Brave New Crypto

A handbook for future society builders

Prashanth Irudayaraj

Disclaimer

The information presented in this book is for educational and informational purposes only. It should not be considered as financial advice, investment guidance, or a recommendation for any specific financial action. The content provided reflects the author's views and experiences, and while it is intended to inform and provoke thought, it is not tailored to the specific circumstances of any individual or entity.

Before making any financial decisions, it is essential to conduct your own research and consult with a qualified financial advisor or other professional who can provide advice tailored to your particular situation. The author and publisher assume no responsibility or liability for any financial outcomes or decisions made based on the information contained in this book.

Contents

Preface

Cryptocurrency today is akin to the Wild West—a vast and chaotic landscape filled with rapid innovation, bold experiments, and unfortunately, numerous scams. It's a world of high risk and high reward, where new technologies are forged, tested, and, at times, broken. However, if you look closely, beyond the noise and hype, you will see the seeds of future society builders being planted. The chaos of today is paving the way for the foundations of tomorrow's world.

Many of the crypto experiments we see today will fail, and that is a natural part of any significant technological shift. But even in failure, there are lessons to be learned and tools to be refined. Each step forward, and even each misstep, is part of a broader narrative of innovation—one that has the potential to reshape our society's future. Through this constant process of trial and error, we are gradually crafting new systems of governance, finance, and community, all driven by the promise of decentralization and self-sovereignty.

"Brave New Crypto" is my beacon of hope in this evolving world, brimming with both potential and pitfalls. This book is not just a collection of thoughts on cryptocurrency; it is a journey and a mission to explore the promising yet uncharted waters of this new era. It aims to equip you with the knowledge, principles, and tools needed to navigate this terrain and thrive.

Despite the perception that the crypto world is dominated by men, I see an unparalleled opportunity for

women to step in and redefine the landscape. The decentralized nature of blockchain technology opens the door to new forms of financial independence and power. This book is my rallying cry to women everywhere: let's harness the transformative power of cryptocurrency to redraw the boundaries of our world and redefine what's possible.

"Brave New Crypto" is not just for reading—it's a call to arms. It echoes the cautionary tale of *"Brave New World"* by Aldous Huxley but with a twist of optimism. Rather than succumbing to a dystopian vision, my aim is to guide us toward a future as hopeful and inclusive as the society depicted in *Star Trek*, where technology serves as a force to uplift and unite us all.

This book is not about Bitcoin, Ethereum, or any specific cryptocurrency. Instead, it's about understanding the broader implications of these technologies and using them as a foundation to build new societal structures. It's an invitation to roll up our sleeves and build a world where trust is a given, not a luxury—where decentralized systems make fairness and accessibility the default rather than the exception. Together, we can shape a future that exceeds our wildest dreams.

This is a call to action for all builders, thinkers, and dreamers—women, men, anyone willing to step forward. Let's construct a better future for all!

My Journey into Crypto

My entry into the world of cryptocurrency was unexpected and far from planned. At the time, I was

deeply involved in humanitarian research projects in Haiti as part of my work at Georgia Tech. Our team was driven by a mission to tackle food insecurity by empowering women to launch agricultural businesses using innovative techniques. We believed that equipping these women with the right knowledge and tools could spark meaningful and sustainable change.

As we immersed ourselves in these projects, however, we uncovered a more profound and systemic challenge that had little to do with agricultural methods and everything to do with finance. The women we worked with were unable to save money securely, nor could they transact safely within their communities or beyond. The lack of a basic, reliable financial infrastructure was holding them back far more than any lack of agricultural knowledge or skills.

This realization was a pivotal moment. We had set out to solve a problem of food insecurity, but we soon recognized that the crux of the issue was financial exclusion. Determined to find a solution, we turned to technology—specifically, blockchain technology and cryptocurrencies.

In response to this challenge, we built a prototype of a simple financial savings and transaction system on Ethereum. Given the limited access to technology in the region, we designed the system to work on basic feature phones, rather than smartphones. This approach allowed us to create a platform where women could safely save, send, and receive money without relying on traditional banking systems, which were often inaccessible or untrustworthy.

The experience was a revelation. What began as a modest attempt to address a local financial issue revealed the broader potential of decentralized finance. I witnessed firsthand how blockchain technology could empower those left behind by conventional systems, providing them with the tools and autonomy to manage their own financial lives. This was the spark that ignited my passion for crypto—a passion rooted not in speculation or hype but in a genuine belief in its capacity for global social good.

This early experiment in Haiti was just the beginning. It planted a seed that has since grown into a deeper exploration of how blockchain and cryptocurrency can be leveraged to create inclusive systems that serve everyone. I came to see crypto as a transformative tool—one that could redefine not just finance, but the very fabric of society. By offering new frameworks for fairness, transparency, and accessibility, crypto has the potential to empower individuals and communities in ways that were previously unimaginable.

Today, my journey in crypto continues with the same vision: to use this technology to build systems that work for everyone. By building on these foundational ideas, I believe we can create a future where trust is democratized and opportunities are accessible to all. This is not just a technical revolution; it's a social one, and I invite you to join me in building it.

Part 1: Why Should I care?

1. Trust

I trust you to be great!

Every single human being on this planet can be great. That is if you are willing to bear the cost of trust.

Trust is something we often take for granted until it's broken or betrayed. Yet, trust is the foundation of human cooperation. It's what holds together families, businesses, and even enables monumental achievements like space exploration[1]. Without trust, these connections would crumble, and our collective efforts would fall apart [2].

Cryptocurrency and the Cost of Trust

Cryptocurrency is on the verge of revolutionizing the very essence of trust. By significantly lowering the cost of trust, cryptocurrencies have the potential to elevate global collaboration to new heights. This isn't just about improving existing relationships; it's about creating new

---

[1] Logsdon, John M. "International Cooperation in the Space Station Programme." *Space Policy*, vol. 7, no. 1, Feb. 1991, pp. 35–45, doi:10.1016/0265-9646(91)90044-I.

[2] Putnam, R. *Bowling Alone: The Collapse and Revival of American Community*. ACM Press, 2000, p. 357, doi:10.1145/358916.361990.

ones and enabling interactions between humans and machines in ways that were previously impossible. Traditionally, global trust at scale has been mediated by third parties—like banks or governments—but cryptocurrencies are changing this dynamic by enabling trust directly between individuals [3] [4].

As we begin this journey into the world of cryptocurrencies, we're not just exploring a new form of money. We're stepping into a new era of trust. This new infrastructure will reveal innovative ways to connect, collaborate, and create, all based on a foundation of trust that was unimaginable before the advent of blockchain technology. This chapter is the start of that exploration, guiding you through the importance of trust, both in our past and in our future, and why understanding its cost is essential as we move into the cryptocurrency age.

Your Role as a Future Society Builder

As a future society builder, you are more than just a participant in this emerging landscape—you are an explorer setting out on a journey into uncharted territory. The world of cryptocurrencies and decentralized technologies is vast and full of potential, much like a

---

[3] Swan, Melanie. *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015.

[4] Mougayar, William. *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons, 2016.

new frontier waiting to be discovered [5]. Your role isn't merely to learn how to use the existing trust infrastructure but to push the boundaries, to explore new possibilities that extend beyond what we can currently envision [6].

Think of yourself as a pioneer, venturing into a new era where the rules are still being written, and the map is only partially drawn. You are at the forefront of shaping a society where trust is redefined—no longer solely mediated by traditional institutions, but distributed, transparent, and more accessible to all.

This journey is not just about understanding how blockchain works or how cryptocurrencies function. It's about questioning the fundamental assumptions of how we interact, collaborate, and build communities. As an explorer, you will chart new paths, creating innovative ways to connect people, fostering collaboration on a global scale, and enabling the creation of value in ways that were previously unimaginable.

Your exploration will require curiosity, creativity, and a willingness to embrace uncertainty. The possibilities are endless, and the impact you can make is profound. As you navigate this new landscape, you will be laying the groundwork for future generations, building the

––––––––––––––––––––––––––

[5] Vigna, Paul, and Michael J. Casey. *Cryptocurrency: how Bitcoin and digital money are challenging the global economic order*. Bodley Head, 2015.
[6] Bashir, Imran. "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications." (2017).

foundations of a society that is more equitable, more inclusive, and more resilient.

So, as you begin this journey, remember that the future is not something that just happens—it is something we create. And your role as a future society builder is to be at the helm of this creation, leading the way into a new world of trust, innovation, and opportunity.

The Cost of Trust

Trust is as essential and pervasive as the air we breathe, yet it's just as difficult to measure. It's like trying to put a price on oxygen—critical but often taken for granted until it's gone. Despite these challenges, researchers have attempted to quantify trust's tangible impact. A 2018 pilot study by Davidson suggests that trust may account for at least 35% of employment in the U.S. alone, highlighting its significant economic value [7]. The perception of trust varies widely around the world. The World Value Survey shows that in countries like Norway and Sweden, over 60% of people believe that "most people can be trusted." In contrast, in nations like Colombia, Brazil, Ecuador, and Peru, less than 10% of people share that belief [8]. In places with low trust, the cost of trust would likely be high, making it more expensive and harder to achieve.

When trust is expensive, the consequences can be severe, potentially hindering societal progress. A study titled "Trust and Economic Growth: A Robustness Analysis" finds a positive correlation between trust and economic growth, even when accounting for education, politics, and income inequality [9]. This shows that the cost of trust isn't just financial; it's a critical factor in a

---

[7] Davidson, Sinclair, et al. "The Cost of Trust: A Pilot Study." *The Journal of the British Blockchain Association*, vol. 1, no. 2, Dec. 2018, pp. 1–7, doi:10.31585/jbba-1-2-(5)2018.
[8] Ortiz-Ospina, Esteban, Max Roser, and Pablo Arriagada. "Trust." *Our World in Data*, 2016, https://ourworldindata.org/trust. Accessed 12 Aug. 2024
[9] Zak, Paul J., and Stephen Knack. "Trust and growth." *The economic journal* 111.470 (2001): 295-321.

society's overall health and success. Societies where mistrust is high face greater obstacles to prosperity. Therefore, creating an environment where trust is abundant and low-cost is crucial for societal well-being.

What Does Low-Cost Trust Look Like?

Low-cost trust is trust that doesn't require significant investment in time, mental energy, or resources. Money, in a way, represents low-cost trust. When you accept $100 USD or ₹100 INR, you trust that it holds that value because it's backed by the government. This system allows you to rely on society's trust in the government rather than having to establish trust yourself during each transaction. However, this borrowed trust has a cost, and we pay for it in various ways.

The Violent Cost of Trust

A historical example of the high cost of misplaced trust is Adolf Hitler's rise to power. During severe economic hardship, many Germans placed their trust in his promises, leading to the horrors of World War II, the loss of countless lives, and widespread destruction across Europe [10].

This example underscores a critical point: power can corrupt, and absolute power corrupts absolutely. In today's world, we still see cases where large groups trust small, often corrupt leaders, leading to violent conflicts with devastating outcomes.

—————————————————

[10] Kershaw, Ian. *Hitler: A biography*. WW Norton & Company, 2010.

Yet, trust in leadership is also crucial for societal stability and can lead to peace and prosperity. It's important for global citizens to constantly evaluate when the cost of trust becomes too high and to explore alternatives that might offer similar benefits at a lower cost.

Cryptocurrency presents one such alternative. With its decentralized structure, crypto reduces the need to trust centralized authorities or small groups. Instead, it uses built-in financial incentives to create trust without violence. The foundational principles of cryptocurrency offer a promising way to build and maintain trust on a global scale without the high costs often associated with violence or corruption [11].

Trust in Government

Governments play a vital role in ensuring the smooth functioning of society by reducing transaction costs for their citizens. But what are transaction costs? These are the hurdles or expenses involved in making an interaction or exchange between people successful.

For instance, consider a routine trip to a store in Mumbai. The security provided by police enforcement, a function of the government, assures you that it's highly unlikely you'll face an attack on your way. This sense of safety stems from the government's ability to enforce laws and maintain order. Similarly, when you buy biscuits from a store, your confidence in the

---

[11] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

transaction—exchanging money for safe, consumable goods—is reinforced by regulations from bodies like the Food Safety and Standards Authority of India (FSSAI), which ensures the products you purchase are safe[12].

The importance of government becomes even more apparent in situations where it fails, such as in the chaotic settings depicted in war movies like "Saving Private Ryan" or "1947 Earth." These films, set during times of conflict or the partition of India, illustrate the dangers and uncertainty that arise when governmental structures collapse. Without government-provided safety and standards, individuals must expend significant energy on ensuring their own security and well-being. This often limits their activities to essential tasks and involves taking considerable risks with something as basic as food safety.

This example highlights not just the necessity of government but the immense value of its services. Without these, daily life would be filled with uncertainty and danger. The government, through its various functions, effectively reduces the energy, time, and resources individuals must otherwise spend to secure basic safety and ensure the integrity of their daily transactions.

---

[12] Owens, Emily, and Bocar Ba. "The Economics of Policing and Public Safety." *Journal of Economic Perspectives*, vol. 35, no. 4, Nov. 2021, pp. 3–28, doi:10.1257/jep.35.4.3.
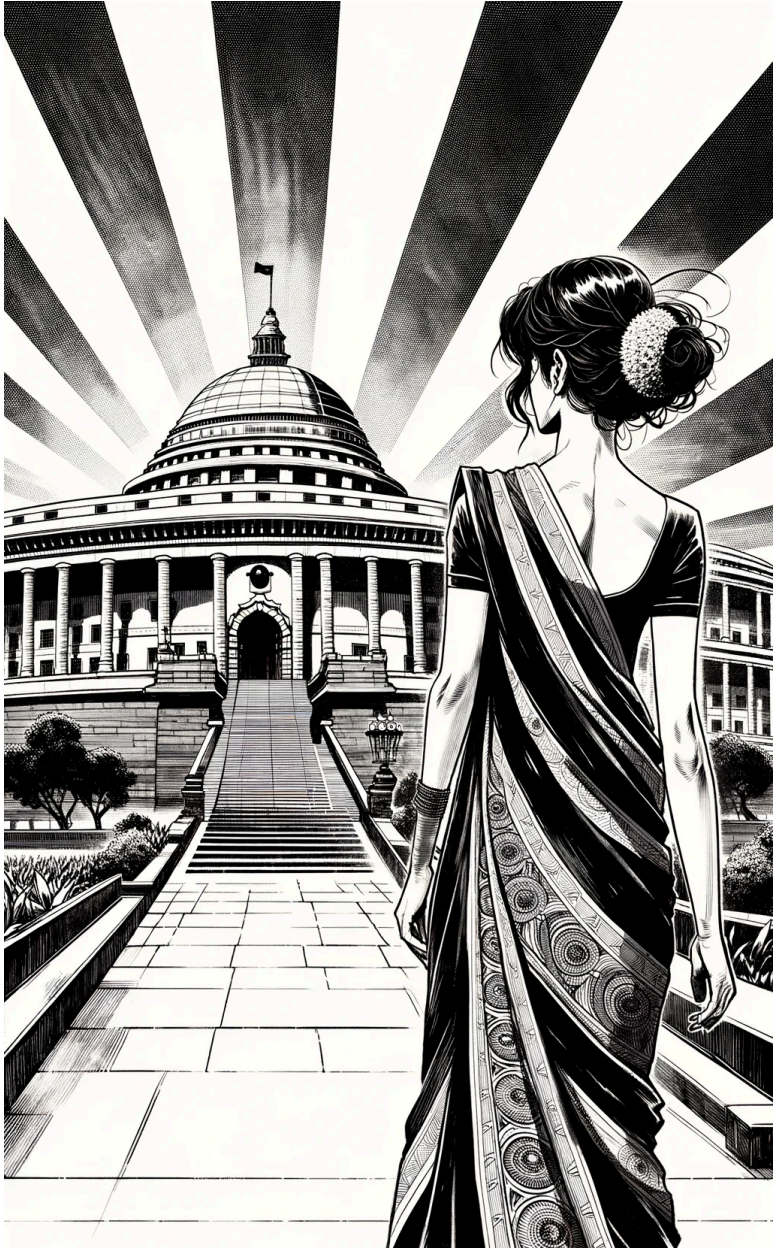
We pay for the trust that the government provides through taxes, which is obvious to everyone. But there are other costs that aren't always apparent. For example, the government issues currency, and the amount of currency in circulation can influence inflation. Inflation directly reduces the value of savings because ₹100 today buys less than it did a year ago. This decrease in purchasing power is a hidden cost that we all bear [13].

Additionally, governments often favor certain entities or initiatives, ideally for the greater good. However, this is not always the case. When governments prioritize their own survival or the interests of a select few over the needs of the people, it's the citizens who pay the price. The movie Don't Look Up [14], a satire about a government that prioritizes the interests of a wealthy tech giant over saving the planet, illustrates this bias effectively. Similarly, the films Mudhalvan and Nayak poetically depict the costs of corruption on the Indian population [15].

This is a significant cost that people around the world have been paying for generations. Monarchies, the oldest form of government, often imposed high costs on citizens, benefiting only a small elite over many

_____

[13] *Money and Inflation: A Functional Relationship - Page One Economics® - St. Louis Fed*. https://research.stlouisfed.org/publications/page1-econ/2013/03/01/money-and-inflation-a-functional-relationship/. Accessed 12 Aug. 2024.
[14] McKay, Adam. Don't Look Up. Netflix, 2021.

[15] Shankar, S. Mudhalvan. Sri Surya Movies, 1999.

generations. The invention of the printing press reduced the cost of changing governments, giving people more freedom in choosing their leaders[16]. This technological shift enabled the rise of democracies, which marginally reduced the cost of government. The industrial revolution, the internet, and advancements in automation and information technology have further streamlined government services, lowering these costs even more [17].

Now, blockchain and decentralized systems promise to reduce the cost of trust in government even further. In many ways, cryptocurrency is the modern equivalent of the printing press, and government-issued currencies are like the monarchies of old—a system most people believe is unchangeable. However, crypto is proving that change is possible, potentially leading to new and improved methods of value transfer that are hard to envision today. Just as peasants 1,000 years ago could not have imagined democracy, we are now beginning to see how money and currency might evolve in ways we never thought possible [18] [19].

———————————————————

[16] Eisenstein, Elizabeth L. *The printing revolution in early modern Europe*. Cambridge University Press, 2005.
[17] Fukuyama, Francis. *Political order and political decay: From the industrial revolution to the globalization of democracy*. Macmillan, 2014.

[18] Tapscott, Don, and Alex Tapscott. Blockchain revolution: how the technology behind bitcoin is changing money, business, and *the* world. Penguin, 2016.
[19] Narayanan, Arvind, et al. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.

In future chapters, we will explore how this new trust infrastructure can help rewrite the rules of society and create innovative governance models. This time, women can take the lead, designing systems that could be far better than those created primarily by the men of the past.

Trust in Financial Firms

For the past 100-200 years, finance has been the domain with the largest profits[20]. This is because it sits at the intersection of transactions between people and provides—yes, you guessed it—trust! We primarily pay banks to be the trusted middlemen who manage our financial assets and ensure that transactions happen as expected. We also trust that investment banks will allocate resources and capital in ways that benefit the broader economy. However, the financial crisis of 2008 exposed the reality that this trust was often misplaced.

In 2008, it became clear that many financial firms were engaged in fraudulent behavior driven by greed, ultimately leading to the collapse of the global financial system. The book and movie The Big Short [21] and Margin Call [22] offer insightful looks into the skewed incentives and the misuse of public trust that resulted in widespread suffering around the world.

In India, the cost of trust in banks is also painfully evident. The Punjab and Maharashtra Co-operative (PMC) Bank scandal is a well-documented case of the misuse of public trust, where the bank's fraudulent activities led to significant financial losses for

---

[20] *Why Did the Financial Sector Get So Big? Ask Your Adviser | Chicago Booth Review*. https://www.chicagobooth.edu/review/why-did-the-financial-sector-get-so-big-ask-your-adviser. Accessed 13 Aug. 2024.
[21] Lewis, Michael. *The Big Short: Inside the Doomsday Machine*. W.W. Norton & Company, 2010.
[22] Chandor, J.C. Margin Call. Lionsgate, 2011.

depositors[23]. Moreover, the outsized influence of Wall Street on the Indian economy raises questions about global financial fairness. Should a city of a few million on the other side of the planet hold so much sway over the lives of 1.5 billion Indians? Many would argue that it shouldn't be the case, and even most Americans might agree[24].

