsum 1 >

21.3.1 Railgun

< lipsum 1 >

21.3.2 Tornado Cash

< lipsum 1 >

22 MEV

22.1 Proposer Builder Separation (PBS)

22.2 Multiple Concurrent Leaders

https://x.com/aeyakovenko/status/1810222589991583922

23 Languages

23.1 Solidity

Is a compiled language

Part VI

Financial

24 Digital Assets

The logical place to start this Almanack is Digital Assets. These include all the financial instruments that exist within the Web3 sphere. For us to represent all Digital Assets within this space, it means we need to include all Web3 financial instruments, both on chain and off chain.

We take inspiration from the Fat Protocol Thesis(Monegro 2016) to define the major categories of Digital Assets within the Web3 realm. We also adhere to the naming convention that stipulates Coins are digital assets relating to the running and operation of a Blockchain, whereas Tokens are digital assets that are issued on a Blockchain.

We thus break down Digital Assets into the following Categories:

- Coins
  - Primary Networks
  - Secondary Networks
    - Ozempic
    - Sugar
  - Derivatives
- Tokens
  - Fungibles
  - Non Fungible

After describing the various categories and classes of Digital Assets we'll then delve into the Markets existing for these Digital Assets, as well as how an entity hodls the Digital Asset and the yield properties of the various types of Digital Assets.

24.1 Coins

This section deals primarily with Digital Assets as a Financial Instrument and as such any information relating to the technical makeup can be found in the Blockchain documentation.

24.1.1 Network Economics

Token Models Utility Tokens: Gas fees, staking, governance Security Tokens: Validator requirements, slashing deposits Network Tokens: Transaction fees, block rewards Incentive Structures Validator Rewards: Block rewards, transaction fees, staking yields User Incentives: Fee markets, priority mechanisms, rebate systems Developer Incentives: Grant programs, protocol fees, treasury funding Economic Security Minimum Stakes: Validator requirements, delegation minimums Slashing Conditions: Downtime penalties, malicious behavior penalties Market Making: Liquidity incentives, trading pair support

24.1.2 Base Networks

This Almanack distinguishes between the financial properties of Coins versus the technical properties of a Blockchain. As such we don't refer to networks here by Layer 1 or Layer 2. That's a classification and distinction you can explore here.

We define a Base Network that maintains it's own Sovereignity. This means that the Coin on the network is used to economically secure the chain as well as final settlement to occur on this network.

24.1.3 Secondary Networks

These are networks that market themselves as settling the transactions on another network. The nuances of how they settle is covered under the Blockchain chapter. We'll encompass the full breadth of L2's including, but not limited to Plasma, Sidechains, Rollups etc.

We then break these networks into Ozempic or Sugar networks. This reflects a hat tip to the Fat protocol metaphor. Ozempic networks are net extractors of value from their host chain, while Sugar networks cause the host chain to become fatter and therefore hold more value.

Please see Ozempic Effect to see how we determine if a network in a net ozempic or sugar network.

24.1.4 Derivatives

- On chain
  - Wrapped
    - Pure
    - Bridged
- Off Chain
  - Spot ETF's

24.1.4.1 On Chain Derivatives

24.1.4.2 Off Chain Derivatives

24.2 Tokens

24.2.1 Fungible

Fungible is a pretty terrible name, but it roughly means divisable. It's easier to explain via an example. If I have 10 dollars and I give you 3. I still have 7. It's divisable. If I have a car and I want to give you 30% of it, I cannot cut it up and give you a portion of it. It's Non fungible, or non divisable. There's more nuances which we can deal with in the vocabulary section. But that's the general idea of it.

We have the following types: * Stable Coins * Fiat backed * Crypto backed * Delta Neutral backed * Shit Coins * Governance * Meme * Utility

Then we have numerous standards. We'll add only the most popular and relevant ones here.

Namely: * ERC20 * ERC777 * ERC1363 * BRC20 * Runes * Solana's SPL Token Standard * ICS20

24.2.1.1 ICS20

The Inter-Chain Standard 20 is a Cosmos based standard for fungible token transfers between blockchains using the Inter-Blockchain Communication Protocol (IBC)

24.2.2 Non Fungible

Has the following attributes:

- Art & Collectibles
- Profile Picture (PFP)
- Gaming
- Domain Names and Identity
- Real World Assets (RWA)

The NFT floor price is the lowest price at which an NFT from a particular collection is listed for sale on a marketplace. It serves as a benchmark for the collection's market value and is widely used to assess the entry point for potential buyers and to gauge the collection's popularity and liquidity.

24.3 Markets

Where can I buy these Digital Assets? The major markets are regulated and unregulated.

These are then divided into spot vs derivatives.

For regulated it's interesting as RedBelly in a blockchain, but it has KYC/AML. So is that regularly compliant. It's probably more truthful to break it down not by regulatory compliance, but anonymity. For if your on chain activity can be tracked then most mature jurisdictions will be able to force an individual to be compliant.

24.4 Hodling

Wallets

24.4.1 Custodial

24.4.2 Non-Custodial

- Pure
  - Cold
  - Hot
- Smart
  - MPC
  - Smart Contract Based (Includes Account Abstraction)

24.5 Yield Properties

Major categories are:

- Network Yield
- Trading Yield
- Protocol Yield

24.5.1 Trading Yield

- Pricing appreciation
- Arbitrage Yield
  - Spot Arbitrage
  - Peg Arbitrage - These are unique to stable coins
- Options and Derivatives Premiums
- Futures funding rates

24.5.2 Network Yield

- Mining Yield
  - Solo Mining
  - Pool Mining
  - Cloud Mining
- Validating Yield
  - Staking
- Network Fee Yield
  - Gas
- MEV
  - Toxic
  - Non Toxic
- Derivatives
  - Liquid Staking

24.5.3 dApp Yield

- Staking
- Liquidity Provision
- Governance Participation
- NFT Rental Income

24.5.3.1 Liquidity Provision

We break this down into the following Categories

- AMM Pool fees
- Concentrated liquidity positions
- Order book market making
- Lending and Borrowing markets

24.5.3.1.1 Concentrated Liquidity Provision

Here we will break down rebalancing and focus on Loss Versus Rebalancing as per this paper https://arxiv.org/pdf/2208.06046

25 Market Structures

Financial markets are complex systems that have evolved over centuries to facilitate the efficient exchange of assets. In this chapter, we'll explore the fundamental structures that make modern markets possible, with a particular focus on how traditional market mechanisms have influenced and been adapted by cryptocurrency markets.

25.1 Understanding Market Structure Basics

At its core, a market is where buyers and sellers come together to trade. But the way this meeting happens has profound effects on how prices are discovered, how fairly participants are treated, and how efficiently trades are executed. Let's examine the key concepts that underpin all market structures.

25.1.1 Price Discovery

Price discovery is the process by which markets determine the true price of an asset. Think of it as the market's way of collectively agreeing on what something is worth. This process is influenced by:

- The flow of new information
- The number of market participants
- The transparency of trading activity
- The rules and mechanisms of the trading venue

For example, when a company announces unexpected positive earnings, traders rushing to buy the stock help discover its new, higher price. In crypto markets, this process happens 24/7, with global participation leading to near-instant price adjustments as new information emerges.

25.1.2 Liquidity

Liquidity is the ease with which an asset can be bought or sold without causing a significant price movement. It's like the depth of a swimming pool - the deeper it is, the less splash you make when jumping in. High liquidity is characterized by:

- Tight bid-ask spreads
- Large order book depth
- High trading volumes
- Minimal price impact from trades

25.2 Central Limit Order Books (CLOBs)

The Central Limit Order Book (CLOB) is perhaps the most important innovation in market structure history. It's essentially a sorted list of all the prices at which market participants are willing to buy (bids) and sell (asks) an asset.

25.2.1 How CLOBs Work

A CLOB operates on simple but powerful principles:

1. **Order Types**
   - Limit Orders: Instructions to buy or sell at a specific price or better
   - Market Orders: Instructions to buy or sell immediately at the best available price
2. **Price-Time Priority**
   - Orders are matched based on price priority (best prices first)
   - When prices are equal, earlier orders get priority
   - This creates a fair "first come, first served" system

Here's a simplified visualization of an order book:

```
     ASKS
Price | Size
105   | 10
104   | 15
103   | 20
-----------------
102   | 25
101   | 30
100   | 35
     BIDS
```

25.2.2 Order Matching Logic

When new orders arrive, they're matched against existing orders following strict rules:

1. Market orders match immediately with the best available price
2. Limit orders join the book if they can't match immediately
3. Partial fills are possible when order sizes don't match exactly

For example, if someone submits a market buy order for 30 units in the above book, they would: - Buy 20 units at 103 - Buy 10 units at 104 - Pay an average price of 103.33

25.3 Evolution to Electronic Markets

The transition from physical trading floors to electronic markets marked a revolutionary change in market structure. Electronic markets brought:

- Faster execution speeds
- Lower transaction costs
- Broader market access
- More sophisticated trading strategies
- Better price transparency

However, they also introduced new challenges like: - Need for robust technology infrastructure - Complex failure modes - High-frequency trading arms race - New forms of market manipulation

25.4 Crypto Market Adaptations

Cryptocurrency markets have taken traditional market structures and adapted them for a decentralized world. This has led to several innovations:

25.4.1 Centralized Exchange Order Books

Crypto exchanges like Binance and Coinbase operate traditional CLOBs but with some key differences: - 24/7 trading - Global access - Multiple quote currencies - Faster settlement - Novel order types

25.4.2 On-Chain Order Books

Attempting to put order books entirely on-chain has revealed interesting challenges: - High gas costs for order placement - Front-running vulnerability - Block time limitations - Settlement finality considerations

25.4.3 Hybrid Solutions

Modern crypto trading often uses hybrid approaches that combine the best of both worlds: - Off-chain order books with on-chain settlement - Layer 2 scaling solutions - State channels for high-frequency trading - Automated Market Makers (AMMs) as complementary liquidity sources

25.5 Market Structure Implications

The choice of market structure has far-reaching implications for:

25.5.1 Trading Strategy

Different market structures favor different trading approaches. CLOBs are ideal for market making and arbitrage, while AMMs excel at providing passive liquidity.