As we continue to explore how trust is being reshaped by technology, we will see how blockchain and decentralized systems can offer alternatives to the traditional financial institutions that have long dominated the landscape.

––––––––––––––––––––––––

[23] Gupta, Ambuj. "The devil's laugh at corporate governance: The case of Punjab and Maharashtra Co-operative Bank (PMC Bank) India." Indian Journal of Corporate Governance 14.2 (2021): 248-267.
[24] Johnson, Simon, and James Kwak. 13 bankers: The Wall Street takeover and the next financial meltdown. Vintage, 2011.
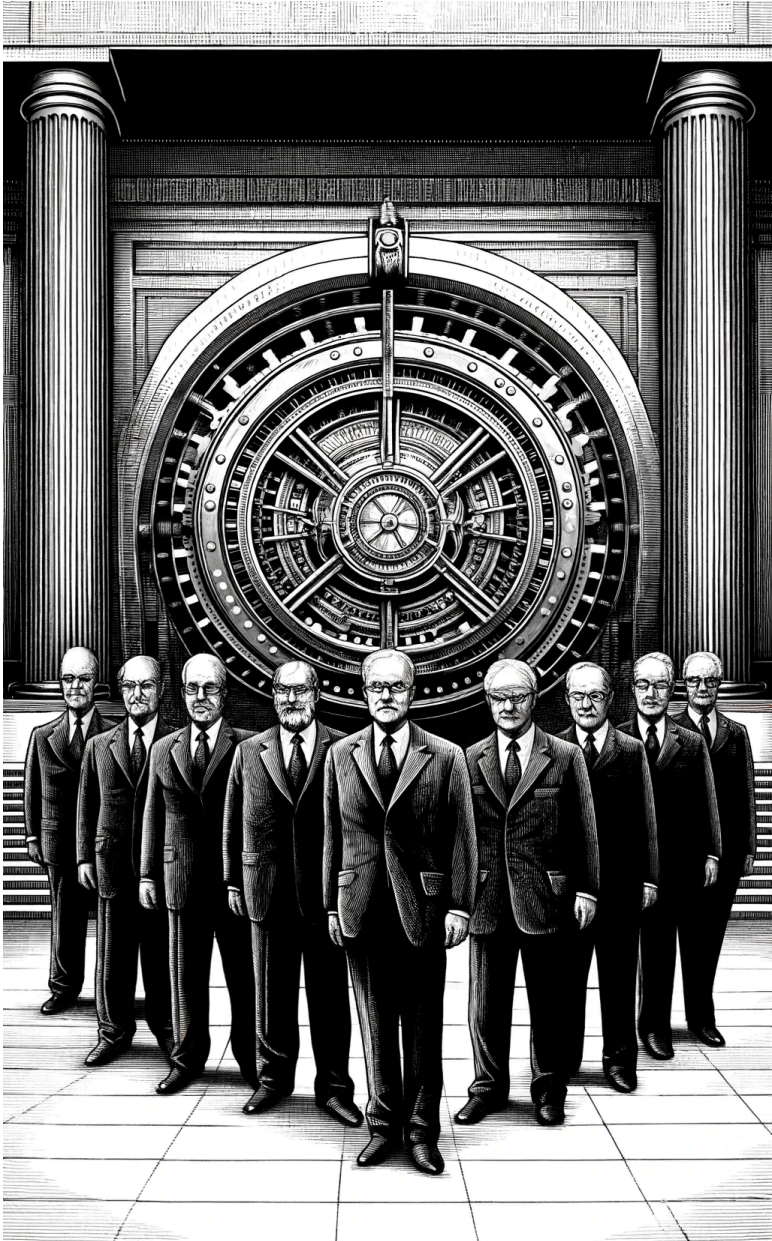
Trust in Technology

Our trust in technology might seem easier to value at first glance. For example, the value of our trust in social networks could be estimated by the market value of Meta, which at the publication of this book is over $1 Trillion[25]. This massive valuation reflects the trust we place in a single company whose primary business is to store and manage social information. The valuation of the tech industry as a whole is much much larger.

However, the full cost of this trust isn't always obvious. Even though these numbers are immense, the total cost might be even higher. As tech giants have grown rapidly, their domination of the internet-driven economy has become global, exerting significant pressure on new entrants. The original goal of the internet was to be free, open, and egalitarian. But because the internet is global and anonymous, we have come to place our trust in these big tech giants, simply because there are no viable alternatives[26].

Ironically, while cryptocurrency has often been associated with the dark web and nefarious activities, it may be the innovation that brings true equality to the internet. By reducing the need to trust a few dominant tech companies, crypto could democratize the online

---

[25] *Meta Platforms Market Cap Trends | YCharts*. https://ycharts.com/companies/META/market_cap. Accessed 13 Aug. 2024.
[26] Wu, Tim. *The Master Switch: The Rise and Fall of Information Empires*. Illustrated, Reprint, Alfred A. Knopf, 2010.

world. Innovations often emerge from unexpected places, and crypto might just be the key to making the internet more open and less reliant on centralized tech giants[27]. Innovations often come from strange places[28][29].

_____

[27] Tapscott, Don, and Alex Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin Publishing Group, 2016.
[28] Roberts, Royston M. *Serendipity: Accidental discoveries in science*. 1989.
[29] Simonton, Dean Keith. *Creativity in science: Chance, logic, genius, and zeitgeist*. Cambridge University Press, 2004.

Innovation needs Trust

Innovation inherently requires trust. By definition, innovations break new ground, and for them to succeed, they need the trust of many people. Having been part of the startup ecosystem for more than 20 years, I've seen firsthand how the vast majority of companies spend most of their time pitching and convincing investors and customers that their offerings can be trusted. In the innovation economy, trust is expensive[30].

---

[30] *Connecting Trust and Economic Growth | Deloitte Insights*. https://www2.deloitte.com/us/en/insights/economy/connecting -trust-and-economic-growth.html. Accessed 14 Aug. 2024.

This is an area where cryptocurrency has already demonstrated its potential. The Initial Coin Offering (ICO) boom of 2017-2018 saw a surge in companies being funded, many of which were unfortunately scams. However, it also proved that ICOs are a viable method for global fundraising[31], particularly for digital projects that can be used and owned globally[32]. These companies could pitch directly to a global audience, and investors could contribute as little as 50 cents or 10 rupees. In return, investors received a stake in the digital project, a right to use the product, participate in the product ecosystem, governance rights, or a combination of these.

ICOs showed that crowdsourcing could fund multi-million-dollar projects serving a global customer base. This opens up possibilities for funding global-scale research on issues like climate change, governance, poverty, and energy. But all of this is only possible because people trust that their funds will reach the right place and that they will see a return on their investment.

_____

[31] Fisch, Christian. "Initial Coin Offerings (ICOs) to Finance New Ventures." *Journal of Business Venturing*, vol. 34, no. 1, Jan. 2019, pp. 1–22, doi:10.1016/j.jbusvent.2018.09.007.
[32] Howell, Sabrina, et al. "Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales." *SSRN Electronic Journal*, 2018, doi:10.2139/ssrn.3201259.

The importance of trust in innovation[33] is well illustrated in the movie *Race the Sun*, where a scrappy underdog Hawaiian team defies the odds to enter the World Solar Challenge in Australia. While it's not a critically acclaimed film, it's one of my favorites because it shows a group of people deemed "least likely to succeed" overcoming entrenched hierarchies. These hierarchies, representing established wealth and privilege, consistently doubt the underdogs' ability to succeed. Imagine if this team could have conducted an ICO to raise funds for their race and create a solar vehicle startup? It would have allowed them to bypass traditional barriers and directly gain the trust and support of a global community[34].

Cypherpunks, Innovation, Freedom and the Cost of Trust

Throughout history, individual freedom has consistently been under threat, and this remains true today. The quest for freedom has always intertwined with the evolution of technology, as each new tool offers a way to shift the balance of power, often reducing the cost of trust and coordination among large groups of people.

---

[33] Steinbruch, Fernanda Kalil, et al. "The Role of Trust in Innovation Ecosystems." *Journal of Business & Industrial Marketing*, vol. 37, no. 1, Jan. 2022, pp. 195–208, doi:10.1108/JBIM-08-2020-0395.

[34] Turkina, Ekaterina, and Ari Van Assche. "Global Connectedness and Local Innovation in Industrial Clusters." *Journal of International Business Studies*, vol. 49, no. 6, Aug. 2018, pp. 706–28, doi:10.1057/s41267-018-0153-9.

As we've discussed, **trust is expensive** in both the innovation economy and traditional systems. Innovators need trust to gain support, secure funding, and bring their ideas to life. However, as we work to reduce the cost of trust—through technologies like blockchain and cryptography—we must be cautious. Lowering the cost of trust can sometimes inadvertently diminish freedom, especially if it consolidates power in fewer hands or reduces the diversity of voices[35] [36].

This is where the cypherpunks' philosophy becomes particularly relevant[37]. While cypherpunks fought for freedom, they did so by using math—in the form of cryptography—to keep the cost of trust low[38]. Cryptography allows for secure, private communications and transactions without relying on centralized authorities that could misuse or control information. Crypto is based on cryptographic technologies which offer a path to increasing freedom while simultaneously lowering the cost of trust .

_____

[35] Cicchiello, Aimee, and Lovisa Gustafsson. "Federal Antitrust Tools Are Inadequate to Prevent Anticompetitive Health Care Consolidation." *Commonwealth Fund*, 2021, doi:10.26099/qd0h-f852.
[36] *Trust and Diversity: Not a Bang But a Whimper - Econlib*. https://www.econlib.org/archives/2017/06/trust_and_diver.html . Accessed 14 Aug. 2024.
[37] Levy, Steven. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*. Reprint, Viking, 2001.
[38] *A Cypherpunk's Manifesto | Satoshi Nakamoto Institute*. https://nakamotoinstitute.org/library/cypherpunk-manifesto/. Accessed 14 Aug. 2024.

Mahatma Gandhi provides a historical parallel to how technology can amplify the fight for freedom. He skillfully used the emerging technologies of his time—newspapers, radio, and other forms of mass media—to spread his message quickly and efficiently. This not only rallied people within India to the cause of independence but also garnered significant international support. The technology of the era helped reduce the 'trust gap' by allowing Gandhi to communicate directly and broadly, confirming his integrity and the righteousness of his cause to a wide audience .

Similarly, today's freedom fighters harness modern technologies. By using cryptography, cypherpunks have shown that it is possible to protect individual freedom while reducing the need for trust in traditional systems. Cryptography, at its core, minimizes the need for trust in potentially untrustworthy systems, replacing it with mathematical certainty[39].

The use of decentralized technologies like blockchain and cryptography introduces a new paradigm. These systems allow for secure interactions without the need for centralized intermediaries, ensuring that the cost of trust remains low while protecting individual freedoms. In doing so, they provide a means to avoid the potential downsides of a "Brave New World" scenario, where reducing the cost of trust could lead to a loss of freedom[40].

---

[39] Sarkar, Sumit. *Modern India 1885–1947*. Palgrave Macmillan UK, 1989, doi:10.1007/978-1-349-19712-5.
[40] Narayanan, Arvind, et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

As we continue to navigate the complexities of modern governance and societal organization, the principles championed by the cypherpunks remain central: trust should be placed not in entities or individuals who may abuse it, but in systems designed to safeguard it through transparency and robustness. This shift not only supports the cause of individual freedoms but also protects them in an increasingly interconnected world, while fostering innovation[41].

---

[41] Tapscott, Don, and Alex Tapscott. Blockchain revolution: how the technology behind bitcoin is changing money, business, and *the* world. Penguin, 2016.
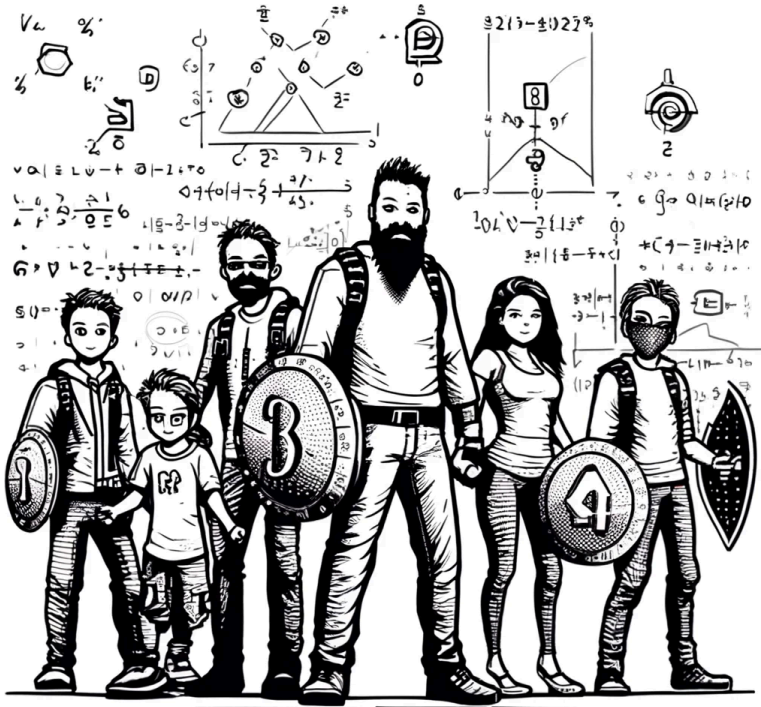
2. The 3rd age of the internet

It was foretold that the internet would be free, open, and permissionless…

But it took several battles to begin the freedom journey, and it's a battle we have to keep fighting!!

"The aim would be to allow a place to be found for any information or reference which one felt was important, and a way of finding it afterwards. The result should be sufficiently attractive to use that the information contained would grow past a critical threshold, so that the usefulness of the scheme would in turn encourage its increased use."[42]

---

[42] Berners-Lee, Tim. (1989). "Information Management: A Proposal." CERN.

As we embark on the next phase of digital evolution, understanding the transformative journey of the internet is not just about reflecting on the past—it's about shaping the future. The internet has evolved through three distinct ages, each fundamentally altering how we interact, conduct business, and trust one another online.

In its early days, the internet served as a tool for sharing information among a small, close-knit community. Trust was implicit, built on mutual respect and shared goals. As the internet expanded, it became a platform for user-generated content and global commerce, but this growth also brought new challenges. Centralized power began to erode the openness that once defined the internet, turning trust into a commodity controlled by a few dominant players[43].

Today, we stand on the brink of a new era—an age where trust is no longer concentrated but distributed across a global network. This third age, driven by blockchain technology, promises to fulfill the internet's original vision of being free, open, and permissionless[44]. However, this vision is not guaranteed; it requires our active participation and vigilance.

---

[43] Zittrain, Jonathan. *The future of the internet: and how to stop it*. Penguin UK, 2009.

[44] Tapscott, Don, and Alex Tapscott. Blockchain revolution: how the technology behind bitcoin is changing money, business, and *the* world. Penguin, 2016.

Your Role as a Future Society Builder

As a future society builder, your role in this new era is more critical than ever. The internet's evolution has shown us that trust, once an implicit foundation, must now be carefully designed and maintained. The lessons from the past inform us that the cost of trust can either empower innovation or stifle it, depending on how it is managed[45].

You are not just a passive observer of this transformation—you are an active participant and creator. Your task is to harness the potential of decentralized technologies to build platforms and systems that embed trust at their core. This means designing solutions that are resilient, inclusive, and capable of standing the test of time.

The open-source community exemplifies the spirit of this new era. For decades, open-source projects have demonstrated how decentralized collaboration can create powerful, trustworthy software without the need for centralized control[46]. The success of open-source software like Linux, which powers everything from servers to smartphones, shows that trust can be built and maintained through transparency, community

---

[45] Fukuyama, Francis. *Trust: The social virtues and the creation of prosperity*. Simon and Schuster, 1996.

[46] Morgan, Eric Lease. "The cathedral & the bazaar: musings on linux and open source by an accidental revolutionary." *Information Technology and Libraries* 19.2 (2000): 105.

involvement, and shared responsibility[47]. As a future society builder, you can draw inspiration from the open-source model to create new systems where trust is a collective endeavor rather than a centralized commodity.

Imagine the internet as a vast, evolving ecosystem. Your role is to nurture its growth, ensuring that it remains free, open, and accessible to all. This involves not only creating new technologies but also advocating for the principles of decentralization and transparency that underpin the third age of the internet[48]. Your efforts will help shape a digital future where trust is distributed, empowering individuals rather than concentrating power in the hands of a few.

As we delve deeper into each of the internet's ages in the following sections, remember that the future is not something that happens to us—it's something we create. Your work as a future society builder will determine how the third age of the internet unfolds, and whether it truly fulfills its promise of being free, open, and permissionless.

---

[47] Weber, Steven. *The success of open source*. Harvard University Press, 2004.
[48] Lessig, Lawrence. *Code: And other laws of cyberspace*. ReadHowYouWant. com, 2009.

The First Age - Read Only

The journey through the ages of the internet begins with the "Read-Only" era, marking the first step toward a globally connected world. This pre-2000s period was characterized by the advent of static web pages, where users primarily consumed information with little ability to interact or contribute.

The "Read-Only" internet was propelled by key technological advancements such as the development of web browsers and the introduction of HTML (Hypertext Markup Language), which enabled the creation of simple websites accessible to anyone with an internet connection. The launch of the World Wide Web by Tim Berners-Lee in 1991 was particularly transformative, laying the groundwork for what would become a vast, interconnected network of information.

During this era, the internet served as a digital library of sorts, where users could search for and read information from servers around the world. However, their role was largely passive; interaction with content was minimal, and user-generated content was virtually nonexistent. The control over what was published and available to the public rested primarily with content creators and website administrators, who acted as the gatekeepers of information. In this context, trust was inherently placed in these entities, as users had few tools to verify the accuracy or reliability of the content they consumed.

While the "Read-Only" era opened up unprecedented access to information, it also highlighted the limitations of a static, one-way flow of data. This lack of interactivity

and user engagement underscored the need for a more dynamic and participatory web, setting the stage for the next evolution—the "Read-Write" era, where users could not only consume content but also create and share it.

For future society builders, understanding the "Read-Only" age is crucial. This era laid the foundational structures of the internet but also exposed the vulnerabilities of a system where trust was concentrated in the hands of a few. As we move forward into the third age of the internet, the lessons from this period remind us of the importance of designing systems where trust is not only distributed but also verifiable. It challenges us to think beyond passive consumption and toward active participation in the creation of a digital future that is free, open, and permissionless.

The Fight for Freedom Begins

Even in the early days of the internet, the battle for freedom and trust was already underway. As the "Read-Only" era unfolded, it became clear that the internet's promise of open access to information was not without its challenges. One of the most significant early battles was centered around the right to privacy and the use of encryption, a tool critical for securing digital communications and ensuring trust in the emerging online world.

At the heart of this battle was RSA encryption, an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA quickly became one of the most widely used methods for securing sensitive data online. However, the U.S. government categorized RSA and other encryption technologies as munitions, placing them under strict export controls. This classification meant that sharing encryption technology outside the United States was akin to exporting weapons, severely limiting the global use of tools that could secure digital communication and protect privacy.

This classification posed a significant threat to the idea of a free and open internet. Encryption was essential not just for protecting sensitive information but for enabling trust in online interactions. Without the ability to securely exchange data, the internet's potential as a platform for commerce, communication, and collaboration would be severely compromised.

In response to these restrictions, a grassroots movement emerged, advocating for the right to use and share encryption technology freely. One of the most iconic acts of defiance came in the form of a simple yet powerful gesture: printing the RSA algorithm on T-shirts. By wearing these T-shirts, activists symbolically challenged the government's control over encryption technology, arguing that mathematical formulas should not be restricted like weapons. This creative form of protest highlighted the absurdity of the restrictions and underscored the importance of encryption in ensuring privacy and trust on the internet.

The fight to freely use encryption was a critical early battle in the broader struggle for digital freedom. It set the stage for future conflicts over privacy, surveillance, and the right to secure communication, all of which would become increasingly important as the internet evolved. The victory in this battle allowed encryption to flourish, becoming a fundamental component of the internet as we know it today.