25.5.2 Market Quality

Market structure affects: - Price efficiency - Transaction costs - Market stability - Fair access

25.5.3 Regulatory Compliance

Market structure choices impact: - Regulatory oversight capability - Market manipulation risk - Customer protection measures - Systemic risk management

25.6 Looking Ahead

Market structures continue to evolve as technology advances and new requirements emerge. Future developments may include: - Greater integration between TradFi and DeFi markets - Novel hybrid market structures - Improved privacy solutions - More efficient cross-chain trading mechanisms

26 Key Takeaways

- Market structures fundamentally shape how assets are traded
- CLOBs remain the gold standard for price discovery and fair trading
- Electronic markets have transformed trading but introduced new challenges
- Crypto markets are innovating on traditional structures while maintaining their core principles
- The future likely holds further convergence between traditional and crypto market structures

27 Further Reading

- Flash Boys by Michael Lewis
- Trading and Exchanges by Larry Harris
- “Understanding Market Microstructure” series on the CME website

27.0.1 Market Caps

Let’s start with a practical example. Imagine two tokens:

Token A: - Total supply: 1 million tokens - Current price: $1 - Market cap: $1 million - Liquidity in DEX pools: $500,000

Token B: - Total supply: 1 billion tokens - Current price: $0.001 - Market cap: $1 million - Liquidity in DEX pools: $5,000

While both tokens show the same market cap, they tell very different stories. Token A has deep liquidity - you could sell $100,000 worth without crashing the price. Token B might crash 90% if someone tries to sell just $1,000 worth.

27.1 Types of Market Cap

In DeFi, we need to understand several variations:

1. Circulating Market Cap = Current Price × Circulating Supply The value of tokens currently trading in the market

2. Fully Diluted Valuation (FDV) = Current Price × Total Supply The theoretical value if all tokens were in circulation

3. Realized Market Cap = Sum of (Price × Amount) for each token last moved A measure that helps identify actual economic activity

27.2 The Liquidity Ratio

One of the most important metrics rarely discussed is the liquidity ratio: Liquidity Ratio = Total DEX Liquidity / Market Cap

Generally: - Ratio > 0.1: Healthy liquidity - Ratio 0.01-0.1: Exercise caution - Ratio < 0.01: High manipulation risk

27.3 Market Cap Manipulation

Understanding how market cap can be manipulated helps avoid common traps:

1. Supply Manipulation
    - Burning tokens to artificially reduce supply
    - Hidden minting capabilities
    - Lock-up periods that temporarily restrict supply
2. Price Manipulation
    - Wash trading to create fake volume
    - Thin liquidity pools easily moved by small trades
    - Strategic buying to push price before token launches
3. Liquidity Games
    - Temporary liquidity adds before major announcements
    - Cross-chain liquidity that's hard to track
    - Flashloan attacks that distort price momentarily

27.4 Real Value vs. Market Cap

Market cap becomes more meaningful when viewed alongside other metrics:

- Daily Active Users (DAU)
- Revenue or fees generated
- Treasury holdings
- Protocol-owned liquidity
- Cross-chain presence and activity

Think of market cap as just one instrument in an orchestra - it only makes sense when played in harmony with other metrics.

27.5 Red Flags in Market Cap Analysis

Watch for these warning signs: - Market cap growing faster than user adoption - Large gaps between circulating and total supply - Sudden changes in supply without clear reason - Market cap much higher than total value locked (TVL)

27.6 Using Market Cap in Trading Decisions

Market cap can be valuable when used correctly:

1. For relative valuation between similar protocols
2. Identifying potential manipulation
3. Assessing room for growth
4. Understanding total risk exposure

Remember: Market cap is a trailing indicator showing where a token has been, not necessarily where it's going.

27.7 Conclusion

Market capitalization in DeFi requires a more sophisticated understanding than in traditional finance. While it shouldn't be ignored, it should never be the only metric you consider. The most successful traders and investors learn to look beyond market cap to understand true value and risk.

28 Ratings

This section will describe our ratings model for Digital Assets.

28.1 Core Rating Categories (60% of Total Rating)

28.1.1 1. Protocol Value Capture (30%)

A. Network Effect Metrics

- Daily Active Users (DAUs)
- Total Value Locked (TVL)
- Transaction volume
- Fee revenue generated
- Protocol revenue retained

B. Value Accrual Mechanisms

- Token economics design
- Fee distribution model
- Staking mechanisms
- Burns and supply dynamics

C. Ozempic Network Effects

- Value extraction efficiency from L1
- Transaction fee capture rate
- User migration metrics from L1
- TVL migration patterns
- Gas savings versus L1
- L1-L2 Value Dynamics
- Sequencer revenue distribution
- MEV capture and distribution
- Bridge volume and efficiency
- Settlement layer costs
- Sustainable Value Creation
- Net new users versus L1 migration

- Ecosystem-specific applications
- Novel transaction types impossible on L1
- Cross-L2 interoperability metrics

28.1.2 2. Protocol Security & Risk Assessment (30%)

A. Smart Contract Security

- Audit history and quality
- Bug bounty program effectiveness
- Historical vulnerability incidents
- Code complexity metrics
- Upgrade mechanism security
- Testing coverage

B. Network Security

- Consensus mechanism robustness
- MEV exposure and protection measures
- Node distribution
- Network attack resistance
- Cross-chain bridge security
- Oracle dependency and security