For future society builders, the story of RSA and the fight for encryption freedom serves as a powerful reminder of the ongoing struggle to ensure that the internet remains a place of trust, privacy, and freedom. As we move into the third age of the internet, the lessons from this early era remind us that the freedoms we enjoy online are hard-won and must be continually defended. The fight for a free, open, and permissionless internet began in the "Read-Only" age, and it continues today, with the same spirit of innovation, resistance, and determination.
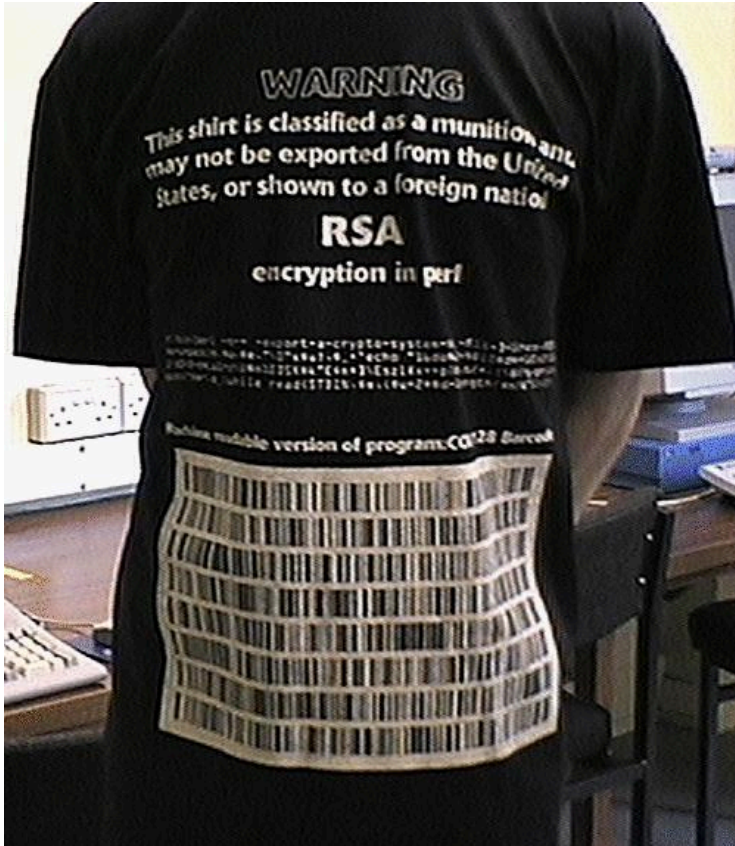
Source: Wikimedia commons[49] - Used under Creative Commons
CC0 1.0 Universal Public Domain Dedication

---

[49] *File:Munitions T-Shirt (Front).Jpg - Wikimedia Commons*. https://commons.wikimedia.org/wiki/File:Munitions_T-shirt_(front).jpg. Accessed 15 Aug. 2024.

The Second Age - Read, Write, and Socialize

As the internet evolved, it entered the "Read-Write" era, a period marked by a profound transformation in how users interacted with the digital world. This age, spanning from the mid-2000s to the early 2010s, saw the internet shift from a static repository of information to a dynamic, interactive platform where users not only consumed content but also created and shared it. The rise of blogs, forums, and social media platforms democratized content creation, empowering individuals to contribute their voices to the global conversation.

However, with this newfound power came new challenges. The internet was no longer a space solely controlled by a few gatekeepers; it had become a vast, decentralized network where anyone could publish information. This shift significantly altered the landscape of trust online. Users were now faced with the task of discerning the reliability of not just official sources, but also the content generated by their peers.

In this era, trust became more complex and multifaceted. It was no longer enough to trust a website or an institution; users had to navigate an ocean of user-generated content, much of which could be biased, misleading, or outright false. The cost of trust increased as the burden of verification shifted to the individual. The rise of misinformation and the challenges of verifying authenticity highlighted the vulnerabilities of a decentralized content ecosystem.

For future society builders, the "Read-Write" era offers critical lessons. It demonstrates how the decentralization of content creation can both empower individuals and introduce new risks to the trust infrastructure. As we move into the third age of the internet, these lessons remind us of the importance of designing systems that not only facilitate participation but also ensure that trust is maintained at a low cost. This means creating mechanisms for verification, fostering transparency, and promoting digital literacy, so that the power of decentralized content creation can be harnessed without compromising the integrity of the information ecosystem.

The "Read-Write" era set the stage for a more participatory internet, but it also underscored the challenges of maintaining trust in a decentralized world. As a future society builder, your role is to take these lessons forward, designing the next generation of platforms and systems where trust is not an afterthought but a foundational principle. In the third age of the internet, trust must be more accessible, more verifiable, and more resilient, enabling a digital future that is both free and trustworthy.

The Fight for Internet Freedom in the Second Age

The "Read-Write" era of the internet was not only marked by an explosion of user-generated content and social interactivity but also by a critical battle for internet freedom. As the internet became more central to daily life, the stakes surrounding its control and regulation grew higher. The debates and policies that emerged during this period in the United States, in particular, played a significant role in shaping the future of the internet as a free and open platform.

One of the central issues during this era was the concept of "net neutrality." Net neutrality is the principle that all internet traffic should be treated equally, without discrimination or favoritism by internet service providers (ISPs). In practical terms, it means that ISPs should not be allowed to prioritize certain websites or services over others, nor should they be allowed to throttle or block access to particular content. This principle was seen as essential for maintaining a level playing field online, where users could access and share information freely without interference.

The fight for net neutrality became a major public policy debate in the United States, particularly in the mid-2000s to early 2010s. Proponents of net neutrality argued that without these protections, ISPs could act as gatekeepers, controlling what content users could access and creating a tiered internet where only those who could afford to pay for premium service would have their voices heard. This would not only stifle innovation and competition but also erode the fundamental

openness that had defined the internet since its inception.

On the other side of the debate, ISPs and some policymakers argued that they should have the right to manage their networks and offer differentiated services. They claimed that the ability to prioritize certain types of traffic, such as video streaming or online gaming, was necessary to manage network congestion and provide better service to customers.

The fight for net neutrality reached a critical point in 2015 when the Federal Communications Commission (FCC) in the United States adopted strong net neutrality rules under the Obama administration. These rules classified ISPs as "common carriers" under Title II of the Communications Act, which subjected them to stricter regulations designed to prevent discrimination and ensure equal access to all online content.

However, the battle was far from over. In 2017, under the Trump administration, the FCC repealed these net neutrality protections, sparking widespread protests and reigniting the debate over the future of the internet. The repeal of net neutrality was seen by many as a significant setback for internet freedom, raising concerns that ISPs could now have the power to control the flow of information and prioritize their own services over those of competitors.

The fight for net neutrality during the "Read-Write" era was emblematic of the broader struggle for internet freedom. It underscored the ongoing tension between

maintaining an open, egalitarian internet and the pressures of commercialization and corporate control. The debates and policies of this era shaped the future of digital interaction, highlighting the importance of vigilance in protecting the freedoms that make the internet a powerful tool for innovation, communication, and social change.

For future society builders, the lessons from the net neutrality debate are clear. As we move into the third age of the internet, the fight for a free and open web remains crucial. The policies and principles established during the "Read-Write" era will continue to influence how the internet evolves, and it is up to the next generation of leaders to ensure that the internet remains a platform where all voices can be heard, innovation can thrive, and trust is accessible to all. The battle for internet freedom is ongoing, and it requires continuous effort to protect the principles that have made the internet a cornerstone of modern society.

The Third Age - Read, Write, Own

As the internet continues to evolve, we find ourselves at the dawn of the "Read, Write, Own" era. This third age marks a pivotal shift in how we interact with digital content, driven by the decentralization of ownership through blockchain technology and the rise of Web3. Unlike the previous phases that centered on consuming and creating content, this era empowers users to take control of their digital assets and data, fundamentally redefining the dynamics of trust online.

In this new age, digital ownership becomes the cornerstone of the internet experience. Users are no longer just passive consumers or even active creators—they are now owners of their content, data, and digital identities. This ownership is not merely symbolic; it is enforceable, transparent, and secure, thanks to the innovations brought forth by blockchain technology. The very concept of trust is evolving alongside these developments. Trust in the "Read, Write, Own" era is not just about ensuring the security of transactions or verifying the accuracy of information; it is about guaranteeing that ownership and control over digital assets are respected and protected.

Chris Dixon, a leading voice in the discussion on Web3, has highlighted the transformative potential of these technologies. He argues that blockchain enables users to achieve true ownership of their digital identities, assets, and data—something that was previously impossible in the centralized models of the past. This shift, Dixon suggests, not only enhances user agency but also restores trust in online interactions by making them inherently transparent and verifiable.

However, with this new era comes a new layer of complexity. The decentralized nature of the "Read, Write, Own" age challenges traditional business models and introduces new paradigms for digital interaction. Centralized authorities, once the arbiters of trust, are being replaced by peer-to-peer networks and decentralized applications (dApps) powered by smart contracts. These blockchain-based systems allow users to interact directly with one another, bypassing

intermediaries and creating a more equitable digital economy.

For future society builders, the opportunities and responsibilities in this era are immense. The challenge is to design and develop platforms that uphold the values of accessibility, equity, and trust on a global scale. The principles espoused by thinkers like Chris Dixon provide a roadmap for building an internet where trust is not an afterthought but an integral part of the architecture. As builders, your role is to ensure that the benefits of this decentralized age are accessible to all, creating systems that are not only innovative but also inclusive and trustworthy.

The "Read, Write, Own" era is about more than just technology; it is about redefining the very fabric of the internet to make it a space where trust is embedded in every interaction. By embracing these principles and leveraging the power of blockchain, future society builders have the opportunity to create a digital world where ownership, transparency, and trust are the new norm. This is the next frontier in the ongoing journey to shape an internet that is free, open, and empowering for all.

Defending Freedom in the Third Age

As we enter the "Read, Write, Own" era, the fight for internet freedom takes on new dimensions. In this third age, where digital ownership and decentralized systems redefine our interactions online, defending freedom becomes both more complex and more critical than ever

before. The principles of openness, transparency, and equity that underpin this era are at risk from forces that seek to centralize control, restrict access, and undermine the trust that is being carefully woven into the fabric of the internet.

One of the most significant threats to freedom in this age is the potential for new forms of centralized power to emerge, even within decentralized systems. While blockchain technology and Web3 promise to decentralize ownership and empower individuals, they are not immune to the influence of powerful entities that may seek to exploit these systems for their gain. Large-scale blockchain networks and decentralized applications (dApps) can still be subject to the control of a few influential stakeholders, whether through the concentration of resources, control over key infrastructure, or manipulation of governance mechanisms. This concentration poses a risk to the very freedoms that the "Read, Write, Own" era is supposed to protect.

Moreover, as governments and corporations increasingly recognize the transformative power of blockchain and decentralized technologies, there is a growing push to regulate these spaces. While regulation can provide necessary protections for users, there is also a danger that overly restrictive policies could stifle innovation and limit the ability of individuals to fully exercise their digital rights. The challenge lies in finding a balance that allows for both innovation and protection, without compromising the foundational principles of freedom and decentralization.

Defending freedom in this new age also means ensuring that the benefits of the "Read, Write, Own" era are accessible to all, not just a privileged few. The digital divide, which separates those with access to the latest technologies from those without, could widen further if decentralized systems are not designed with inclusivity in mind. Future society builders must work to create platforms and technologies that are not only decentralized but also equitable, ensuring that everyone has the opportunity to participate fully in the digital economy.

Another critical aspect of defending freedom in this era is the protection of privacy. As users gain ownership over their digital identities and assets, the ability to control personal data becomes more important than ever. However, the very transparency that makes blockchain systems trustworthy can also pose risks to privacy if not carefully managed. Future society builders must prioritize the development of privacy-preserving technologies and practices that allow individuals to maintain control over their data without sacrificing the transparency that ensures trust in decentralized systems.

The defense of freedom in the "Read, Write, Own" era is not just about resisting external threats; it is also about fostering a culture of vigilance and responsibility within the decentralized communities themselves. This means promoting ethical behavior, encouraging active participation in governance, and ensuring that the principles of decentralization are upheld in practice, not just in theory.

For future society builders, the task of defending freedom in this new age is both a challenge and an opportunity. It requires a deep commitment to the principles of decentralization, a keen awareness of the potential risks, and a proactive approach to designing systems that protect and enhance the freedoms that are now at stake. By embracing this responsibility, you can help shape an internet that remains a force for good—a place where freedom, trust, and innovation thrive together, ensuring a future that is both secure and free for all.

3. India will awaken to life and freedom!

The Indian dream is humanity's dream. Let's make it real.

But what exactly is the mission statement?

As we transition into the third age of the internet—an era defined by decentralized trust and shared ownership—the mission of a nation like India becomes more crucial than ever. Just as the internet has evolved, so too must India's vision for its future. But what exactly

is India's mission statement as it steps forward into this new era of innovation, growth, and transformation?

In this new age, where digital ownership and decentralized systems are redefining the dynamics of trust, I believe India's mission is clear: to build a resilient, inclusive, and progressive society grounded in a strong foundation of trust. Trust is not just a concept; it's the key that will unlock India's vast potential to overcome its many challenges—whether they be economic inequality, technological divides, or governance issues.

The third age of the internet, with its focus on "Read, Write, Own," emphasizes the importance of trust in every aspect of digital and social interaction. For India, a country rich in diversity and driven by a young, dynamic population, the cultivation of trust is essential. It is trust in technology, governance, and human relationships that makes effective collaboration possible, drives investment, and fosters the sharing of ideas. In a nation as populous and varied as India, when trust is strong, the collective efforts of its people can lead to monumental changes.

But this mission extends beyond India's borders. As India rises on the global stage, the trust it builds in international partnerships—whether in trade, climate action, or technology—will define its global influence. Indian innovators have a unique opportunity to set new standards by creating systems that are not only cutting-edge but also reliable, transparent, and equitable. These systems can serve as models not just for India but for the world, showcasing how technology

can be harnessed to build a future where trust is accessible to all.

This chapter seeks to redefine India's mission statement by centering it on trust. We invite Indian builders, innovators, and leaders to think beyond immediate solutions and consider how their efforts can strengthen the fabric of society by building lasting trust. This foundational trust is what will awaken India to new possibilities, driving life and freedom for all its citizens. In the previous chapters, we explored the evolution of the internet and the growing importance of trust as we moved from the "Read-Only" era to the "Read-Write" era, and now to the "Read, Write, Own" age. We've seen how trust has been challenged and redefined through each stage, and how the fight to maintain a free and open internet has shaped the digital landscape we navigate today. Now, as we turn our attention to India's future, we must recognize that the cost of trust is not just an abstract concept but a critical factor in the nation's development.

India's journey towards becoming a global leader in technology and sustainable development hinges on creating an environment where trust flourishes. It is this trust that will empower Indian innovators to build systems that drive progress, uplift communities, and contribute to a more equitable world. As future society builders, your role is to ensure that this trust is not only established but nurtured, so that India—and indeed the world—can awaken to a future full of life, freedom, and endless possibilities.
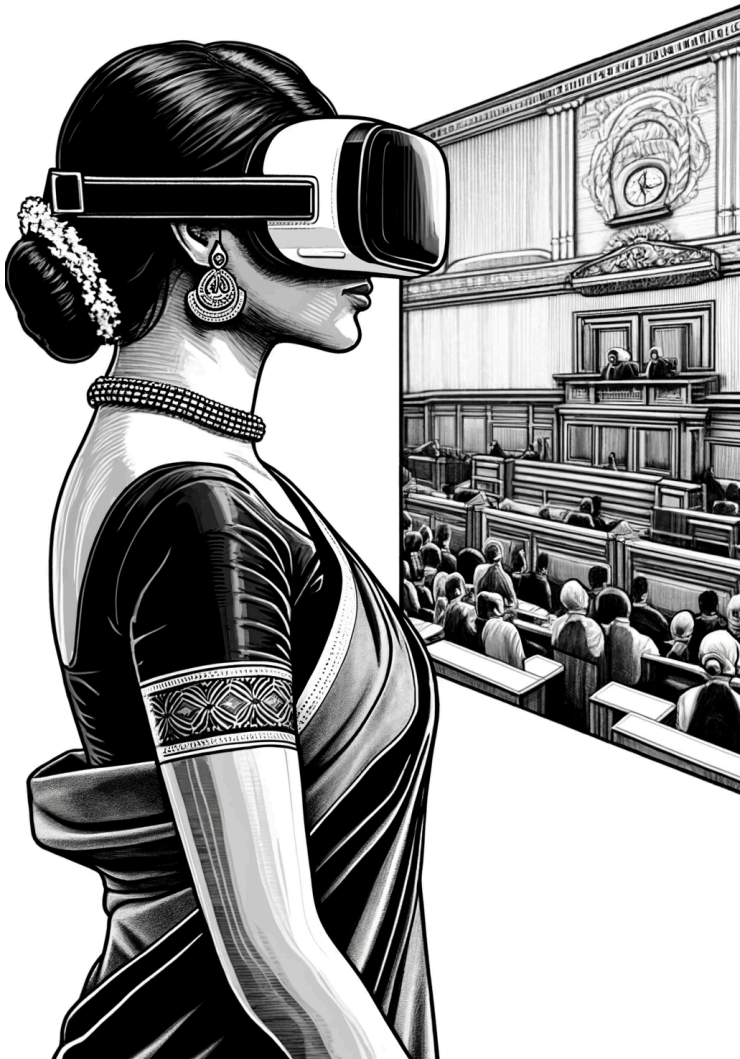
The Future of Trust and Leadership

As we advance into the era of Web 3.0—the "Read, Write, Own" phase of the internet—India stands on the brink of a transformative leap. This new age is not merely about consuming or creating content but about empowering individuals to own and control their digital assets and data. For Indian builders, this moment presents a unique opportunity to lead on both a national and global scale by redefining the cost of trust in digital interactions.

In Web 3.0, trust is no longer a commodity controlled by centralized authorities; instead, it is embedded into the very fabric of decentralized systems. These systems facilitate transparent and secure interactions without the need for intermediaries, drastically lowering the cost of trust. Decentralized systems ensure that transactions and data exchanges are immutable and verifiable, reducing the risks of fraud, corruption, and data manipulation. For India, mastering and adopting these technologies presents a pathway to address some of its most persistent challenges, such as data privacy, financial inclusion, and secure governance.

The future of India in this decentralized era must also embrace and celebrate the rich diversity of Indian culture while simultaneously forging a strong and unified whole. India's strength lies in its diversity—languages, religions, traditions, and cultures—that have coexisted and enriched one another for centuries. Decentralized systems can play a crucial role in supporting this diversity by allowing for localized solutions that respect

regional differences while enabling collaboration and unity on a national scale.

At the heart of this vision is a commitment to first principles: the foundational ideas that guide innovation, governance, and societal development. These principles include transparency, equity, and trust, which are not just technological goals but ethical imperatives. Decentralized systems offer a way to build these principles into the very architecture of society, ensuring that trust is not an afterthought but a core component of all interactions.

Transparency in decentralized systems ensures that actions and decisions are open to scrutiny, which fosters accountability and reduces the potential for corruption. Equity ensures that all individuals, regardless of their background or status, have equal access to the opportunities provided by these systems. Trust, the most critical of these principles, is maintained by the decentralized nature of these systems, where no single entity holds undue power, and the integrity of interactions is guaranteed by the system itself.

For Indian builders, embracing these first principles means creating platforms and solutions that do more than just innovate—they must also align with the ethical and cultural values that have shaped Indian society. This approach ensures that the diversity of India is respected and preserved while building a strong and unified nation that can lead in the global digital landscape.
As we explore the cost of trust in this new digital age, it becomes clear that the systems we build today will

determine the level of trust in our society tomorrow. For India, the challenge and opportunity lie in leading the way, not just for itself but for the world, realizing an Indian dream that reflects the aspirations of all humanity. By building a future where trust is accessible, transparent, and decentralized, India can awaken to a new era of life and freedom—serving as a beacon for others to follow.

A Proposed Vision

The year is 2050, and India has emerged as a global leader, not only through its economic strength and technological prowess but by pioneering a new paradigm of trust in digital and societal interactions. This leadership has been built on the mastery and implementation of decentralized Web 3.0 technologies, which have fundamentally lowered the cost of trust and transformed how communities engage with each other, both within the nation and across the globe.

In this future, India has revolutionized key sectors by embedding transparency, accountability, and trust at the core of its systems. The government and financial institutions have adopted decentralized technologies, making operations transparent and eliminating corruption. Public confidence in these institutions has soared, and India has gained international respect for its integrity and effectiveness in governance.