C. L1 Dependency Risks

- Settlement layer congestion exposure
- Bridge security and liquidity depth
- L1 fee market correlation
- Sequencer centralization risk
- Value extraction sustainability

28.2 Risk Categories (40% of Total Rating)

28.2.1 1. Technical Risk Assessment (15%)

A. Smart Contract Vulnerabilities - Code audit findings severity - Time-tested deployment - Complexity of interactions - Dependencies on external protocols - Historical incident analysis

B. Network Level Risks

- MEV exposure metrics
- Network partition resistance

- Node centralization factors
- Infrastructure dependencies
- Cross-chain vulnerability exposure

C. Key Management & Wallet Security

- Multi-sig implementation
- Key generation processes
- Hardware security modules usage
- Social recovery mechanisms
- Access control systems

28.2.2 2. Economic Risk Assessment (10%)

A. Market Dynamics

- Liquidity concentration
- Price impact resistance
- Collateral quality
- Market manipulation resistance

B. Economic Model Vulnerabilities

- Game theory attack vectors
- Incentive alignment analysis
- Economic exploit resistance
- Stress test scenarios
- Flash loan attack surface

28.2.3 3. Operational Risk Assessment (10%)

A. CeFi/CeDeFi Risks

- Centralization points
- Custody arrangements
- Third-party dependencies
- Operational redundancy
- Emergency procedures

B. Oracle Dependencies

- Oracle manipulation resistance
- Price feed reliability
- Backup oracle systems

- Historical oracle incidents
- Data quality metrics

28.2.4 4. External Risk Assessment (5%)

A. Regulatory Risk

- Jurisdictional exposure
- Compliance frameworks
- Regulatory clarity
- Legal structure
- Historical regulatory interactions

B. Social Engineering Risk

- Team security practices
- Access control policies
- Social attack history
- Security awareness training
- Incident response readiness

28.3 Risk-Adjusted Rating Scale

AAA: Exceptional protocol with comprehensive risk mitigation

- Multiple independent security audits with no critical findings
- Proven resistance to all major attack vectors
- Strong regulatory compliance framework
- Decentralized operations with minimal points of failure
- Multiple layers of economic security

AA: Strong protocol with robust risk management

- Regular security audits with minor findings
- Documented resistance to common attack vectors
- Clear regulatory strategy
- Limited centralization risks
- Strong economic security measures

28.4 Risk Multipliers

Each risk category can apply a multiplier to the base rating:

- Critical Risk: -3 rating notches
- High Risk: -2 rating notches
- Medium Risk: -1 rating notch
- Low Risk: No adjustment
- Minimal Risk: +1 rating notch

28.5 Continuous Monitoring Triggers

- Smart contract vulnerability disclosure
- Network attack detection
- Regulatory action
- Economic model stress
- Oracle deviation events
- Cross-chain bridge incidents
- Social engineering attempts
- MEV activity spikes

28.6 Review Framework

- Monthly security metric review
- Quarterly risk assessment update
- Annual comprehensive review
- Real-time monitoring of critical indicators
- Incident-triggered reassessment

28.7 Ozempic Effect

We'll base this upon value flows. Defillama doesn't actually display this. So we'll need to get this data directly from the smart contracts. We can start with Base, Arbitrum, BSC, Optimism and Polygon.

Let's build a comprehensive framework for tracking the true "Ozempic effect" of L2s on Ethereum. We'll need several interconnected metrics to understand the complete value flow dynamics.

1. Wallet Migration Analysis

- Track addresses that first appeared on Ethereum before a certain date (let's call them "Ethereum Native Wallets")
- Monitor their activity transition to L2s over time
- Analyze their ETH holdings distribution between L1 and L2s
- Calculate the ratio of their transaction activity on L2s versus L1

2. L2 Native User Analysis

- Identify wallets that first appeared on L2s
- Track what percentage never bridge to Ethereum
- Measure their total value held
- Calculate their transaction activity

3. Fee Flow Dynamics

- Track L2 sequencer fees paid back to Ethereum
- Calculate the net fee difference (what these transactions would have cost on L1 versus actual L2 + L1 calldata costs)
- Monitor the ratio of fees paid back to Ethereum versus fees retained by the L2

We could create a composite "Value Migration Score" that looks like:

```
def calculate_migration_score(l2_data):
    # Value Migration
    eth_native_migration = (
        eth_native_wallets_on_l2 / total_eth_native_wallets *
        eth_value_moved_to_l2 / original_eth_holdings
    )

    # Activity Migration
    activity_migration = (
        l2_transactions_by_eth_wallets /
        (l1_transactions_by_eth_wallets + l2_transactions_by_eth_wallets)
    )

    # L2 Native Growth
    l2_native_strength = (
        l2_only_wallets / total_l2_wallets *
        l2_native_value / total_l2_value
    )

    # Fee Economics
    fee_efficiency = (
        sequencer_fees_to_ethereum /
        theoretical_l1_fees_for_same_transactions
    )

    return (
        eth_native_migration * 0.3 +
        activity_migration * 0.3 +
        l2_native_strength * 0.2 +
        fee_efficiency * 0.2
    )
```

This would give us a quantitative measure of how effectively an L2 is:

1. Attracting value from Ethereum
2. Generating new value through native users
3. Maintaining a sustainable fee relationship with Ethereum

A true Ozempic L2 should show:

- High migration of ETH native wallets
- Strong L2 native user growth
- Efficient fee generation that still provides meaningful revenue to Ethereum
- Sustained or growing activity ratios over time

Would you like me to elaborate on how we could implement the data collection for any of these metrics, or should we explore additional factors to consider in the scoring?