One of the most transformative innovations has been the use of token offerings to fund public infrastructure. Instead of relying solely on traditional taxation and debt, India has implemented a system where citizens and investors can directly contribute to infrastructure projects through tokenized offerings. These tokens represent fractional ownership or stakes in public assets like highways, bridges, or renewable energy installations. This model has democratized investment in public goods, allowing citizens to participate actively in the nation's development while benefiting from the returns generated by these projects.

In the healthcare sector, decentralized systems have enabled the creation of blockchain-enabled health records that ensure both privacy and data integrity. This has led to significant improvements in healthcare delivery, as patient data is secure and easily accessible, facilitating seamless medical care across different regions and fostering international collaborations in medical research and treatment.

The education system, too, has been transformed. Decentralized platforms now provide secure, interactive learning environments that not only make quality education accessible to all but also ensure that creators and educators are fairly compensated for their contributions. This has democratized education, making it a shared, equitable resource across the country.

India's legal system, once plagued by inefficiencies, now operates with unprecedented transparency and fairness. Digital ledgers track legal processes, ensuring that all actions are transparent and accessible, leading to faster resolutions and greater public trust in the justice system. Furthermore, India has become a global leader in environmental sustainability by using decentralized systems to manage carbon credits and environmental impact assessments, ensuring that development is balanced with ecological responsibility.

The financial system has also been reimagined. Token-based incentives have been used to address societal challenges such as climate change and social inequality, creating a more equitable and sustainable economy. The automation of financial services has

streamlined the industry, shifting the focus from profit-driven operations to solving pressing human challenges and enriching lives.

By 2050, India is not only a hub of innovation but also an inspiration to the world. It demonstrates how technology, when aligned with ethical values, can serve society and drive global progress. Through its pioneering use of decentralized systems and token offerings for public infrastructure, India has set new standards in trust, transparency, and inclusivity, showing that the future is brightest when technology empowers people and nations alike.
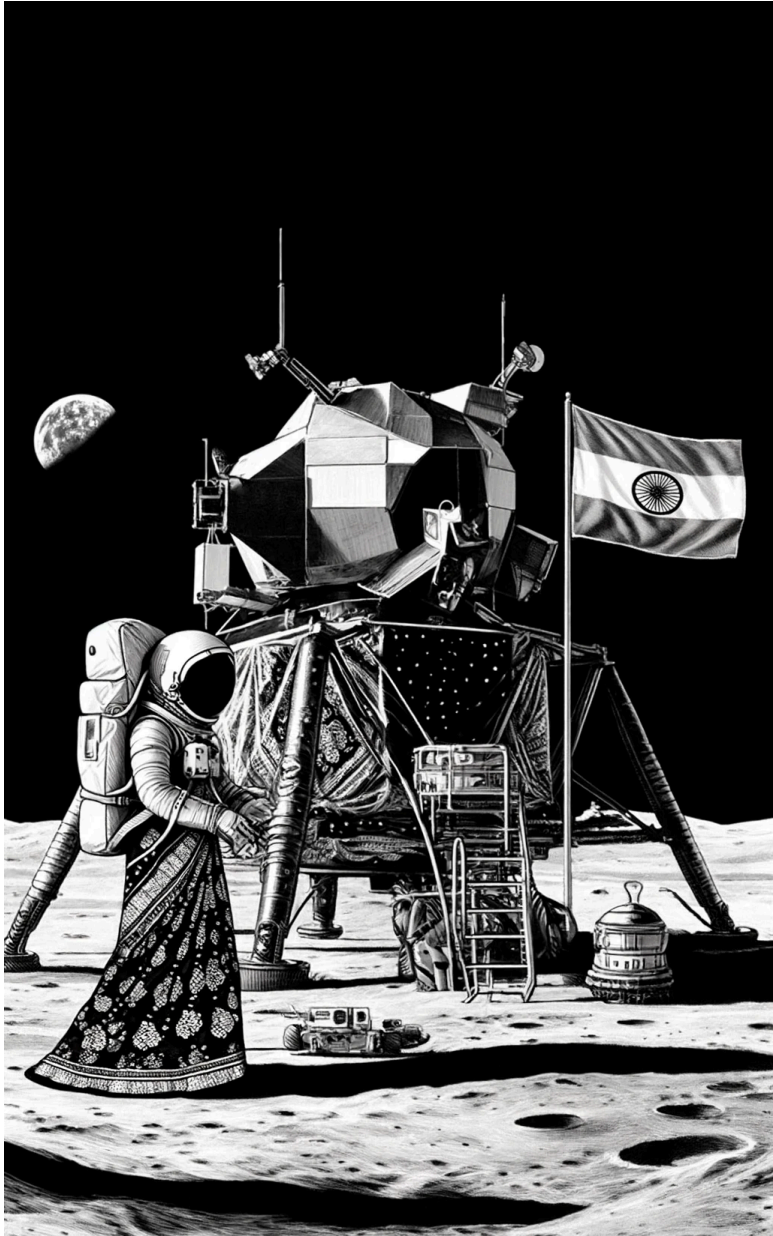
Part 2: What is the minimum I should know?

4. Crypto Basics

What is Crypto Exactly? And why is it a big deal?

Crypto is a broad term. So let's take a moment to discuss what it is exactly.

As we continue our exploration of trust and innovation, it's time to delve into crypto. But what exactly is crypto, and why is it causing such a stir?

Crypto is a broad term that encompasses a world of digital currencies and technologies, all built on an underlying system called blockchain. If we look back at the evolution of the internet—from the "Read Only" era, through "Read, Write, and socialize," to the current "Read, Write, Own" phase—crypto plays a crucial role in this transformation, particularly in how it redefines ownership and trust in the digital age.

To make sense of crypto, let's use an analogy that everyone can relate to: movies. In the world of cinema, the script is fundamental. It shapes the story, the characters, and the direction of the film. Without a script, there's no movie. Similarly, in the world of crypto, blockchain is like the script. It's the foundation upon which everything else is built. Just as different movies

have different scripts, different cryptocurrencies are built on different blockchains.

For example, think of Bitcoin as the movie Bahubali and Ethereum as RRR. Both are blockbuster films with powerful stories, but their scripts—their blockchains—are different. Bahubali tells a fantasy story set in ancient India, while RRR revolves around a revenge narrative. Both scripts share common elements like a beginning, middle, and end, with protagonists overcoming incredible odds. However, they differ in the specifics of the story and how they unfold it.

Similarly, the Bitcoin blockchain and the Ethereum blockchain share fundamental elements like blocks, a consensus mechanism, and hash functions. But, like the movies, they differ in how these elements are implemented. Bitcoin's blockchain is structured differently from Ethereum's, their consensus mechanisms operate in distinct ways, and they use different technologies to ensure security and integrity.

To help visualize this, imagine:

Script = Blockchain : Movie = Crypto

We're going to stretch this movie analogy further to build a mental model that will help you understand crypto in more depth. This requires a bit of imagination, so we'll

use a technique called "Mental Imagery." [50] [51] Get ready to picture how these abstract concepts work together, just like scenes in a movie.

[50] Johnson-Glenberg, Mina C., et al. "Improving Science Learning with Visualizations of Embodied Processes." Journal of Experimental Psychology: Learning, Memory, and Cognition, vol. 38, no. 4, 2012, pp. 1104-1113

[51] Nemirovsky, Ricardo, et al. "Mental Imagery, Motivation, and Mathematical Problem Solving." Learning and Instruction, vol. 15, no. 5, 2005, pp. 507-525.

Blockchain

Continuing with our movie analogy, think of a blockchain as a script that is constantly being written. Just as a script has pages, a blockchain has blocks. The key difference is that while a script for a movie like Bahubali or RRR has a finite number of pages, a blockchain keeps growing as more blocks are added. In the world of movies, several writers collaborate to decide what goes into each page of the script. In the world of blockchain, however, a decentralized group of anonymous computers works together to add each block.

Let's extend this mental model further. Imagine that we're creating a script for a movie that never ends—each page represents a new event or piece of information, and once a page is added, it can never be changed. This script would be an ongoing, unalterable record, much like a blockchain. In a sense, crypto, built on blockchain technology, can be seen as an unbiased record of events, beginning with the launch of Bitcoin in 2008, and continuing indefinitely.

But how does a blockchain ensure that once a block is added, it can never be altered? This is where something called a hash function comes into play—a critical piece of the crypto story. A hash function is like a seal that secures each page of our never-ending script, ensuring that no one can go back and alter what has already been written. This seal makes the blockchain not only a dynamic record but also a trustworthy one, where each

new block builds upon the previous ones, creating an unbreakable chain of information.

By understanding this, we can begin to grasp the power and significance of blockchain technology. It's not just about recording transactions or data; it's about creating a secure, transparent, and unchangeable history—a record that, like our imaginary movie script, is continuously written and preserved for all to see.

The Hash Function

If you haven't already, you should watch *The Imitation Game.* It's a film about an intelligence unit led by Alan Turing, played by Benedict Cumberbatch, that develops an early form of a modern computer to break encrypted Nazi codes. These codes were generated using the Enigma Machine, a predecessor to what we now call a hash function. This might sound complex and deeply rooted in computer science—because it is. But the good news is, all you really need to understand is that a hash function uses math to create a unique fingerprint for any piece of information.

Continuing with our movie analogy, imagine if each page of our never-ending script could be represented by a unique fingerprint—a fingerprint that would change completely if even a single letter or space on that page were altered. If you capitalized one tiny letter, the entire fingerprint would be different. That's essentially how a hash function works. It ensures that each block in a blockchain is represented by a unique fingerprint, making it nearly impossible to alter the information without everyone noticing.

Example:

Sha 256 Hash of **Prashanth Irudayaraj** :

74d6eb5ff51fb8a5122bf71c26e6c0d09bad1a6b7888fa02fcc7a364 0ea90688

Sha 256 Hash of **prashanth Irudayaraj** :

814681d6ec4d8a07b222f8b5b1f0bfd00d8092348e08f4ac3912e8c 62eedf7a8

In this example, the first hash is generated from "Prashanth Irudayaraj" with the first letters of the first and last names capitalized. The second hash is from the same name, but with the first letter of the first name in lowercase. Despite this small change, the entire hash output is completely different.

This illustrates how even a tiny modification to the input can drastically alter the hash, ensuring that each block in a blockchain has a unique and secure identity. This unique fingerprint is what keeps the blockchain secure and unchangeable, as any attempt to alter a block would result in a completely different hash, alerting everyone to the change.

Keep this concept in mind as we continue to build out your understanding of crypto and blockchain. It's a fundamental part of how trust is maintained in these systems—each block, like a page in our script, is secured with a unique, unalterable fingerprint.

Peer-to-Peer Networks & Gossip

So, who exactly is writing this never-ending script? In a blockchain, each block is added by a single computer selected by a protocol, but the process involves many computers that work together to put transactions into blocks and 'attempt' to add them to the blockchain. In our imaginary movie analogy, it's as if multiple writers are drafting the same new page with more or less the same events, but only one of those drafts gets chosen to be added to the script. The method by which this selection occurs is known as the consensus

mechanism, and just like in the real world, it's a complex process.

This network of computers that collaborate to write the script is known as a peer-to-peer (P2P) network. Our imaginary writers, who share information with each other to construct the new page, can also be considered part of a peer-to-peer network. In the digital world, P2P networks have been around for quite some time. If you were a kid like me in the late 90s or early 2000s, you probably remember downloading movies and songs using Bittorrent.

Let's take a moment to talk about Bittorrent. Bittorrent is a peer-to-peer network that allows people to share files, with each computer in the network holding a piece of the file. When you download something via Bittorrent, your computer is piecing together parts of that file from multiple sources, eventually assembling the complete file on your machine[52]. For example, if you're downloading a movie, different parts of that movie exist on various computers. Your computer searches for those parts and combines them into a full movie file that you can watch. Napster, another disruptive innovation from the same period, operated in a similar way.

In the context of our blockchain script, think of these P2P networks as the underlying infrastructure that enables our writers (or computers) to communicate and

---

[52] Qiu, D., & Srikant, R. (2004). Modeling and performance analysis of BitTorrent-like peer-to-peer networks. In ACM SIGCOMM Computer Communication Review (Vol. 34, No. 4, pp. 367-378). Retrieved from https://dl.acm.org/doi/10.1145/1030194.1015500

share their drafts. Each writer has a version of the new page, but through a consensus mechanism, only one version is selected and added to the script. This ensures that everyone in the network agrees on the final version of the story, just as a blockchain ensures that all participants agree on the state of the ledger.

This P2P communication and consensus-building process is what keeps the blockchain secure, decentralized, and resistant to manipulation. It's a fundamental part of how trust is distributed across the network, without relying on a single, centralized authority.
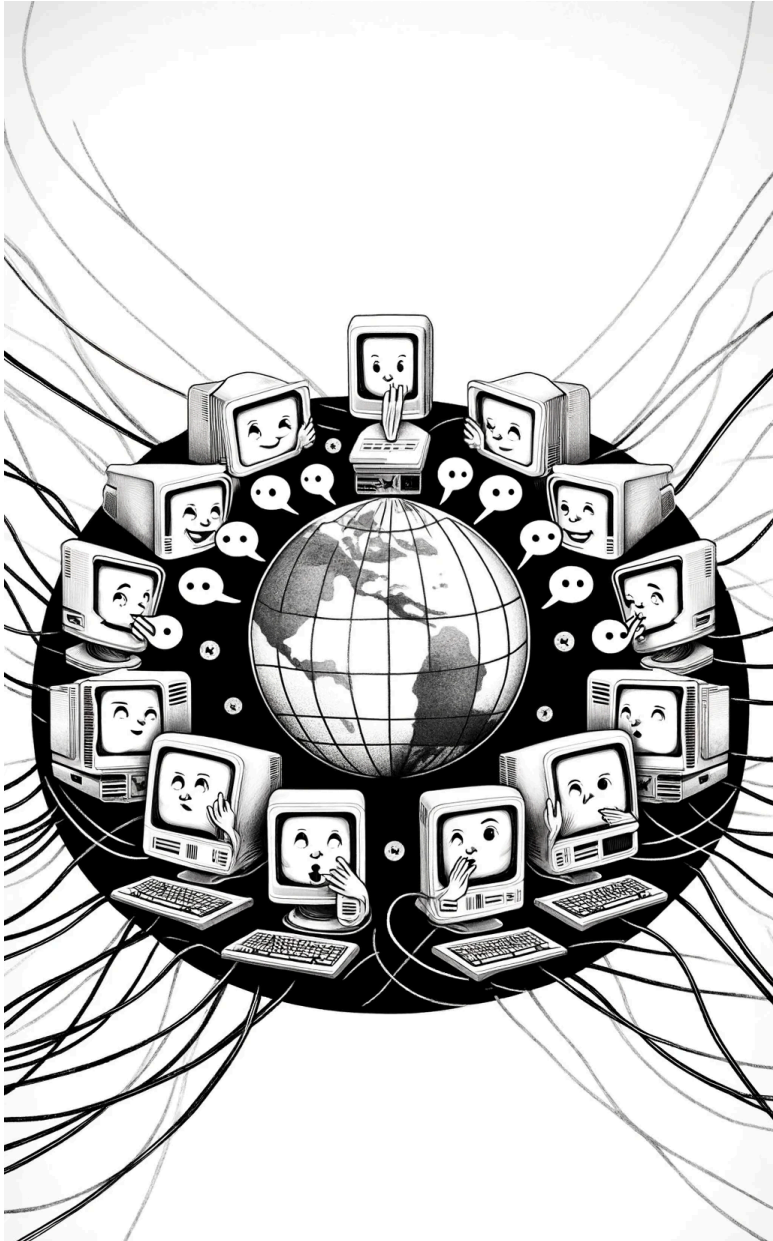
Consensus

How do you get writers to agree on a story? If you're in the film business, you've probably noticed that this can be a pretty challenging task—and it only gets harder as the number of writers increases. In our imaginary movie, let's picture a scenario where there are at least 100,000 writers, each with their own version of the next page. Now, imagine that the writer whose page gets chosen earns $100,000, while the others get nothing. The stakes are high, making the decision process even more complicated.

This is very similar to the challenge faced in selecting the next block to be added to a blockchain. In most crypto systems, a large number of computers propose their version of the next block. These blocks are typically similar, containing more or less the same transactions. The block that ultimately gets selected is rewarded with a compensation—just like the chosen writer in our analogy.

Here's where things get a bit complex. In Bitcoin, the first computer to produce a block with a specific fingerprint pattern—determined by solving a complex mathematical puzzle—gets selected. This process is known as Proof of Work. In Ethereum, the process is different. Smaller committees are formed from the entire pool of computers, and one member of the committee is selected to add the block while the others ensure there's no cheating. This method is called Proof of Stake. These and other consensus mechanisms are designed to ensure that the block added to the blockchain is

chosen fairly and without undue advantage to the computer that adds it—aside from the reward it receives.

Yes, this is complex, but the core idea is simple: consensus mechanisms are the processes that allow all these computers (or writers) to agree on which block (or page) gets added next. It's a way to maintain fairness and trust in a decentralized network, where no single entity has control over the system.
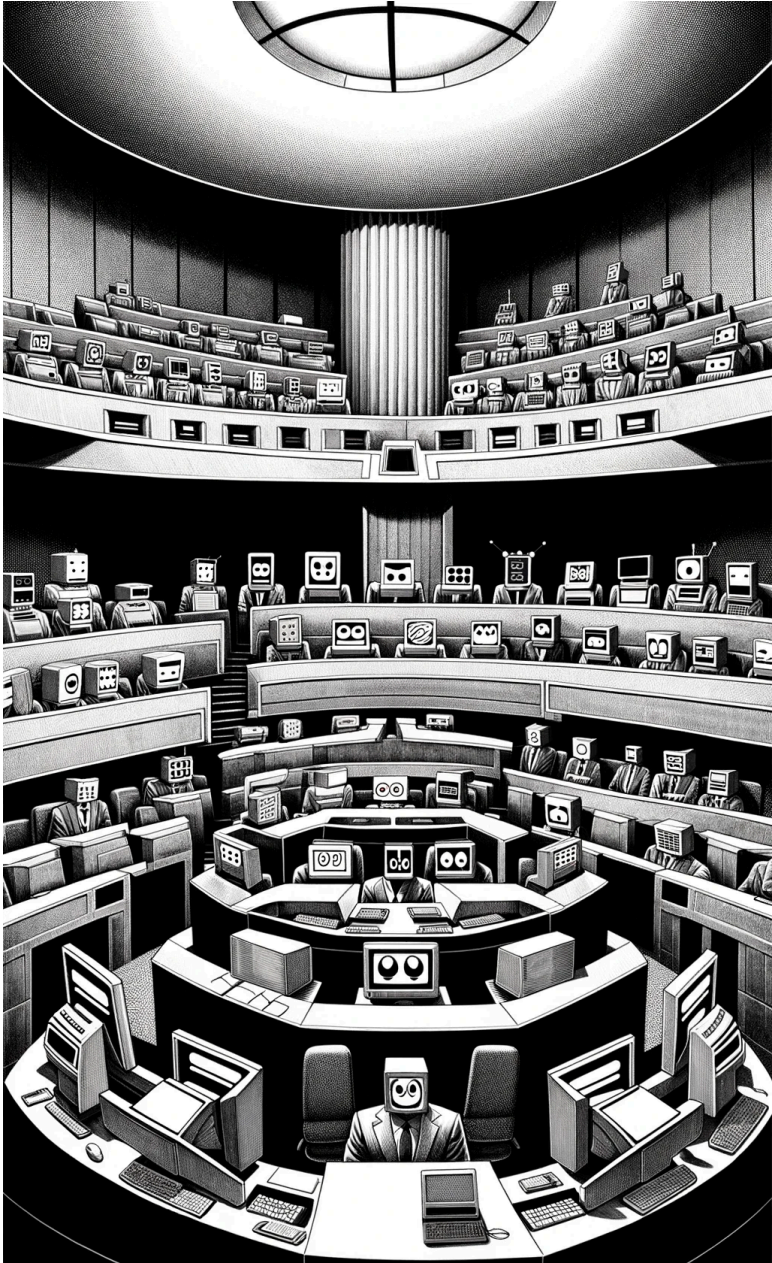
Double Spending

Now, let's shift gears and talk about a unique challenge in the world of digital money: double spending. Double spending occurs when a single digital token is spent more than once, a problem that arises because digital files, unlike physical money, can be easily duplicated or falsified.

To understand double spending, consider a simple everyday scenario: suppose you buy a coffee using a $5 bill. Once you hand over that bill to the barista, you no longer have it, so you can't use the same $5 to buy something else. However, in the digital world, if you were to pay with a digital $5, it's possible to create a copy of that digital $5 and attempt to spend it again elsewhere.