- Net Value Extraction Rate = (Value Bridged In - Value Bridged Out) / Total Time Period

28.8 Risk Factors

28.8.1 1. Technical Risks

- Implementation bugs
- Security vulnerabilities
- Upgrade coordination failures
- Network splits

28.8.2 2. Governance Risks

- Capture by special interests
- Low participation
- Contentious decisions
- Unclear processes

28.8.3 3. Social Risks

- Community fragmentation
- Loss of developer support
- Reputation damage
- Market impacts

28.9 Future Considerations

28.9.1 1. Emerging Trends

- Automated governance systems
- AI-assisted proposal analysis
- Cross-chain governance
- Dynamic parameter adjustment

28.9.2 2. Challenges

- Scaling governance participation
- Balancing security and innovation
- Managing increasing complexity
- Maintaining decentralization

28.9.3 3. Opportunities

- Improved governance tools
- Better simulation capabilities
- Enhanced coordination mechanisms
- More sophisticated voting systems

28.10 Dependent Network Ratings

Polygon zkEVM Settlement Guarantees (10/10 weight): Score: 9/10 The zkEVM uses zero-knowledge proofs to validate all state transitions. Every transaction batch includes a proof that mathematically demonstrates the correctness of all computations and state changes. These proofs are verified by Ethereum's consensus mechanism, providing cryptographic certainty that state transitions are valid. This is nearly the highest level of settlement guarantee possible, just slightly below fully integrated L2s because of some optimizations in the proving system.

Dispute Resolution (9/10 weight): Score: 10/10 Ethereum serves as the absolute source of truth for the zkEVM. If there's ever a dispute about the state, the zero-knowledge proofs verified by Ethereum's consensus provide mathematical certainty about what is correct. There's no dependency on fraud proofs or challenge periods - the cryptographic proofs mean disputes are resolved immediately and with absolute certainty by Ethereum.

Economic Security Inheritance (8/10 weight): Score: 9/10 The zkEVM inherits its fundamental security from Ethereum. The validity proofs mean it can't confirm invalid state transitions, and its assets are secured by Ethereum's consensus mechanism. While it has its own token (MATIC) for gas fees and other purposes, the core economic security - particularly for assets like ETH and tokens - comes directly from Ethereum.

State Finality (7/10 weight): Score: 9/10 Once Ethereum confirms a zkEVM batch and its validity proof, that state is final with the same guarantees as Ethereum itself. The mathematical nature of the zero-knowledge proofs means there's no waiting period for finality beyond Ethereum's own finality period. This is as strong as state finality can get for a settlement-dependent network.

Exit Rights Guarantees (6/10 weight): Score: 8/10 Users can always withdraw their assets back to Ethereum by submitting a withdrawal request. These withdrawals are guaranteed by Ethereum's consensus - once a withdrawal is proven valid through a ZK proof, no one can prevent the user from claiming their assets on Ethereum. The only limitation is the normal proving and processing time.

State Progression Dependency (5/10 weight): Score: 7/10 While the zkEVM can process transactions independently, it can't finalize new states without submitting proofs to Ethereum and having them verified. This creates a strong dependency on Ethereum for state progression, though there's some independence in transaction processing.

Asset Movement (4/10 weight): Score: 10/10 Native ETH and ERC-20 tokens can move seamlessly between Ethereum and the zkEVM. When assets move to the zkEVM, they're locked on Ethereum and can only be unlocked through valid proofs. This provides the strongest possible guarantees for asset movement between the networks.

Total Score: 62/70 (approximately 89%)

This analysis places Polygon zkEVM firmly in the "Fully Non-Sovereign" category. Arbitrum Let me analyze Arbitrum's relationship with Ethereum as a Settlement-Dependent Network by carefully examining each criterion. This will help us understand how optimistic rollups differ from ZK rollups in their settlement dependency.

Settlement Guarantees (10/10 weight): Score: 7/10 Arbitrum uses an optimistic rollup design where transactions are assumed valid but can be challenged during a dispute period (currently 7 days). While this provides strong settlement guarantees, it's not as immediate or mathematically certain as ZK rollups. The challenge period introduces a time-based element to settlement finality. However, the ability to prove fraud on Ethereum's consensus layer still makes this a robust settlement mechanism.

Dispute Resolution (9/10 weight): Score: 8/10 Ethereum serves as the ultimate arbiter for Arbitrum through its fraud proof system. If someone identifies an invalid state transition, they can submit a fraud proof to Ethereum, which will automatically resolve the dispute and revert invalid transactions. This is strong dispute resolution, though not as immediate as ZK proofs since it requires active challengers and a challenge period. The key strength is that Ethereum's consensus automatically enforces the correct resolution once fraud is proven.

Economic Security Inheritance (8/10 weight): Score: 9/10 Arbitrum inherits its fundamental security from Ethereum. The ability to prove fraud on Ethereum means that any attempt to corrupt Arbitrum's state would require corrupting Ethereum itself. The sequencer role adds some centralization risk, but the fundamental economic security - particularly for assets - comes directly from Ethereum. Users can always force transactions through Ethereum if the sequencer fails.