The cost of trust in digital transactions revolves around this issue. If people could easily duplicate their digital money and spend it multiple times, trust in that digital currency would quickly evaporate. Sellers would begin to refuse it, knowing it could be fraudulent, rendering the currency practically worthless.

Blockchain technology, as used by cryptocurrencies like Bitcoin, solves the double spending problem without needing a trusted third party like a bank. It does this by maintaining a public ledger of all transactions, distributed across multiple computers in the network. Once a transaction occurs, it is recorded on this ledger and secured through cryptographic means. Since every participant in the network has access to the blockchain,

they can verify whether a digital token has already been spent, making double spending virtually impossible.

This decentralized verification process is what restores trust in digital transactions. By ensuring that each unit of digital currency can only be spent once, blockchain technology upholds the integrity and value of digital money, allowing it to function reliably in a digital economy.

Cryptography

Cryptography plays a critical role in the world of cryptocurrencies, adding immense value by ensuring that all transactions are secure and virtually tamper-proof. In digital currencies like Bitcoin, cryptography creates a secure environment for transactions to occur without relying on a central authority. This is achieved by generating complex codes that secure each transaction recorded on the blockchain.

The impact of cryptography on the cost of trust in the cryptocurrency world is profound. Traditionally, transactions have required intermediaries like banks to verify and facilitate the process, which often involves time and fees. Cryptography eliminates the need for these intermediaries by enabling direct peer-to-peer transactions. Each transaction is securely encrypted, and its verification depends on the consensus of participants in the network, rather than on any single authority. This decentralized approach drastically reduces the cost of trust by minimizing the risks of fraud and corruption, and by lowering transaction fees through the elimination of middlemen.

In essence, cryptography not only secures transactions but also enhances efficiency, reducing the economic and social costs traditionally associated with establishing trust in financial exchanges. This foundational security is what allows cryptocurrencies to function as a reliable medium of exchange in the global economy.

By enabling secure, transparent, and direct transactions, cryptography is a cornerstone of the trust that underpins the entire cryptocurrency ecosystem. It ensures that participants can engage in exchanges with confidence, knowing that their transactions are protected by sophisticated mathematical algorithms. This level of security is what makes cryptocurrencies a revolutionary force in the world of finance, offering a new model for how trust can be established and maintained without the need for centralized control.
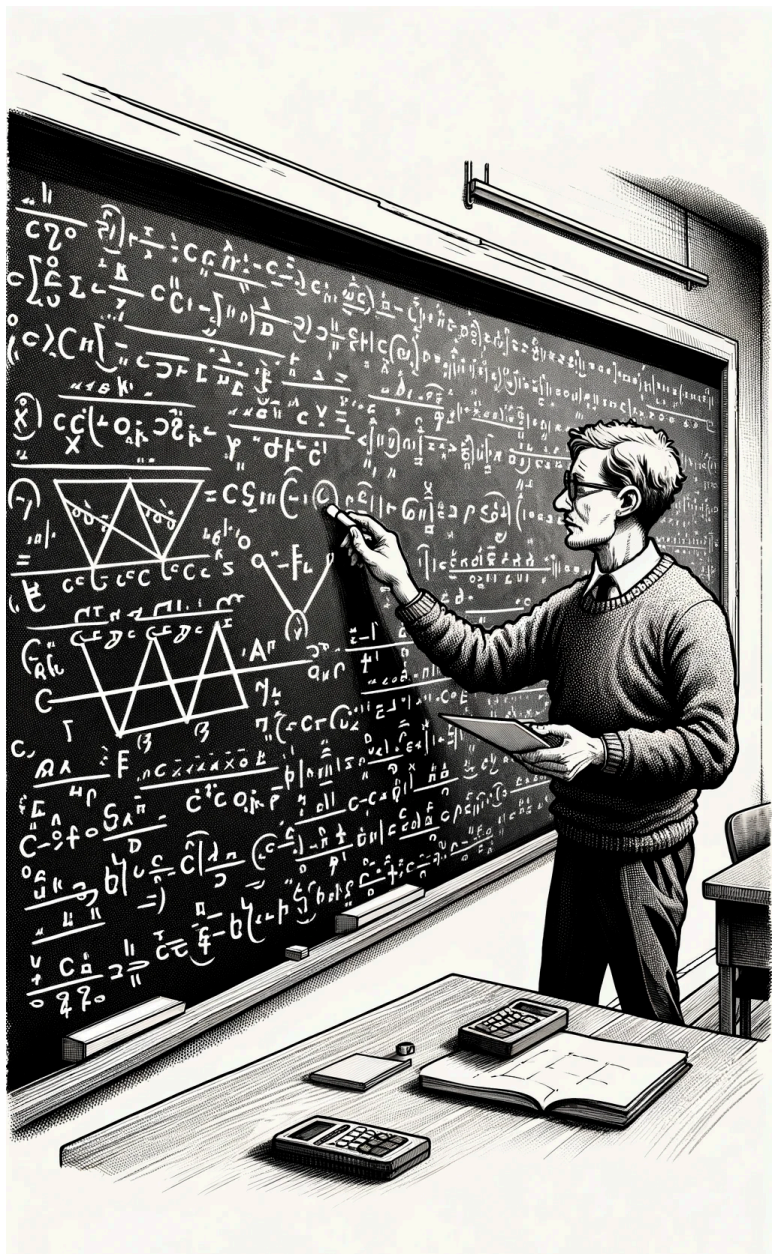
5. Practical Crypto

Freeeeeeedom!!!!!

As we continue our journey into the world of crypto, let's pause for a moment to recap. So far, we've explored the concept of trust, the evolution of the internet, and how crypto is reshaping the landscape by redefining ownership and trust. Now, it's time to get practical and see how these ideas translate into the tools and platforms that make up the crypto world.

Remember our analogy from earlier? Just like a movie script guides the entire production, shaping the story and characters, a blockchain is the script for crypto. It's

the foundation on which everything is built, where each block is like a new scene in the story, added in sequence without erasing what came before. Think of it as a book written in permanent ink—once something is added, it stays there forever, and the story continues to unfold with each new block.

In this chapter, we'll dive into the practical aspects of this "movie production." You'll learn about the tools and platforms that allow you to interact with the blockchain—the scripts of various cryptocurrencies—and understand how they all fit into the bigger picture. We'll cover essential topics like wallets, addresses, and keys—your gateway to the crypto world. We'll explore how exchanges work, both centralized and decentralized, and how you can navigate them. You'll also discover what block explorers are and why they're important. Finally, we'll touch on Layer 1 (L1) and Layer 2 (L2) solutions, and how they enhance the blockchain's capabilities, much like how special effects enhance a movie's impact.

Wallets, Addresses & Keys

Now that you have built a minimum viable mental model of crypto and blockchain, we finally get to the point where you can directly participate in crypto. You do this through wallets and keys.

An address and a public key are essentially the same thing. To understand why it's called a public key, we would have to delve deeper into cryptography, but that's not necessary at this stage. A simple way to think about

a public key is like your bank account number or your street address. When you want a wire transfer, you give people your bank account number; when you want mail delivered, you give out your street address. Similarly, when you want to receive money in the crypto world, you provide your public key, also known as your address.

A wallet is what you use to store your private key. Your private key is like a password that allows you to authorize transactions on the blockchain, and it's crucial that you never show it to anyone. The wallet should be designed to keep your private key secure and hidden. Keeping your private key secret is absolutely critical. If someone else gets hold of it, they can steal your money or, worse, pretend to be you and make transactions that could get you into serious trouble.

In most blockchain systems, managing your wallet and keys is extremely important. Unlike traditional banking, where transactions can sometimes be reversed, blockchain transactions are final. Once a transaction is made, it cannot be undone, so it's essential to protect your keys and double-check before making any transaction.

Some easy-to-use wallets to get started with include Brave Wallet, Metamask, and MyEtherWallet. If you want to be extra secure, consider using a Ledger or Trezor hardware wallet. These hardware wallets are especially useful in some countries where they also allow you to buy crypto directly.

Exchanges

The easiest way to buy crypto is through an exchange. There are two kinds of exchanges: Centralized Exchanges (CEX) and Decentralized Exchanges (DEX). Because crypto is still a relatively new and evolving space, it's important to be cautious about which CEX or DEX you use, as the wrong choice could result in the irrecoverable loss of your funds.

Centralized Exchanges (CEX) are typically run by a company, and you'll need to go through a Know Your Customer (KYC) process and sign up to buy and trade crypto. These exchanges often provide a user-friendly interface, making it easier for beginners to get started. However, it's crucial to research the exchange thoroughly before signing up, as withdrawing your funds can sometimes be difficult if the exchange has poor banking relationships or runs into regulatory issues.

Decentralized Exchanges (DEX), on the other hand, allow people to trade cryptocurrencies directly with each other without needing an intermediary or central authority. DEXs operate using blockchain technology, which ensures that all transactions are recorded transparently and securely. Typically, DEXs are used for trading once you've already acquired some crypto. Their fees are usually higher, and you'll need to transfer crypto to them from a centralized exchange. There's plenty of information available on how to do this.

Decentralized Exchanges (DEX)

A Decentralized Exchange (DEX) is a type of cryptocurrency exchange that allows individuals to trade cryptocurrencies directly with one another, without the need for an intermediary or a central authority. This setup operates using blockchain technology, which ensures that all transactions are recorded transparently and securely.

To understand how a DEX works, think of it as a marketplace where buyers and sellers connect directly. Unlike traditional exchanges, where the exchange itself controls the transaction process, a DEX uses smart contracts—self-executing contracts with the terms of the agreement directly written into code. This means that the rules of the trade are set and automatically enforced by the technology, without the need for any human intervention.

One popular example of a DEX is Uniswap. Platforms like Uniswap are often seen as superior alternatives to centralized exchanges for several reasons:

1. **Security**: Since there's no central point of control, DEXs are less vulnerable to hacks, which are common in centralized systems where all data is stored in one place.
2. **Privacy**: Users on DEXs typically do not need to undergo identity verification processes, offering greater privacy.

3. **Control**: Users maintain control of their funds and trade directly from their own wallets, rather than entrusting their assets to a third party.
4. **Open and Inclusive**: DEXs are generally open to anyone in the world, not restricted by location or requiring approval from a central authority.

The shift towards decentralized exchanges reflects a broader movement towards decentralization in the financial world. Many experts believe that as technology progresses and more people seek alternatives to traditional financial systems, the world is likely to move towards decentralized exchange models. These platforms offer a more resilient, open financial system that can potentially lower costs, reduce barriers to entry, and increase access to financial services globally.

Decentralized exchanges embody the principles of decentralization and trust that are foundational to the crypto world. By allowing users to trade directly and securely without intermediaries, DEXs represent a significant step forward in creating a more equitable and transparent financial system. As you continue to explore the practical tools and platforms of the crypto world, understanding how DEXs operate will be key to navigating this evolving landscape with confidence.

Block Explorers

To navigate and explore the information stored on a blockchain, you can use a tool called a block explorer. Block explorers are essential for anyone interacting with cryptocurrencies, as they allow you to view the details of

transactions and other data recorded on the blockchain. For example, Etherscan is a popular block explorer used to view transactions on the Ethereum blockchain, but most blockchains have their own native explorers.

Block explorers like Etherscan serve several important functions. They allow you to verify that a transaction has been recorded on the blockchain, providing transparency and security. Additionally, you can use them to review all the transactions associated with a specific account. Often, an address might be linked to a known entity, such as Coinbase, making it easier to identify the source or destination of funds. If you know the public address of a friend or family member, you could even view all the transactions they've ever made on that blockchain.

Block explorers are invaluable for understanding how accounts and transactions work within each blockchain ecosystem. They provide a real-time view of what's happening on the network, allowing you to see the most recent transactions, the status of various blocks, and other critical data. Whether you're verifying a transaction, researching the history of an account, or simply curious about the activity on a particular blockchain, block explorers are your go-to tools.

These explorers are not just useful for individual users; they also play a key role in maintaining the transparency and integrity of the entire blockchain ecosystem. By making all transactions visible and verifiable, they help ensure that the decentralized nature of the blockchain remains intact and that trust in the system is upheld.

L1s and L2s

In the world of blockchain and cryptocurrencies, L1 and L2 refer to two layers of blockchain technology, each playing a distinct role in managing transactions and enhancing overall performance.

L1, or Layer 1, is the base layer of a blockchain network. This includes foundational blockchains like Bitcoin and Ethereum. The primary role of L1 is to maintain and secure the entire network using its own blockchain protocol. This layer handles all transactions directly on the blockchain itself, ensuring accuracy and security through consensus mechanisms like Proof of Work or Proof of Stake. However, because all transactions are processed on the main chain, Layer 1 can suffer from issues like slower transaction speeds and higher costs, especially during periods of high network congestion.

L2, or Layer 2, is built on top of the L1 blockchain to improve its scalability and efficiency. Layer 2 solutions handle transactions off the main chain and only interact with the L1 blockchain to finalize them. This significantly reduces the load on L1, allowing for faster and cheaper transactions. Examples of Layer 2 solutions include the Lightning Network for Bitcoin and various scaling solutions for Ethereum, such as rollups and sidechains.

The relationship between L1 and L2 is crucial in reducing the cost of trust in blockchain networks. By offloading transaction processing to L2, the main blockchain (L1) isn't bogged down by high volumes of

transactions, which can lead to slower processing times and higher fees. This setup not only enhances the network's scalability but also maintains the security and decentralization that are essential for trust in the network.

To better understand this, think of **Mumbai** as Layer 1 (L1) in a blockchain analogy. Mumbai, much like an L1 blockchain, is the foundational layer where all the core activities happen. It's the bustling, main network where daily transactions—whether economic, social, or cultural—take place. Mumbai's infrastructure supports these activities, but it can become congested due to the sheer volume of interactions, similar to how a blockchain like Ethereum can experience slow transaction times and high fees when it's overly busy.

Now, imagine **Navi Mumbai** as the Layer 2 (L2) solution. Navi Mumbai, developed as a planned extension to reduce congestion in the main city, functions similarly to an L2 in the blockchain world. Just as Navi Mumbai alleviates the pressure on Mumbai's infrastructure by offering additional space and facilities, Layer 2 solutions help ease the load on L1 by handling transactions off the main blockchain. These transactions are processed more efficiently and then finalized on the main chain, much like how Navi Mumbai supports the greater Mumbai region by providing an alternative space for growth and development.

By handling transactions off the main blockchain, L2 solutions like Navi Mumbai enhance the system's overall efficiency, improving speed and reducing costs while maintaining the security and trust inherent in the L1

blockchain. This layered approach allows the entire system to function more smoothly and effectively, just as Navi Mumbai contributes to the overall livability and functionality of the Mumbai metropolitan area.
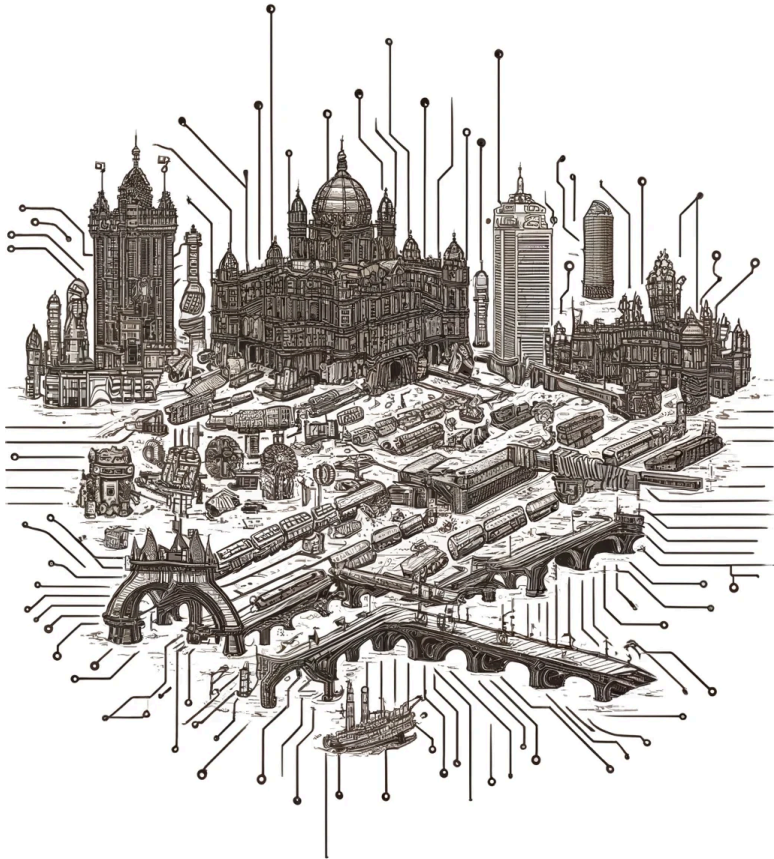
6. Bitcoin

Not your Keys, Not your coin!

Money can be agency. You give away
your keys, you give away your agency.

Bitcoin (BTC) is the most well-known cryptocurrency and the reason this entire industry exists. Its creation marked a pivotal moment in the history of trust, finance, and technology. While no one knows for sure who created Bitcoin, we do know that the Bitcoin whitepaper was released by a pseudonymous individual or group known as Satoshi Nakamoto.

To understand why Bitcoin is so revolutionary, let's revisit the themes of trust and control we discussed earlier. In the first chapter, we explored the cost of trust—the idea that trust is essential but often comes with a price, especially when placed in centralized institutions. This cost became painfully clear during the 2008 financial crisis, a moment that revealed just how much of the global economy was controlled by a small group on Wall Street and how their reckless pursuit of wealth led to a catastrophic collapse.

The 2008 financial crisis was a wake-up call. It exposed the fragility of a financial system built on trust in a few powerful entities and highlighted the dangers of inflation—a concept we'll delve into further in this

chapter. As governments around the world scrambled to bail out big banks, people began to question the integrity and fairness of the existing financial system.

In this environment of uncertainty and mistrust, Bitcoin was born. Bitcoin was designed as a response to these failures—a decentralized form of money that operates independently of governments and traditional financial institutions. It was a radical idea: to create a system where trust is not placed in any one person, company, or government, but in the network itself, secured by cryptography and consensus mechanisms.

The significance of Bitcoin's creation is highlighted by a note embedded in the first block of its blockchain (the first "page" of its script, as we've used in our movie analogy). This note references the German bank bailout, symbolizing Bitcoin's intent to challenge the status quo of centralized financial control.

Understanding Bitcoin and how it works is crucial because it has successfully achieved something previously thought impossible: generating trust without a centralized intermediary. This chapter will explore how Bitcoin accomplishes this and why it matters. We'll look at key features of Bitcoin, how it addresses issues like inflation and scarcity, and how it works from a technical perspective.

To make these concepts more tangible, we'll also introduce a game that illustrates how Bitcoin generates trust through its decentralized network. This game will help you grasp the principles behind Bitcoin in an interactive and engaging way.

Understanding Inflation

When the U.S. government created bailout packages for big banks during the 2008 financial crisis, they added more money to the economy through a process called quantitative easing. The effects of this were felt over the following years as the prices of goods and services began to rise. This happened because there was more money available to buy things, leading to more dollars competing for the same goods and services. As a result, these goods and services could command higher prices, increasing the cost of living for everyone.

Let's break this down further.

Bitcoin is an attempt to create a global currency with a limited supply, designed to increase in value over time. For instance, if you can buy one loaf of bread with one Bitcoin today, after a few years, you might be able to buy that same loaf with just 0.75 BTC. And after a few more years, it could cost even less. This deflationary model contrasts sharply with traditional fiat currencies, where increasing the money supply typically leads to inflation and the erosion of purchasing power.

Bitcoin's value comes from several factors that interplay to give it worth in the eyes of its users and investors. Over the years, as more people have adopted Bitcoin, its value relative to the dollar has seen a significant increase. For instance, while one Bitcoin could buy around $300 in 2015, by 2022, that same Bitcoin could purchase approximately $30,000. This increase in value can be attributed to a combination of factors, including

increased adoption, speculative buying and selling, and a decrease in the overall value of the dollar.

One of the core reasons behind Bitcoin's rising popularity is its role as a diversification tool in investment portfolios. Particularly in countries where local currencies are unstable and less trusted, Bitcoin offers an alternative store of value despite its volatility. Its decentralized nature—free from government or financial institution control—and the fixed limit on the total number of Bitcoins that can ever exist make it attractive to those wary of traditional inflationary monetary policies.

To illustrate Bitcoin's value, consider my experience working with humanitarian technologies in Haiti to solve food insecurity. In regions like Haiti, where the local currency may be unstable and banking systems not robust, Bitcoin provides a secure, trustworthy alternative for transactions and savings. This trust is crucial in areas with weak financial infrastructure, offering a reliable means of economic exchange and a safe haven for assets.

In essence, Bitcoin's value is closely tied to the trust its users place in it as a secure, decentralized, and potentially appreciating asset. This trust, contrasted with the declining trust in traditional currencies subject to inflation and political risk, underscores the growing shift towards digital currencies in the global economy.

Value through Scarcity

Bitcoin's value is significantly influenced by its scarcity, a principle that is fundamentally built into its design. The total supply of Bitcoin is capped at 21 million coins, and these coins are introduced into the system at a diminishing rate over time. Specifically, the rate at which new Bitcoins are mined halves approximately every four years, an event known as "halving." This design makes Bitcoin deflationary, unlike traditional fiat currencies, which can be printed indefinitely and are thus inflationary.

Let's delve deeper into why this scarcity impacts Bitcoin's value. Since the supply of Bitcoin is limited, and no more Bitcoins will ever be produced once the cap is reached, it becomes a scarce resource. Scarcity is a powerful economic driver that can increase the value of an asset, particularly if the demand for it grows. As Bitcoin becomes more widely accepted and used as a store of value, the demand for it increases. With more people wanting to buy Bitcoin while the supply remains fixed, the price naturally goes up.

To illustrate this concept, consider a supply and demand curve. The supply curve for Bitcoin is vertical, reflecting a fixed supply. As demand increases, the demand curve shifts to the right. Since the supply is limited and cannot expand to meet rising demand, the equilibrium price rises. This is a classic economic illustration of how scarcity affects price, particularly when an asset like Bitcoin becomes more desirable either for its potential returns as an investment or as a hedge against inflation and currency devaluation.

This mechanism of capped supply and diminishing issuance is a key reason why many view Bitcoin as 'digital gold'—a scarce asset that can potentially appreciate over time, offering a hedge against inflation and currency devaluation, similar to traditional gold. Thus, the trust in Bitcoin's value continues to grow as it gains acceptance among more users and investors, acknowledging its utility as a decentralized store of value that is not subject to manipulation by any government or central entity.

Key Features of Bitcoin

Most people value Bitcoin because it is scarce, making it a good store of value similar to gold. But why use Bitcoin instead of gold? Gold has proven itself as a store of value for thousands of years. Well, Bitcoin has several advantages over gold: it is available anywhere the internet is available, all transactions can be viewed online, and you alone have control of your Bitcoin. You can walk a thousand miles carrying all your savings with you, and no one would be the wiser because you physically carry nothing.

It's easier to understand the value in Bitcoin's usability with an example. Imagine you're living in a destabilized country like Ukraine. How would you protect your wealth when banks and the country's financial infrastructure are no longer operational, and your country could cease to exist?

Bitcoin is one way to ensure that you don't lose all your savings. By converting your assets to Bitcoin, you can leave your destabilized country and start fresh anywhere. Enemy soldiers can't loot you because there is no way for them to tell that you own Bitcoin.

What if Bitcoin had existed during the Nazi era? Schindler's List is a great movie that describes the plight of the Jewish people during the Holocaust. It shows how their physical wealth was taken from them illegally by people who had been brainwashed into believing that they were lesser and therefore did not deserve the same rights and benefits as their German countrymen. Many Jewish families lost generations' worth of wealth and had to start fresh in new countries. If Bitcoin had existed then, perhaps they could have converted their wealth to Bitcoin and been able to flee Germany more easily and transfer their wealth to start new lives in other countries.

The phenomenon of having to flee a place that has become hostile to you and your family still occurs on this planet. It is unlikely to go away soon. Ukraine is just the latest example, but there will likely be more in the near future. There is always a need to preserve wealth and transfer it without the ability for a government to illegally seize or restrict you. Bitcoin supports that need. Bitcoin has value because of its scarcity, but also because it solves a real human need.

How Does Bitcoin Work?

Bitcoin is a blockchain that uses a consensus mechanism called Proof of Work to ensure that

transactions are recorded correctly and that the record-keeping is immutable. We briefly touched on Proof of Work earlier, but now we will look at how exactly it creates a trustless system that can handle trillions in value transfer. The best way to do this is through a game.

The bitcoin game Illustrated

The aim of the game is for each person to make as much money as they can. The winner of the game is the one with the most money. You can make up the values or the currency as needed.

Step 1. Get each of the players a notepad, a smartphone, and a pen.

Step 2. Record transactions between the members of the group, on the notepad. The transactions should be spoken out loud.
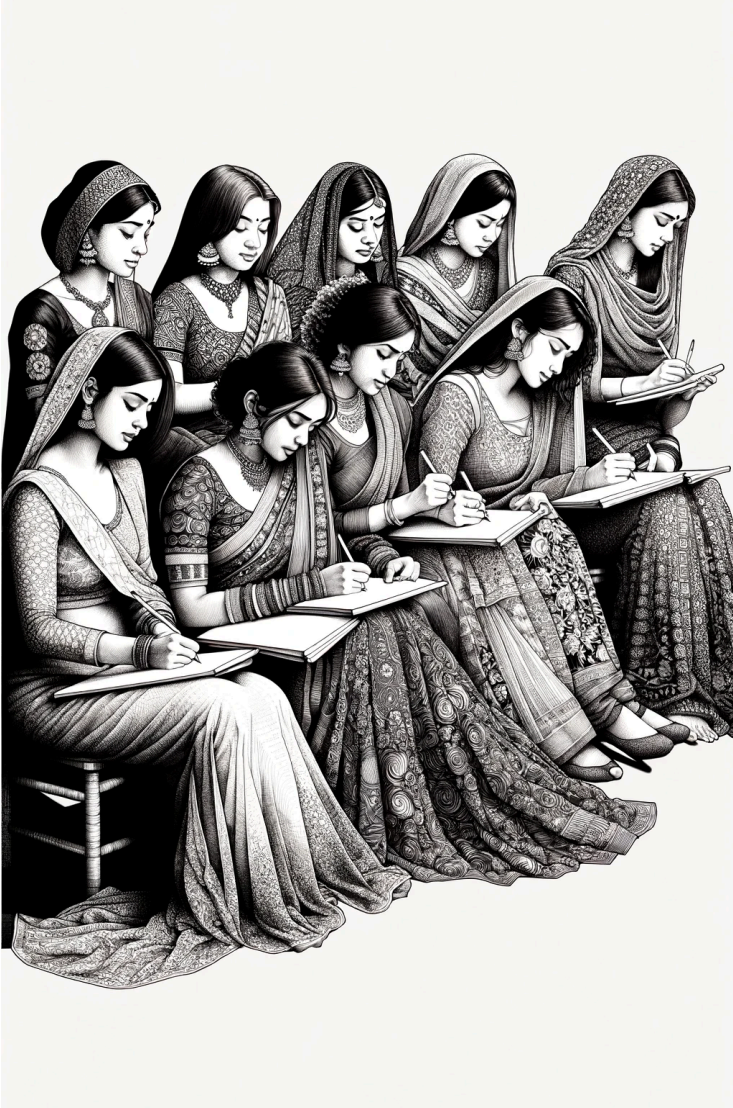
The transactions should look like this with small quantities. You can roll a dice if you like to decide how much someone gets.

Step 3. Calculate the Hash function. You can use an online SHA 256 function or use this simpler version.

- Take the first character of each transaction
- Keep adding the letters until you have at least 5 characters
- This is the fingerprint for this page or "block"
- Then multiply the numerical value of the letters together

Dimple ------> Kajal 1BTC
Ann ----> Sonal 5 BTC
Rupa ----> Sara 0·5 BTC
Seema ----> Roshan 0·3 BTC
Puri ----> Kajal 5 BTC

$D \times A \times R \times S \times P =$
$4 \times 1 \times 18 \times 19 \times 16 = 21888$

Step 4. Mine the block
- ● Divide the numerical value by 100000
- ● Then keep dividing that result using different random numbers, until the first three non zero characters are all even.
- ● The first one to get this number wins some amount of bitcoin

The first person to meet the criteria should reveal the result to the group, and each member of the group should check the result.

Step 5. If more than half of the others in the group agree that the result is correct, the block has been successfully minded. Now do this again one more time for the second block. Start the next block with a transaction granting the winner of the last block 3.125 Bitcoin, or whatever currency you choose to call it.

Now comes the fun part. To win the game you need to change the entries in either of the two blocks to have the money go to you instead of to the people in the transactions. You can do this at any time during any of the steps. But you have to somehow convince everyone else to also change their entries to match.

End of the game

At the end of the game someone will have the most amount of money. It will most likely be the ones who successfully won each block. The chances of it being someone who tried to get the group to change the transactions are low. This is very similar to how the BItcoin protocol ensures honest behavior.

7. Ethereum

For talented young wizards!

If you can imagine it, you can make it real. Just pay the miners their gas.

As we continue our exploration of the world of crypto, we move from Bitcoin, the original disruptor of traditional finance, to Ethereum—the platform that has expanded the possibilities of what blockchains can do. While Bitcoin laid the foundation by creating a decentralized, trustless system for storing wealth, Ethereum took this concept further by creating a global computer where code, like money, is immutable and trust is distributed.

In the first chapter, we discussed the cost of trust and how centralized systems often demand high prices—both literally and figuratively. Ethereum builds on Bitcoin's revolutionary approach to trust by offering a more versatile and potent system that doesn't rely on any centralized intermediaries. This makes Ethereum crucial to understand because it not only stores value but also enables complex interactions and applications to run securely without needing to trust any single entity.

To grasp Ethereum's significance, think of it as a magical world where spells—known as smart contracts—can perform incredible feats. In the Harry Potter universe, spells can do just about anything, from

levitating objects to summoning great power. Similarly, in the world of Ethereum, smart contracts can automate tasks, create new tokens, and even manage entire organizations, all without the need for a central authority.

The simplest and most common "spell" in Ethereum is the creation of tokens, thanks to the ERC-20 smart contract standard. This spell allows anyone to create their own cryptocurrency, often referred to as tokens. While some tokens represent real value and innovation, many have become what are known as "shitcoins," created with the sole purpose of duping unsuspecting investors out of their money. This duality shows the power and the risks of a decentralized system where anyone can create and share new forms of value.

In this chapter, we'll dive into the magic of Ethereum and how it works. We'll explore its origins, the concept of smart contracts, and the many powerful applications that have emerged from this platform—such as Decentralized Finance (DeFi), Non-Fungible Tokens (NFTs), and Decentralized Autonomous Organizations (DAOs). We'll also discuss Ethereum's evolution from Proof of Work to Proof of Stake, and what lies ahead for this groundbreaking network.

Understanding Ethereum is key to grasping the broader potential of blockchain technology. It represents the next step in building a global trust system, where trust is encoded into the very fabric of digital interactions, enabling a world of possibilities limited only by our imagination.

Ethereum's Origin and Transition

Ethereum's story begins with six founders, but the one who stands out the most is Vitalik Buterin. As the most prolific figure and the current face of Ethereum, Buterin has been instrumental in shaping much of the new "money lego" ecosystem being developed.

When Ethereum launched, I bought 100 ETH at around $1 each but unfortunately lost the keys a few months later. This serves as a cautionary tale about the importance of good key management.

A Brief History of Ethereum: 2013-2024

- **2013:** Vitalik Buterin introduces Ethereum through a white paper, conceptualizing the Ethereum Virtual Machine (EVM) and smart contracts. This marked the beginning of a new era in blockchain technology, enabling programmable applications beyond simple transactions.
- **2014:** Ethereum's Initial Coin Offering (ICO) raises $18 million, laying the groundwork for future blockchain projects. Notable founders include Buterin, Gavin Wood, and Joseph Lubin. The ICO format becomes a template for many subsequent blockchain projects, sparking a wave of innovation and investment.
- **2015:** The "Frontier" release of Ethereum launches on July 30th, marking the network's official launch. Developers begin building

decentralized applications (dApps) on the platform, showcasing its potential.

- **2016:** The DAO hack results in the theft of 3.6 million ETH, leading to a controversial hard fork to reverse the effects of the hack. This split creates two separate blockchains: Ethereum (ETH) and Ethereum Classic (ETC), highlighting the challenges of governance in decentralized systems.
- **2017:** The ICO boom sees unprecedented levels of funding and innovation. Projects like CryptoPunks introduce the concept of Non-Fungible Tokens (NFTs), laying the groundwork for the NFT explosion that would follow.
- **2018:** Decentralized exchange Uniswap launches, introducing Automated Market Makers (AMMs) and revolutionizing how digital assets are traded. Uniswap's success demonstrates the power of decentralized finance (DeFi) and sparks a wave of innovation in the space.
- **2020:** Ethereum begins its transition from Proof of Work (PoW) to Proof of Stake (PoS) with the launch of the Beacon Chain. This shift aims to reduce energy consumption and increase the network's scalability. The DeFi boom changes the global financial landscape, with Ethereum at its core.
- **2021:** Ethereum reaches new price highs and implements the London hard fork, which includes the EIP-1559 upgrade. This upgrade introduces a new fee structure, making ETH a deflationary asset and enhancing its economic model.

- **2022:** Despite a market crash caused by the collapse of Terra Luna and FTX, Ethereum solidifies its place in the crypto ecosystem. On September 15th, Ethereum successfully completes its transition to PoS, significantly reducing its energy consumption and marking a new era for the network.
- **2023:** The Shanghai upgrade enables stakers to withdraw previously locked ETH, enhancing the network's flexibility and accessibility. Despite market volatility, Ethereum's price continues to rise, demonstrating the network's resilience and ongoing innovation.

Ethereum's journey over the past decade showcases its resilience, innovation, and transformative impact on the crypto and global financial landscapes. From its early days of conceptualization by Vitalik Buterin to its current status as a leading platform for decentralized applications and financial services, Ethereum continues to push the boundaries of what's possible in the world of blockchain technology.

The Smart Contract

Imagine living in a world where, instead of casting spells with wands, you program smart contracts to perform tasks with digital precision and trust. In this scenario, Ethereum acts as your magical toolkit, enabling you to create and execute these digital spells effortlessly.

The Magic of Smart Contracts

Think of a smart contract as a magical scroll that, once activated, performs exactly as it's written. In the digital realm, a smart contract is a self-executing program where the terms of the agreement are embedded in lines of code. These contracts reside on the Ethereum blockchain, ensuring they are immutable (unchangeable) and transparent (visible to everyone). Like a spell cast from a scroll, a smart contract executes its instructions with precision, following the code it was programmed with.

The Spell of Token Creation

One of the most common and simplest spells in the Ethereum world is the ERC-20 smart contract. Imagine you have a scroll that can conjure new tokens out of thin air. This spell creates a new type of digital currency whenever it is activated. This is how many cryptocurrencies, often referred to as tokens or sometimes as "shitcoins," come into existence.

These tokens can represent a wide range of values. True believers in the Ethereum magic use these tokens

to represent real value, such as shares in a project, access to a special service, or even digital assets in games. However, just as there are charlatans in the world of magic, some people create tokens with the sole purpose of deceiving others, offering worthless tokens in exchange for real money.

The Power of Automation

Imagine having a magical box that only opens when a specific person approaches or when a particular time comes. Smart contracts can perform similar automated tasks. For instance, a smart contract can be programmed to release payment only when certain conditions are met, such as the delivery of goods or the completion of a project milestone.

This automation significantly reduces the need for trust between parties. Just as you trust the magical box to open only under the right conditions, you can trust a smart contract to execute its code accurately. This trustworthiness comes from the fact that the code is visible to everyone and cannot be altered once it is on the blockchain.

Immutability: The Unchanging Spell

Immutability is a core feature of smart contracts that adds to their reliability and trustworthiness. Once a smart contract is deployed on the Ethereum blockchain, it cannot be changed. This is like casting a spell that remains in effect forever, ensuring that the contract's terms will always be honored as originally written.

This immutability prevents tampering and fraud. Imagine a magical contract written on indestructible parchment. No one can alter the terms once it's in place, ensuring that all parties involved can trust the contract to behave exactly as expected. This permanence provides security and confidence, especially in complex transactions or agreements involving multiple parties.

Global Access: A Universal Spellbook

Ethereum operates on a decentralized network, providing global access to its magical capabilities. This means that anyone, anywhere in the world, can create, deploy, and interact with smart contracts. It's like having a universal spellbook that every wizard can use, regardless of their location.

This global access democratizes the power of smart contracts. Entrepreneurs in developing countries can access the same tools as those in tech hubs like Silicon Valley. It allows for innovation and collaboration on a worldwide scale, enabling anyone with an internet connection to participate in the digital economy. Imagine wizards from all corners of the world working together, sharing spells, and building new magical applications without geographical barriers.

Advanced Magical Applications

The possibilities of smart contracts extend far beyond simple token creation and conditional payments. These advanced applications demonstrate the true potential of Ethereum, showing how it can reshape entire industries and societal structures by embedding trust directly into the fabric of digital interactions.

Decentralized Finance (DeFi)

DeFi is like a magical bank that operates without a central authority. In this decentralized world, smart contracts enable borrowing, lending, and trading of assets directly between users, without the need for traditional banks or financial institutions. Imagine a world where you can borrow money using your digital assets as collateral, without ever stepping into a bank. Smart contracts automatically enforce the loan terms, reducing the need for intermediaries and lowering the cost of trust. This system not only democratizes access to financial services but also creates a more resilient and transparent financial ecosystem.

Non-Fungible Tokens (NFTs)

NFTs are unique digital assets, akin to one-of-a-kind magical artifacts. Each NFT is distinct, representing ownership of digital art, collectibles, or even virtual real estate. Smart contracts govern the creation, ownership, and transfer of these NFTs, ensuring their authenticity and rarity. In a world where digital content is easily duplicated, NFTs provide a way to create and verify the

uniqueness of digital items, offering creators and collectors a new form of value that is secure and verifiable. This shifts the cost of trust away from centralized platforms and places it directly within the hands of creators and consumers, enabling new forms of ownership and exchange.

Decentralized Autonomous Organizations (DAOs)

DAOs are like digital guilds or councils that operate based on pre-set rules encoded in smart contracts. Members of a DAO can vote on decisions, allocate resources, and manage projects collectively. The smart contract ensures that all actions are transparent and executed as per the agreed rules, providing a new way to organize and govern communities and businesses. DAOs represent a revolutionary approach to governance, where trust is not placed in a single leader or board but is distributed among all members. This decentralization of trust allows for more democratic decision-making processes, reducing the potential for corruption and mismanagement.

Proof of Work to Proof of Stake

We've learned how proof of work (PoW) is used to secure and create trust in the Bitcoin network. When Ethereum launched, it initially used a similar mechanism, which, while effective in maintaining security, also consumed vast amounts of energy. On September 15, 2022, Ethereum made a groundbreaking transition, known as "The Merge," where it switched

from proof of work to a proof of stake (PoS) mechanism, reducing its energy consumption by a staggering 99.5%.

Proof of Stake (PoS)

Proof of stake differs from proof of work in that it doesn't require expending vast amounts of energy to secure the network. Instead, validators—who are the equivalent of miners in PoS—are required to stake or bond 32 ETH to participate in the validation process. This staking serves as a security deposit that disincentivizes malicious behavior. If a validator acts dishonestly or fails to perform their duties, they stand to lose some or all of their staked ETH.

While there were several proof of stake chains in existence prior to Ethereum's transition, what made Ethereum's merge notable was that, for the first time ever, a major blockchain transitioned from proof of work to proof of stake without any downtime or losses, marking a significant milestone in the evolution of blockchain technology.

Let's dive a little deeper into how proof of stake works.

Before a new block is added to the blockchain, a committee of validators is randomly selected to decide what goes into the block. One member of this committee is chosen to put the block together, while the rest of the committee validates that the transactions included are correct. This process is crucial to ensuring the integrity and trustworthiness of the blockchain.

But how does the protocol ensure that the members of the committee are honest? The answer lies in the concept of staking. To be eligible to participate in the committee or to validate any transaction on the network, the node operator must stake 32 ETH. This means that they put this amount of ETH at risk, with the understanding that they could lose it if they act maliciously or fail to perform their duties.