State Finality (7/10 weight): Score: 6/10 While Arbitrum's state updates are recorded on Ethereum, true finality requires waiting through the challenge period. This creates a tradeoff between practical finality (which can be quite fast) and absolute finality (which requires waiting for the challenge period). This is lower than ZK rollups where finality is immediate once proofs are verified.

Exit Rights Guarantees (6/10 weight): Score: 8/10 Users can always withdraw their assets to Ethereum, guaranteed by Ethereum's consensus. While withdrawals require waiting through the challenge period, they cannot be prevented by Arbitrum's operators. The delay is longer than with ZK rollups, but the guarantee is just as strong once the period passes.

State Progression Dependency (5/10 weight): Score: 7/10 Arbitrum can process transactions independently but must submit state roots to Ethereum for potential verification. While it has more processing independence than some systems, it ultimately depends on Ethereum for final state confirmation, especially during disputes.

Asset Movement (4/10 weight): Score: 10/10 Native ETH and ERC-20 tokens move seamlessly between Ethereum and Arbitrum through a strong bridge mechanism backed by Ethereum's consensus. When assets move to Arbitrum, they're locked on Ethereum and can only be unlocked through valid withdrawals after the challenge period.

Total Score: 55/70 (approximately 79%)

This analysis places Arbitrum in the “Fully Non-Sovereign” category, though with a lower score than Polygon zkEVM. The main differences come from the challenge period required for absolute finality and the reliance on fraud proofs rather than validity proofs.

Stacks Settlement Guarantees (10/10 weight): Score: 4/10 Stacks uses Bitcoin for checkpointing and security anchoring However, it lacks cryptographic enforcement of settlement by Bitcoin’s consensus Bitcoin doesn’t automatically enforce or validate Stacks’ state transitions Falls into the “checkpoint systems” category rather than stronger settlement guarantees Dispute Resolution (9/10 weight): Score: 3/10 While Stacks records its state on Bitcoin, Bitcoin’s consensus doesn’t serve as the ultimate arbiter Disputes are primarily resolved within Stacks’ own consensus mechanism Bitcoin can’t automatically correct or resolve issues in Stacks’ state Economic Security Inheritance (8/10 weight): Score: 6/10 Miners must commit actual Bitcoin through PoX mechanism This creates some economic security dependency on Bitcoin However, Stacks maintains its own economic incentives through STX State Finality (7/10 weight): Score: 5/10 Stacks achieves finality through a combination of its own consensus and Bitcoin anchoring State is recorded on Bitcoin but not in a way that Bitcoin consensus enforces Provides stronger finality than fully independent chains but weaker than true L2s Exit Rights Guarantees (6/10 weight): Score: 4/10 With sBTC, users can move Bitcoin between chains However, this relies on Stacks’ mechanisms rather than being guaranteed by Bitcoin’s consensus Exit rights depend on threshold signatures rather than cryptographic guarantees State Progression Dependency (5/10 weight): Score: 7/10 Stacks blocks are linked to Bitcoin blocks through PoX State progression is tied to Bitcoin’s block progression However, Stacks can still process transactions independently within this framework Asset Movement (4/10 weight): Score: 5/10 sBTC enables Bitcoin movement between chains But this movement isn’t directly enforced by Bitcoin’s consensus Relies on threshold signatures and Stacks’ mechanisms Total Score: 34/59 (approximately 58%)

This places Stacks in the “Moderately Dependent” category on our spectrum.

28.11 Risks

Sub categories of risks include smart contract vulns regulatory risks centralization risks for CeDeFi and CEX’s MEV network level key and wallet compromise cross chain exploits oracle manipulation Social engineering exploitation of economic models

29 Trollip's Index

Trollip's index, taking a cue from the S&P 500, will aim to classify 500 Digital Assets.

The general approach would be to classify the top 500 via marketcap. However, a good characteristic of a degen is to not follow conventional wisdom and groupthink. So as the Almanack grows and more strategies are added to the the Degen Chapters, we'll add the assets as we discuss strategies around them. This means that it will contain some absolute shit coins. This will also help us to refine our Risk models

29.1 BTC

Bitcoin has emerged as the world's first successful digital store of value, creating a new paradigm for wealth preservation in the digital age. Much like gold served ancient civilizations through to modern times as a reliable store of wealth, Bitcoin provides similar characteristics but with distinct advantages native to the digital realm.

At its foundation, Bitcoin's value proposition rests on its absolute scarcity - there will never be more than 21 million bitcoins. This hard cap, combined with a transparent and immutable issuance schedule through mining "halvings" every four years, creates a predictability that even gold, with its uncertain mining output, cannot match. When new gold deposits are discovered or mining technology improves, supply can increase unexpectedly. Bitcoin's supply schedule, in contrast, is mathematically certain.

Bitcoin's digital nature offers significant advantages over traditional stores of value. Unlike gold, it can be transferred instantly across borders, divided into microscopic units, stored without physical vault costs, and verified for authenticity without specialized equipment. Its self-custody properties allow individuals to maintain direct control over their wealth without relying on third-party custodians or financial institutions.