A simple mental model to understand this is to compare it to owning an expensive car like a Ferrari or Lamborghini. In effect, every node operator is putting something of great value—akin to a Ferrari—on the line. They are essentially saying, "If I misbehave, the protocol can punch a hole in my car." Would you misbehave if your precious Ferrari was at risk of being damaged?

This shift from proof of work to proof of stake represents a significant reduction in the cost of trust for the Ethereum network. By moving away from energy-intensive processes to a system where validators are economically incentivized to act honestly, Ethereum has not only reduced its environmental impact but also made the process of maintaining trust more efficient and scalable.

For future society builders, understanding the implications of this transition is crucial. Proof of stake showcases how trust can be maintained through economic incentives rather than brute computational power, paving the way for more sustainable and inclusive blockchain networks. This evolution reflects a broader trend in technology—finding smarter, more

efficient ways to build systems that are secure, trustworthy, and accessible to everyone.

Where is Ethereum Heading?

Ethereum is not yet the base layer of trust on the internet, but it is steadily moving toward that goal. To get there, Ethereum must undergo several more upgrades. As it evolves, the way it operates will continue to change, creating new opportunities for technologies, innovations, and businesses that build on top of it.

One of the biggest changes coming to Ethereum in the near future is the move to something called Proto-Danksharding. This upgrade is expected to significantly enhance Ethereum's scalability, allowing it to process over 100,000 transactions per second, compared to the current capacity of around 15 transactions per second. For comparison, Visa processes approximately 1,700 transactions per second. This leap in capacity would position Ethereum as a serious contender for handling global-scale financial and non-financial transactions.

Currently, transaction fees on Ethereum can be prohibitively expensive, especially during times of high network usage. However, future upgrades are expected to drastically reduce these fees to less than $0.001 per transaction. Lower fees combined with higher transaction volumes will improve the economics for businesses operating on Ethereum, making it a more attractive platform for a wide range of applications.

These upgrades, aimed at increasing transaction volumes and lowering fees, are expected to take place within the next two years. However, the Ethereum roadmap also looks further ahead, contemplating what Ethereum might become beyond this period.

In several talks, Vitalik Buterin, Ethereum's co-founder, has discussed various possibilities for the network's future. Many of these involve "outsourcing" certain tasks away from the core network. For instance, currently, the Ethereum blockchain contains all transactions since its inception, which means that maintaining the network requires significant storage capacity from participants. One proposal for Ethereum's future state is to incentivize service providers to store historical data, allowing the main network to maintain only 2-3 years' worth of information at a time. This could create new business models focused on archiving old data, further expanding Ethereum's ecosystem.

Future upgrades will primarily focus on making Ethereum even more efficient and aiming for a state where it will no longer require significant changes for 10-20 years. This is important because each time Ethereum is upgraded, trillions of dollars are affected, and businesses built on Ethereum need to expend significant technical resources to ensure their systems are ready for the change. For Ethereum to truly become the base layer of trust, it will need to offer stability in a rapidly changing world.

But what does it mean for Ethereum to be the trust layer of the internet? Because Ethereum is highly decentralized, it is extremely unlikely that malicious

actors can corrupt the information processed by the network. This level of security allows the network to serve as a source of trust between large numbers of anonymous individuals and entities interacting online. Businesses can "borrow" this trust from the network, enabling them to perform high-value transactions and activities without needing the long periods of time typically required to build trustworthy relationships.

As the base layer of trust, Ethereum has the potential to strengthen global collaboration in ways previously unimaginable. This could empower humanity to address some of its most pressing challenges, such as climate change, poverty, and even the goal of becoming a multi-planetary species.

Restaking

Restaking is a recent innovation in the Ethereum ecosystem, pioneered by Sreeram Kannan. As of the writing of this book, it has not yet been implemented, but it promises to radically transform the domains of innovation within Ethereum.

At its core, staking in Ethereum accomplishes two primary objectives. First, it allows stakers to earn additional rewards by reusing their "security guarantee" to secure other services that applications might need. Second, it enables new applications to be decentralized from day one by borrowing trust directly from the Ethereum network.

Let's revisit our car analogy to explain this concept. Imagine you are applying for a critical job managing the cash register at a fashion store. To help your friend get this job and ensure that his peers trust him, you offer your Ferrari as collateral. You tell the store owner, "If my friend behaves maliciously, you can have my Ferrari." Since the value of the money in the register is far less than the Ferrari, the store owner is likely to trust you.

Now, let's say you're also asked to take on a short project with an accounting firm, but they need assurance that you won't manipulate the books. You can use the same Ferrari as collateral, telling the firm, "If I misbehave, you get the Ferrari." You can continue making similar offers for any other task requiring trust, effectively reusing the value locked in the Ferrari to guarantee your trustworthiness.

However, just as with the Ferrari, there are limits to how much you can restake. At some point, the reuse of this collateral could get you into trouble. After all, how many people can you make the same promise to—10, 100, 1,000? This concern is similar to those expressed with Eigenlayer, a protocol that enables restaking, and the Ethereum community is still evaluating the security implications of this approach.

Restaking represents a new frontier in the Ethereum ecosystem, offering a powerful tool for decentralization and trust. It reduces the cost of trust by allowing existing staked assets to be leveraged across multiple applications, creating new opportunities for innovation. However, it also introduces new risks, as the overuse of

staked collateral could potentially compromise the security of the network.

For future society builders, restaking offers both a cautionary tale and a powerful opportunity. It underscores the need to carefully balance innovation with security, especially when it comes to building systems of trust that millions of people will rely on. As Ethereum continues to evolve, restaking may become a critical component of its ecosystem, enabling the creation of more robust and decentralized applications while pushing the boundaries of what's possible in the world of blockchain technology.

Part 3: What if I want to get a bit more advanced?

8. Tokens

Let there be tokens!

Basic crypto spells for the new and uninitiated.

You've probably heard a lot about tokens. In fact, most of the coins listed on exchanges are tokens. But it's important to note that not all digital assets are the same—ETH and BTC, for example, are not tokens.

So what's the difference between a token and a cryptocurrency? To understand this, let's build on the concept of trust that has been central to our discussion. In the first chapter, we explored how trust is a foundational element in both traditional and digital systems. As we moved into the world of crypto, we saw how Bitcoin and Ethereum established new trust mechanisms without relying on centralized intermediaries. Tokens represent another layer in this evolving landscape, offering new ways to represent value and manage digital interactions.

Tokens are typically created on platforms like Ethereum, which has its own native cryptocurrency, ETH. While ETH is a cryptocurrency, tokens can also function as a currency within their respective ecosystems, enabling value transfer and transactions in decentralized
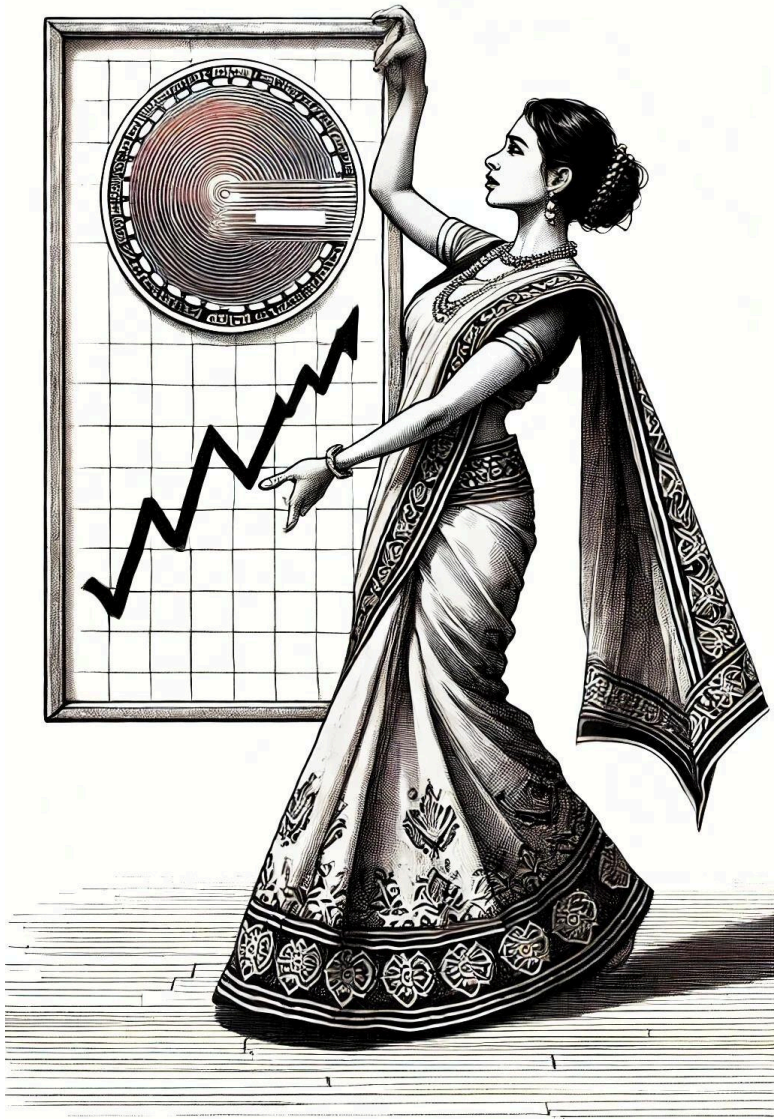
protocols. For example, utility tokens like the T token, which can be staked on the Threshold Network, serve specific purposes within that network. However, the key distinction most in the ecosystem agree on is this: cryptocurrencies are native to their blockchain protocols, while tokens are built on top of these protocols.

To visualize this, imagine that a cryptocurrency like ETH is the foundation or the core spell in a wizard's toolkit. Tokens, on the other hand, are like specialized spells created using that core magic, each designed for a particular purpose within the broader magical framework.

In this chapter, we'll delve into the world of tokens, exploring the different types—utility, governance, and security tokens—and their specific roles within blockchain ecosystems. We'll also examine the economic principles behind tokens, such as how supply and demand dynamics influence tokenomics, and how inflation and deflation can impact the value of tokens over time.

Understanding tokens is essential because they add another layer of complexity and flexibility to the blockchain world, allowing for more advanced applications and interactions. Just as trust in Bitcoin and Ethereum allows for secure value exchange, tokens extend this trust by enabling more nuanced and specialized functions within decentralized networks. This chapter will guide you through the basics, helping you grasp the various functions and potential of tokens, and how they play a crucial role in the broader context of trust and value in decentralized systems.

Token Types - Utility, Governance, and Security Tokens

Token ecosystems are innovating constantly, but over the last few years, tokens have emerged that can broadly be categorized into Utility, Governance, and Security tokens, with some even categorized as commodities. The technical application of tokens and their legal definitions are still evolving. In particular, the legal world is grappling with creating an effective mental model to categorize tokens within existing frameworks.

Because this technology is fundamentally different from most legal precedents, legal systems worldwide—many of which are still based on rules from the era of wooden ships—are struggling to classify tokens and crypto in general. Despite these challenges, understanding the types of tokens and how they are valued is crucial for anyone looking to engage more deeply in the crypto space.

Let's explore each type of token in detail:

Utility Tokens

Utility tokens are essential for some function of a decentralized system. Think of oil, which is necessary for a car to function, providing the energy to run the engine and other systems. Oil has value because it is needed for the functioning of automobiles, planes, plastics, etc. Similarly, utility tokens are like oil in a decentralized ecosystem—they are needed for the

system to function, which creates demand and gives them value.

Staking tokens are a prime example of utility tokens. For instance, Ethereum's ETH and Threshold Network's T token must be staked to secure their respective networks and prevent malicious behavior within decentralized consensus systems (as discussed in the chapter on Ethereum). Without these tokens, the security of the system would be severely compromised. In Ethereum's case, ETH also functions like oil, as it is used to pay for transactions on the network.

However, utility tokens have limited legal recognition. Unless it is very clear that a token is a necessary part of a decentralized system, it won't be recognized as a utility token by legal authorities. This distinction is important as it affects how these tokens are regulated and used in the broader financial system.

Governance Tokens

Governance tokens are used primarily in Decentralized Autonomous Organizations (DAOs) to enable owners to participate in the governance of a decentralized system. DAOs, which are covered in more detail in a later chapter, use governance tokens to give holders the right to vote on proposals and make decisions about the direction of the organization. In many systems, the number of tokens owned directly correlates with voting power, meaning more tokens often equal more influence.

Like utility tokens, governance tokens also have limited legal recognition. For a token to be legally categorized as a governance token, its value must primarily come from the right to govern the system. However, because governance tokens are still relatively new, there are not many laws or regulations governing their use, leaving their legal status in a gray area.

Security Tokens and the Howey Test

Most legal systems, particularly the U.S. Securities and Exchange Commission (SEC), consider most tokens to be securities. A security is a financial instrument that promises to earn you revenue simply by owning it. The SEC uses the Howey test to determine whether a particular asset qualifies as a security.

The Howey test consists of three parts, all of which must be true for something to be considered a security:

1. **Investment of Money:** There must be an investment of money, meaning the individual must contribute funds, assets, or capital to a common enterprise.
2. **Expectation of Profit:** The investment must be made with the expectation of earning a profit. This implies that the investor is looking to gain from the efforts of others, primarily the promoter or the issuer of the investment.
3. **Common Enterprise:** The profit must come from the efforts of others, typically the promoter or third parties associated with the investment. In other words, the success of the investment is

largely dependent on the managerial or entrepreneurial efforts of those responsible for the investment.

If all three parts of the Howey test are met, the investment is classified as a security, falling under the regulatory purview of the SEC. This classification is crucial because it triggers various legal and regulatory requirements designed to protect investors and ensure fair and transparent markets.

The application of the Howey test is not limited to traditional financial instruments like stocks and bonds. The test has also been used to determine whether certain cryptocurrencies and tokens fall under the definition of securities, leading to potential regulatory implications for issuers and investors in the United States.

Token economics

Where does token value come from? Tokenomics is the study of the economic models and mechanisms that govern the creation, distribution, and management of tokens within a blockchain ecosystem. The primary goal of tokenomics is to increase the value of the token through various methods, with a strong emphasis on enhancing its utility. By providing tangible use cases such as facilitating transactions, enabling access to services, and driving decentralized applications (dApps), tokens can gain intrinsic value. Staking is a primary method of generating token value, where participants lock up their tokens to secure the network and earn rewards, thus reinforcing the token's economic model and encouraging its broader adoption.

Inflation and Deflation Dynamics

Tokens can be either inflationary or deflationary, each impacting their value in distinct ways.

Inflationary Tokens: An inflationary token increases its supply over time. This is common in networks where new tokens are created as rewards for miners or validators, such as Bitcoin. While this can incentivize participation and security, it can also lead to a dilution of value if the increase in supply outpaces demand.

Deflationary Tokens: A deflationary token decreases its supply over time through mechanisms like burning, where tokens are permanently removed from circulation. This reduction in supply creates scarcity, which can increase the token's value, assuming demand remains

steady or grows. Ethereum, for instance, was deflationary following its upgrade known as "the merge," where more tokens were burned than created, enhancing its scarcity and potential value.

Ethereum's Transition: Previously, Ethereum was deflationary, with the total supply decreasing yearly, creating scarcity and potentially driving up the price due to increased demand. However, Ethereum is no longer deflationary, meaning its supply is more stable or slightly increasing. This shift alters its economic dynamics, making other factors like utility and demand growth more critical in determining its value.

Bitcoin's Inflationary Nature: Bitcoin follows a predictable inflationary model where new bitcoins are introduced to the market through mining rewards. However, Bitcoin's inflation rate decreases over time through a mechanism called "halving," which occurs approximately every four years, cutting the reward for mining new blocks in half. This controlled inflation, combined with a capped total supply of 21 million bitcoins, creates a unique economic model. Despite being inflationary in the short term, Bitcoin is deflationary in the long run due to its maximum supply cap. As the total supply approaches this cap and the rate of new supply decreases, Bitcoin becomes increasingly scarce, enhancing its value proposition as a store of value, akin to digital gold.

In both models, the balance between supply and demand is crucial. Inflationary models rely on demand growth to absorb the increasing supply, while

deflationary models leverage scarcity to maintain or boost value. Understanding these dynamics helps in assessing the long-term potential and stability of a token's value.
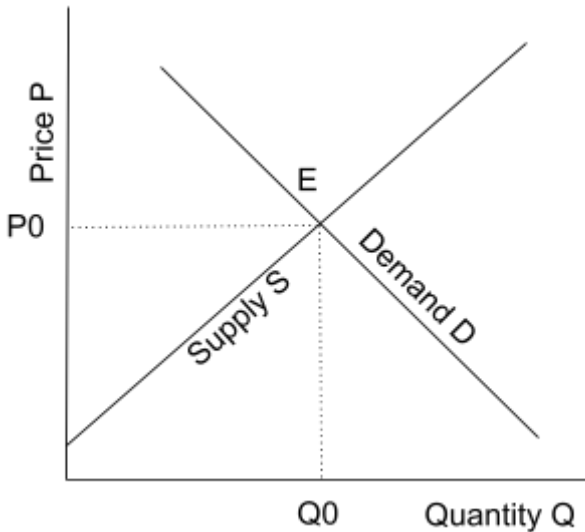
Supply and Demand Curve in Tokenomics

The supply and demand curve is a fundamental concept in economics that also applies to tokenomics, illustrating how the price of a token is determined by the interaction between supply and demand.

Basic Supply and Demand Model
In the basic supply and demand model:

Demand Curve (D): This downward-sloping line represents the relationship between the price of the token and the quantity demanded by consumers. As the price decreases, the quantity demanded increases, and vice versa.

Supply Curve (S): This upward-sloping line represents the relationship between the price of the token and the quantity supplied by producers. As the price increases, the quantity supplied increases, and vice versa.

Equilibrium (E): The point where the supply and demand curves intersect is the equilibrium price and quantity. At this point, the quantity of tokens demanded by consumers equals the quantity of tokens supplied by producers.

Application to Tokenomics

Demand Increase: When the demand for a token increases, perhaps due to greater utility, more applications, or broader adoption, the demand curve shifts to the right (D0 to D1). This shift results in a higher equilibrium price (from P0 to P1) and a higher equilibrium quantity (from Q0 to Q1). For example, if a new decentralized application (dApp) built on Ethereum becomes popular, the demand for ETH may rise, shifting the demand curve to the right.

Supply Decrease: If the supply of a token decreases, such as through token burning or a reduction in mining rewards, the supply curve shifts to the left (S to S1). This shift also results in a higher equilibrium price and a

lower equilibrium quantity. For example, when Ethereum was deflationary, more ETH was burned than created, shifting the supply curve leftward and increasing the token's price.

Combined Effect: If both demand increases and supply decreases, the combined effect amplifies the increase in price. For instance, if Ethereum experiences higher demand due to increased network usage and simultaneously reduces its supply through burning mechanisms, the price of ETH can rise significantly.

Specific Examples

Bitcoin: Bitcoin's inflationary model currently increases supply through mining rewards. However, due to the fixed maximum cap of 21 million bitcoins, the supply will eventually stabilize, making Bitcoin deflationary in the long run. As the supply of new bitcoins decreases over time (due to halving events), the supply curve shifts leftward, potentially increasing Bitcoin's price if demand remains steady or grows.

Ethereum: Ethereum's transition from a deflationary model has stabilized its supply. The token's value now relies more on demand growth, driven by utility in decentralized finance (DeFi), non-fungible tokens (NFTs), and other blockchain applications. As demand for these applications increases, the demand curve shifts rightward, raising the equilibrium price.
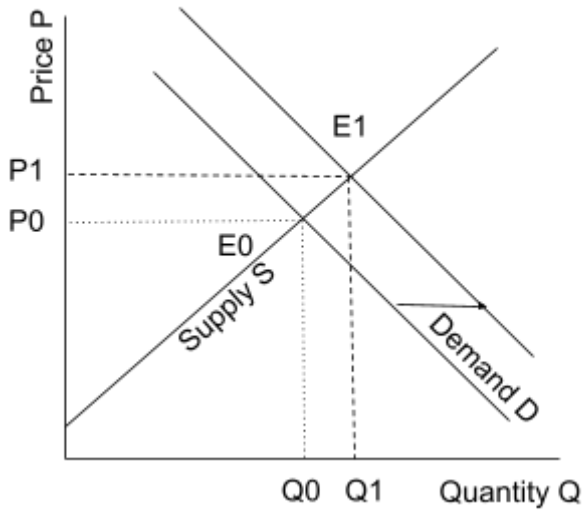
Demand Shift Right

When demand for a token increases, perhaps due to factors such as greater utility, more applications, or broader adoption, the demand curve shifts to the right from D1 to D2. This shift represents an increase in the quantity of tokens demanded at every price level.