The network's security model, backed by massive computational power through proof-of-work mining, has proven remarkably resilient over more than a decade. This track record has gradually built confidence among institutional investors, who increasingly view Bitcoin as a legitimate asset class for portfolio diversification and inflation hedging. Major financial institutions now offer Bitcoin investment products, while some corporations have adopted it as a treasury reserve asset.

While Bitcoin began as a peer-to-peer electronic cash system, its evolution into a store of value mirrors how gold transformed from a medium of exchange into a wealth preservation tool. The emergence of Layer 2 solutions like the Lightning Network now handles Bitcoin's payments functionality, allowing the base layer to focus on its primary role as digital gold - the foundational layer of monetary security in the cryptocurrency ecosystem.

29.1.1 Derivatives

29.1.1.1 cbBTC

Coinbase Base Bitcoin (cbBTC) represents a novel approach to Bitcoin tokenization, launched by Coinbase to bridge the gap between Bitcoin and Ethereum-based DeFi applications. It functions as an institutional-grade wrapped version of Bitcoin, backed 1:1 by actual Bitcoin held in Coinbase's custody. What makes cbBTC particularly noteworthy is its institutional focus, leveraging Coinbase's reputation as a publicly traded company and its robust custody infrastructure to provide a secure and regulated way to use Bitcoin across different blockchain ecosystems.

The technical architecture of cbBTC operates through a burn-and-mint mechanism on the Base network, Coinbase's layer-2 blockchain built on top of Ethereum. When users deposit Bitcoin into Coinbase's custody, an equivalent amount of cbBTC is minted on Base. This process allows Bitcoin holders to participate in Base's growing DeFi ecosystem while maintaining exposure to Bitcoin's value. The token implements additional security measures, including proof of reserves and regular audits, making it particularly appealing to institutional investors who require high levels of security and regulatory compliance. Unlike some other wrapped Bitcoin tokens, cbBTC's key differentiator is its direct integration with Coinbase's established infrastructure and its focus on institutional-grade security and compliance measures.

29.2 ETH

Ethereum represents a revolutionary leap in computing - it's humanity's first attempt at creating a global, decentralized computer that's always running and accessible to everyone. Like how the internet connected computers worldwide for information sharing, Ethereum connects computers globally to create a single, unified computational platform that no one controls but everyone can use.

Think of Ethereum as a massive, worldwide computer with some unique properties: it never shuts down, can't be censored, and maintains perfect records of everything it processes. Instead of storing photos or documents like a regular computer, this world computer specializes in running smart contracts - pieces of code that automatically execute agreements and handle digital assets without needing intermediaries.

ETH, the network's native asset, serves as the essential "fuel" that powers this world computer. Every computation, whether it's processing a DeFi trade or minting an NFT, requires ETH to run. After Ethereum's transition to Proof of Stake through The Merge, ETH also gained a new role - network validators must stake ETH to participate in securing the network, similar to how a computer needs electricity to function and stay secure.

What makes Ethereum truly revolutionary is its programmability. Just as early personal computers transformed from specialized calculators into general-purpose machines that could run any software, Ethereum evolved blockchain technology from a simple transaction ledger into a platform that can run any programmable application. This has spawned entire new industries: decentralized finance (DeFi) protocols that operate 24/7 without human intervention, NFT marketplaces that enable digital ownership and royalties, and DAOs that coordinate human activity through code rather than hierarchies.

The platform continues to evolve through ambitious technical upgrades. Layer 2 scaling solutions like rollups act as specialized processors that handle heavy computations off the main chain, while the planned implementation of sharding will divide the network into parallel processing units - similar to how modern computers use multiple cores to increase performance. These improvements aim to make the world computer more efficient and accessible while maintaining its core properties of decentralization and security.

As this world computer grows in capability and adoption, ETH's value proposition strengthens - it's not just a digital asset, but the essential resource needed to access and use what might become the foundation of our digital future.

Part VII

Social

30 Governance

This section will compare how Blockchains implement the three tiers of traditional governance. Namely:

- Legistlative - Who makes the rules and how they created
- Executive - Who executes the rules
- Judicial - Referee between them

So in Bitcoin BIP's cover the Legislative aspect, Executive is Node operators for Networks then for dapps it gets more complex. Judicial is where it gets challenging. This is pretty much the entire community. People interpret rules by economic activity and nodes. Look at Bitcoin Cash. No money. So everyone agreed with the block size of Bitcoin.

There is also the concept of Canvassing or Lobbying can also occur. Let's look at Ethereum. If I wanted to increase the gas limit from 30 million to 31 million. I'd need to canvas all the nodes to come along with me. Currently there is 5,333 nodes. So I'd need to convince ~3k node operators to increase the gas limit.

30.0.0.1 1. Hard Forks

- **Definition**: Protocol changes that make previously invalid blocks/transactions valid (or vice-versa), requiring all nodes to upgrade
- **Characteristics**:
  - Non-backwards compatible
  - Requires coordinated network upgrade
  - Creates potential for chain splits if not unanimously adopted
- **Use Cases**: Major protocol upgrades, fundamental rule changes, bug fixes
- **Examples**: Ethereum's merge to PoS, Bitcoin's SegWit upgrade

30.0.0.2 2. Soft Forks

- **Definition**: Backwards-compatible protocol changes that tighten rules without invalidating existing blocks
- **Characteristics**:

    - Backwards compatible
    - Old nodes can still participate (with limitations)
    - Lower coordination requirements
- **Use Cases**: Adding new features, incremental improvements
- **Examples**: Bitcoin's P2SH implementation, taproot upgrade

30.0.0.3 3. Parameter Updates

- **Definition**: Changes to network variables within predefined bounds
- **Characteristics**:
    - No code changes required
    - Often automated through on-chain governance
    - Lower risk than protocol changes
- **Use Cases**: Fee adjustments, block size modifications, staking parameters
- **Examples**: Tezos' regular parameter updates, Cosmos' governance parameters

30.0.1 Governance Mechanisms

30.0.1.1 1. Off-Chain Governance

- **Characteristics**:
    - Social consensus through discussion forums, social media, conferences
    - Informal decision-making processes
    - Relies on node operator coordination
- **Advantages**:
    - Flexible and adaptable
    - Allows for nuanced discussion
    - Natural resistance to capture
- **Disadvantages**:
    - Can be slow and messy
    - May lack clear resolution mechanisms
    - Potential for contentious outcomes

30.0.1.2 2. On-Chain Governance

- **Characteristics**:
  - Formal voting mechanisms
  - Smart contract-based execution
  - Token-weighted or identity-based participation
- **Advantages**:
  - Clear process and outcomes
  - Automated execution
  - Transparent participation
- **Disadvantages**:
  - Potential plutocratic capture
  - Reduced flexibility
  - Voter apathy risks

30.0.1.3 3. Hybrid Systems

- **Characteristics**:
  - Combines off-chain discussion with on-chain execution
  - Multiple stages of proposal refinement
  - Mixed participation models
- **Advantages**:
  - Balances flexibility with formality
  - Combines benefits of both approaches
  - Can adapt to different types of changes
- **Examples**: Polkadot's governance system, Cosmos Hub's proposal process

30.0.2 Improvement Proposal Systems

30.0.2.1 1. Structure

- **Stages**:
  - Draft: Initial proposal development
  - Review: Community feedback and refinement
  - Last Call: Final period for major objections
  - Accepted/Final: Ready for implementation

  - Rejected: Proposal declined

- **Components**:
  - Technical specification
  - Motivation and rationale
  - Backwards compatibility analysis
  - Reference implementation (if applicable)
  - Security considerations

30.0.2.2 2. Common Frameworks

- **BIP (Bitcoin Improvement Proposals)**:
  - Focus on consensus changes
  - Conservative approach
  - High emphasis on security
- **EIP (Ethereum Improvement Proposals)**:
  - Multiple tracks (Core, ERC, Interface)
  - Regular cadence of updates
  - Strong emphasis on standardization
- **Network-Specific Systems**:
  - Customized to network needs
  - Varying levels of formality
  - Different voting thresholds

30.0.3 Centralization Factors

30.0.3.1 1. Development Centralization

- **Core Development Teams**:
  - Control over codebase
  - Technical expertise concentration
  - Funding dependencies
- **Client Implementation**:
  - Diversity of node software
  - Implementation independence
  - Bug discovery and fixes

30.0.3.2 2. Governance Centralization

- **Voting Power Distribution**:
  - Token concentration
  - Delegate systems
  - Voter participation rates
- **Proposal Control**:
  - Who can propose changes
  - Filtering mechanisms
  - Discussion venue control

30.0.3.3 3. Infrastructure Centralization

- **Node Operation**:
  - Geographic distribution
  - Hardware requirements
  - Operating costs
- **Service Providers**:
  - API services
  - Block explorers
  - Development tools

30.0.4 Best Practices

30.0.4.1 1. Change Management

- Clear documentation of changes
- Adequate testing periods
- Coordinated upgrade schedules
- Emergency response procedures

30.0.4.2 2. Community Engagement

- Regular communication channels
- Multiple feedback mechanisms
- Transparent decision-making
- Educational resources

30.0.4.3 3. Technical Implementation

- Comprehensive testing frameworks
- Clear upgrade paths
- Fallback mechanisms
- Security audits

31 Contributing

This Almanack will change often and get things wrong. It's only by being intellectually honest that it can ever hope to be the canonical guide to crypto and Web3. We follow Sophocles as our North Star

> "All men make mistakes, but a good man yields when he knows his course is wrong, and repairs the evil. The only crime is pride." Here we'll list all the outstanding contributions we're looking for.

I'll also use it as a dumping ground where I can keep track of things I need to read to include:

- https://bitcoinrollups.org/
- https://tr3y.io/articles/crypto/bitcoin-zk-rollups.html

31.1 Current requirements

31.1.1 Translations

Be good to focus on the most widely spoken languages first. So

- Mandarin
- Hindi
- Spanish
- French
- Arabic
- Bengali
- Russian
- Portuguese
- Indonesian

31.1.2 Data Dynamism

I'd like an easy way to embed live data in every version publish. So for example if I want to reference the current ETH price, I should be able to do something like {{eth.current_price}} and it will embed the current price during the Quarto render with the latest price.

References

Monegro, Joel. 2016. "Fat Protocols." Union Square Ventures. https://www.usv.com/writing/2016/08/fat-protocols/.