New Equilibrium

New Equilibrium Price (P1): After the demand shift, the new equilibrium price is higher than the initial equilibrium price. This occurs at the intersection of the new demand curve D2 and the supply curve S.

New Equilibrium Quantity (Q2): The new equilibrium quantity is higher than the initial equilibrium quantity, reflecting the increased quantity of tokens demanded.

Example in Tokenomics

In the context of tokenomics, an increase in demand can occur for several reasons:

Increased Utility: As more applications are built on a blockchain platform, the utility of the native token increases. For instance, if new decentralized applications (dApps) are developed on Ethereum, the demand for ETH may rise, causing a rightward shift in the demand curve.

Broader Adoption: Increased adoption of the token for transactions, smart contracts, and other blockchain activities can drive demand. More users and developers participating in the ecosystem create greater demand for the token.

Market Sentiment: Positive market sentiment and speculation can also drive demand. News of technological advancements, partnerships, or regulatory approvals can lead to increased interest and demand for a token.

Network Effects: As the network grows, the token's value can increase due to network effects. More users and applications on the network can lead to higher demand for the token.

Implications

The rightward shift in the demand curve leads to a higher equilibrium price and quantity, reflecting increased value and demand for the token. This increase in demand and the resulting higher price can be beneficial for token holders and the overall network, as it may attract more participants and further drive adoption.
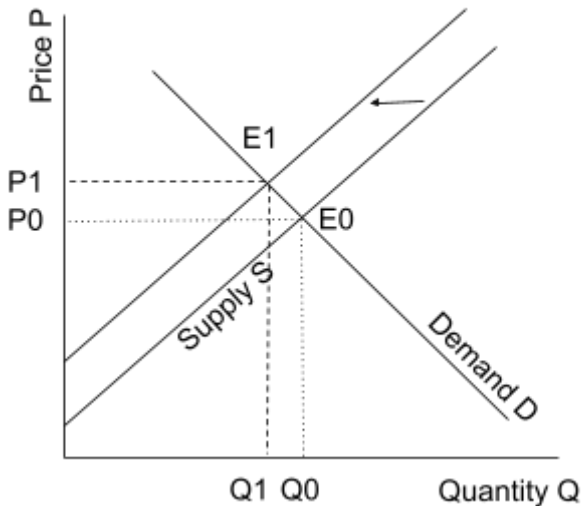
Supply Shift Left

When the supply of a token decreases, perhaps due to mechanisms such as token burning, reduced mining rewards, or other supply-limiting actions, the supply curve shifts to the left from S to S1. This shift represents

a decrease in the quantity of tokens supplied at every price level.

New Equilibrium

New Equilibrium Price (P1): After the supply shift, the new equilibrium price is higher than the initial equilibrium price. This occurs at the intersection of the new supply curve S1 and the demand curve D1.

New Equilibrium Quantity (Q1): The new equilibrium quantity is lower than the initial equilibrium quantity, reflecting the decreased quantity of tokens supplied.

Example in Tokenomics

In the context of tokenomics, a decrease in supply can occur for several reasons:

Token Burning: Reducing the number of tokens in circulation by permanently removing them can decrease supply. For example, if a blockchain protocol implements a burning mechanism that destroys tokens during transactions, the supply curve shifts leftward.

Reduction in Mining Rewards: Lowering the rewards for miners or validators can reduce the rate at which new tokens are introduced into the ecosystem. Bitcoin's halving events are a prime example, where the reward for mining new blocks is cut in half, reducing the growth of the supply.

Supply-Limiting Protocols: Some blockchain protocols may have built-in mechanisms to limit supply growth,

such as capping the total number of tokens that can ever exist. This ensures that the supply does not increase indefinitely.

Staking and Locking Mechanisms: Tokens locked in staking or other financial mechanisms reduce the circulating supply, effectively shifting the supply curve leftward.

Implications

The leftward shift in the supply curve leads to a higher equilibrium price and a lower equilibrium quantity. This reflects the increased scarcity of the token, which can drive up its value. For token holders, a reduced supply can enhance the value of their holdings, assuming demand remains constant or increases.

9. Decentralized Finance

Zindagi Na Milegi Dobara!

Less time on money, more time for life.

Maybe DeFi can help us get there?

As we journey further into the world of crypto, we arrive at Decentralized Finance, or DeFi—one of the most transformative aspects of blockchain technology. DeFi has the potential to completely change how we interact with financial systems by reducing our reliance on intermediaries and making financial services accessible to everyone. But to understand why DeFi is so important, we need to revisit a concept we discussed in the first chapter: the cost of trust.

In traditional finance, trust is expensive. We rely on banks, brokers, and other financial institutions to manage our money and ensure that transactions are fair and secure. But this trust comes with a price. The 2008 financial crisis is a stark example of this. Information asymmetry—where one group knows more than another—allowed financial institutions to exploit their position, leading to disastrous consequences for the global economy. The movie *Margin Call* vividly depicts how a firm's early knowledge of an impending collapse allowed it to offload toxic assets, minimizing its own losses while triggering a broader market crash.

This scenario highlights the high cost of trust in centralized systems: we place our trust in institutions that may not always act in our best interests, and when they fail, the consequences can be catastrophic. The first block of Bitcoin's blockchain, with its reference to a government bailout of banks, is a direct response to these failures, marking the beginning of a new approach to trust and financial systems.

DeFi aims to reduce this cost of trust by eliminating intermediaries and bringing transparency to financial transactions. In a DeFi system, all financial assets and actions are visible on the blockchain, accessible to everyone. This transparency reduces information asymmetry, making it harder for any one group to exploit their position. By doing so, DeFi creates a more trustworthy financial environment where bad behavior is less likely to go unchecked.

But DeFi's impact goes beyond just lowering the cost of trust. It democratizes finance, allowing anyone with an internet connection to create and participate in financial products and services. Just as the internet transformed content creation—enabling anyone to start a blog, publish a magazine, or stream video content—DeFi is poised to do the same for finance. No longer do you need a large institution to innovate in finance; DeFi opens the door for financial creativity on a global scale.

In this chapter, we'll explore the core components of DeFi, beginning with stablecoins, which provide a bridge between traditional finance and the decentralized world. We'll then examine the different types of stablecoins—fiat-backed, crypto-backed, and

algorithmic—and how they operate within the DeFi ecosystem. We'll also look at decentralized lending and borrowing platforms, and the role of decentralized exchanges in reshaping financial markets.

Understanding DeFi is crucial because it represents the next step in reducing the cost of trust in financial systems. By removing intermediaries and making finance more transparent and accessible, DeFi is not just changing how we manage money—it's paving the way for a future where we can spend less time worrying about financial systems and more time living our lives.
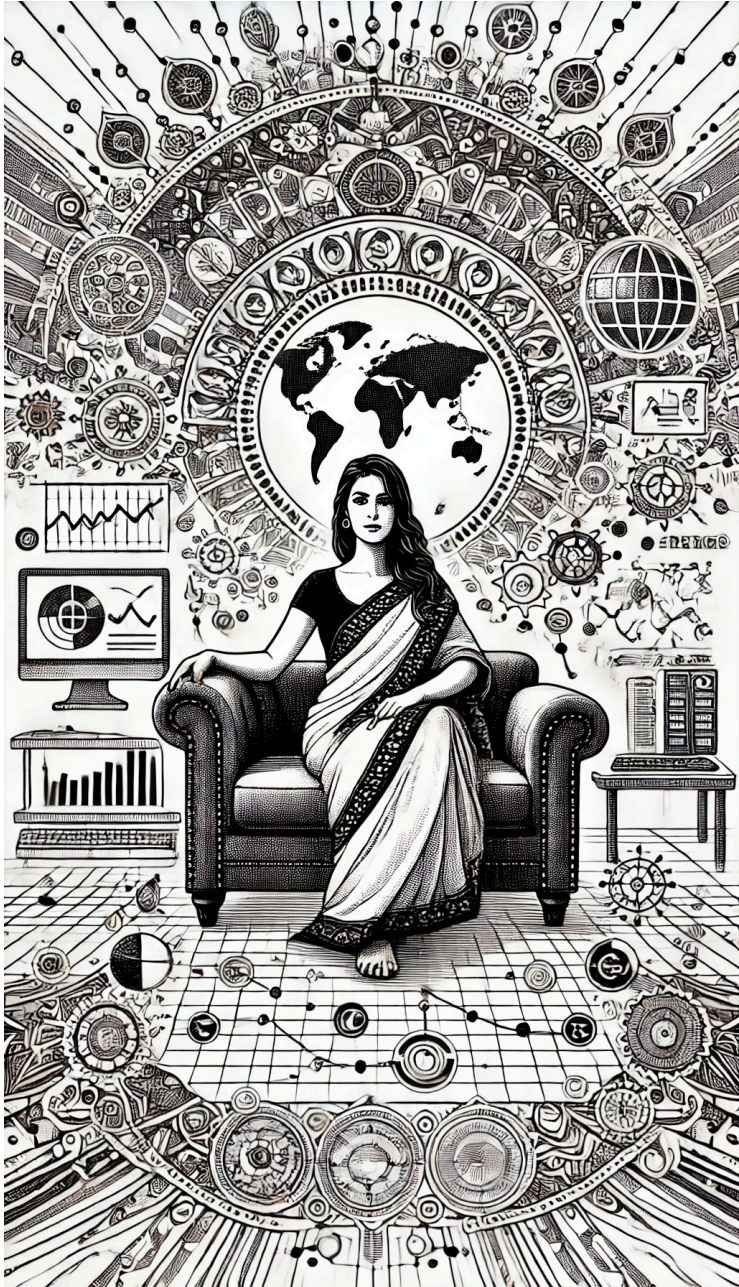
Stable Coins

The crypto ecosystem is known for its volatility—something that is no secret to anyone. But in a world where stability is essential, especially when it comes to financial transactions, how can people rely on a currency that fluctuates wildly? This is where stablecoins come into play. As the name suggests, stablecoins are designed to offer stability, providing a reliable store of value within the often tumultuous crypto markets. USDT, for example, is one of the largest stablecoins and is built on the Ethereum platform. It maintains its stability because it is backed by actual U.S. dollars.

Stablecoins can be categorized into three main types: fiat-backed, crypto-backed, and algorithmic. Understanding these types and how they function within the DeFi ecosystem is crucial for anyone looking to navigate the world of decentralized finance effectively.

Fiat-Backed Stablecoins

Fiat-backed stablecoins are considered the safest assets on blockchains because they are backed one-to-one by actual fiat currency, ensuring they maintain their peg. USDT and USDC, both Ethereum-based stablecoins, are the oldest and most widely used. The value of 1 USDT or USDC has consistently stayed close to 1 USD, even surviving multiple market crashes and downturns. These stablecoins are often seen as lifeboats in the crypto ecosystem, providing a stable refuge during crises.

Popular Fiat-Backed Tokens:

- **USDC:** USDC is a stablecoin fully backed by U.S. dollars held in reserve, and its value remains pegged to the USD. It is known for its transparency and regular audits, which enhance its trustworthiness in the market.
- **USDT:** USDT, or Tether, is another widely used fiat-backed stablecoin, designed to mirror the value of the U.S. dollar. Despite some controversies regarding its reserves, it remains a dominant force in the stablecoin market due to its liquidity and widespread acceptance.

Understanding fiat-backed stablecoins is essential for participants in the crypto ecosystem, as they serve as a reliable anchor during market turbulence. USDT and USDC, in particular, have proven their stability and trustworthiness across multiple crises, including the Terra Luna crash, which we will discuss more in the algorithmic stablecoin section.

Crypto-Backed Stablecoins

Crypto-backed stablecoins like DAI are innovative digital currencies that maintain a stable value relative to fiat currencies while being collateralized by cryptocurrencies such as ETH, USDC, and WBTC. Unlike fiat-backed stablecoins, which rely on traditional currency reserves, crypto-backed stablecoins operate through decentralized ecosystems. These systems use smart contracts to manage collateral, requiring over-collateralization to cushion against the volatility of

the underlying assets, ensuring the stablecoin's value remains near its target price.

However, the inherent volatility of the collateral assets introduces significant risks. If the value of these assets drops sharply, the stablecoin system may face a deleveraging spiral, where forced liquidations put further downward pressure on collateral prices, potentially destabilizing the stablecoin. Additionally, in extreme market conditions, the liquidity of these assets could dry up, making it difficult to maintain the stablecoin's peg and eroding user confidence.

Despite these risks, crypto-backed stablecoins have the potential to become more trustworthy as their ecosystems mature. Diversifying collateral bases, implementing advanced risk management mechanisms, and benefiting from a maturing crypto market could enhance stability. Moreover, the transparency and decentralized governance offered by these stablecoins may foster greater trust compared to their fiat-backed counterparts.

Algorithmic Stablecoins

On the riskier end of the spectrum are algorithmic stablecoins, whose value is determined by supply and demand, with incentive mechanisms designed to maintain a peg to a fiat currency. However, these mechanisms can unravel quickly, leading to catastrophic failures. A notable example is the collapse of the Terra Luna ecosystem. TerraUSD (UST), the algorithmic stablecoin of the Terra network, lost its peg in May 2022

when a large amount of UST was suddenly sold, leading to a rapid devaluation. As panic ensued, UST's value plummeted, and the interconnectedness with Terra's native coin, Luna, caused the entire ecosystem to collapse, resulting in a loss of $60 billion in less than a month.

The Terra Luna disaster highlights the inherent risks of algorithmic stablecoins, which rely on market dynamics and confidence to maintain stability. When confidence erodes, these systems can enter a death spiral, as seen with UST and Luna. This event, among others, has shown that algorithmic stablecoins are currently the most precarious form of stablecoins, with a history of failures that underscore the challenges of maintaining stability in a decentralized, algorithm-driven system.

In contrast to crypto-backed stablecoins, which might gain trust as their ecosystems mature, algorithmic stablecoins have generally struggled to achieve long-term stability. The repeated failures in this space emphasize the need for caution and robust design when attempting to create stable value through purely algorithmic means.

Decentralized Lending and Borrowing

Yes, just like in the traditional financial system, you can lend out your crypto or take crypto loans. While this is still a developing space, most people currently use it for DeFi purposes. However, applications are emerging that allow you to borrow crypto for real-world uses, such as buying a house or a car.

Compound Finance and **AAVE** are two of the most notable services in the crypto ecosystem that facilitate decentralized lending and borrowing. As long as your crypto exists on the Ethereum network, you can lend or borrow it through these platforms. What makes these platforms unique is their decentralized nature—there is no central company or individual controlling them. Instead, they rely on the community to decide how they operate, making them true examples of decentralized finance.

Compound, for instance, is a decentralized lending protocol that operates through transparent smart contracts visible to the community and its users. This transparency is a stark contrast to traditional banks, where the inner workings of loan processes and asset management are often opaque. On Compound, every user can track how assets are being lent out, ensuring that trust is built through transparency rather than reliance on a central authority.

However, the journey of decentralized lending and borrowing has not been without challenges. There have been several attempts to attack these protocols. Some of the notable attacks include flash loan exploits and other vulnerabilities that have been exploited by hackers. These incidents have tested the resilience of DeFi protocols, highlighting both their strengths and weaknesses.

As AAVE founder and CEO Stani Kulechov noted in an interview with Decrypt, "DeFi protocols are being battle-tested, and it highlights how communities can implement new parameters to enhance risk mitigation

factors in volatile market environments that are moving fast. It's been fascinating to watch the DeFi community discuss, propose, vote, and implement new parameters—with incredible transparency—to adapt and safeguard the protocol. This is what DeFi is all about."[53]

These attacks and the community's response underscore the evolving nature of trust within the DeFi ecosystem. Unlike traditional financial institutions that might rely on opaque decision-making processes, DeFi platforms like AAVE and Compound are proving that trust can be built and maintained through transparency, community governance, and rapid adaptation to new challenges.

As we continue to explore the world of DeFi, it's essential to understand that decentralized lending and borrowing are more than just financial services—they represent a shift in how we think about trust, control, and the democratization of finance. For future society builders, these platforms offer a glimpse into a world where financial services are accessible, transparent, and governed by the people who use them, rather than by centralized institutions.

---

[53] *DeFi Giants Aave, Compound Freeze Markets and Cap Loans to Mitigate Risks - AICoin*. https://www.aicoin.com/en/article/325083. Accessed 18 Aug. 2024.

10. NFTs

Can a picture be worth a thousand dollars?

Maybe, but definitely not always. Art world rules still apply.

As we continue exploring the advanced aspects of the crypto world, we arrive at NFTs—Non-Fungible Tokens. NFTs have sparked both fascination and controversy, especially with the idea that a digital image could be worth thousands or even millions of dollars. But to understand NFTs and their value, we need to return to a concept we've discussed throughout this book: **trust**.

In the art world, trust plays a crucial role in determining value. What makes the Mona Lisa priceless? Some might argue it's the uniqueness of the piece and the story surrounding it. Art becomes valuable not just because of its aesthetic appeal but because of its rarity, provenance, and the trust that these factors inspire in collectors and the public. This is where NFTs come into play—by providing verifiable uniqueness.

NFTs stand for Non-Fungible Tokens, which simply means they are unique digital assets. "Non-fungible" means that each token is one-of-a-kind and not interchangeable with another. For instance, a valuable

painting like the Mona Lisa is non-fungible because it can't be exactly replicated or replaced. On the other hand, fungible assets like gold bars or Bitcoin are interchangeable—one is exactly the same as another of the same weight or value.

In the digital world, it's easy to destroy uniqueness. A digital image or file can be copied and pasted endlessly, making it difficult to maintain any sense of originality or rarity. However, the blockchain, the technology underlying NFTs, can restore this lost uniqueness by creating a unique ID for each digital item. This allows ownership and provenance to be traced, ensuring that each digital asset is truly unique.

This concept of "verifiable uniqueness" is what NFTs bring to the art world. You can verify that a digital item is unique, and you can verify who owns it. This has solved a significant problem for digital art, but it doesn't change the fact that the other factors that make art valuable—like the artist's reputation, the piece's history, and its cultural significance—still apply.

One of the misconceptions that has arisen with the advent of NFTs is the belief that simply turning a piece of art into an NFT automatically increases its value. While this worked for a few projects early on, the reality is that the traditional factors that determine art's value are far more important than the NFT-ification process. The market has shown that not all NFTs are valuable, and many have been used in scams, preying on the excitement and lack of understanding among new investors.

Later in this chapter, we'll explore how successful NFT projects address these traditional questions of value and how they leverage the concept of verifiable uniqueness.

This chapter will guide you through the world of NFTs, including the different types of NFTs on Ethereum and Bitcoin, and some essential rules for creating or investing in NFTs. As we dive deeper, it's important to remember that while NFTs bring a new dimension to digital ownership, they are not a guarantee of value. Trust, as always, remains a critical component in determining what is truly valuable.

Ethereum NFTs

NFTs were an innovation of the Ethereum ecosystem, made possible through a specific type of smart contract known as **ERC-721**. While the technical intricacies of how this contract functions are complex and beyond the scope of a basic introduction, the key takeaway is that ERC-721 allows for the easy creation, or "minting," of NFTs using a standardized smart contract.

But here's something important to understand: the ERC-721 contract itself does not contain the art or digital work that is being turned into an NFT. Instead, it points to data stored elsewhere, associating that data with a unique ID on the blockchain. In essence, an NFT is simply a record on the blockchain that links some external information with a unique ID. This is the foundation of what makes NFTs work, but it's not what gives them value.

The value of an NFT, like any other piece of art, depends on a variety of factors: the reputation of the artist, the significance of the work, its rarity, and the story behind it. These are the same elements that determine the value of physical artworks, and they are equally applicable in the digital world of NFTs.

Semi-Fungibility and ERC-1155

A relatively new concept in the NFT space is **semi-fungibility**, which is enabled through another Ethereum standard called **ERC-1155**. Semi-fungibility means that an asset can start off as fungible—meaning

it is interchangeable with other similar items—but can become non-fungible through the addition of specific characteristics.

For example, consider a concert ticket. Initially, this ticket is fungible because there are many identical tickets for the same event, and each ticket is priced the same and is interchangeable with the others. However, imagine that Deepika Padukone used one of these tickets to attend a once-in-a-lifetime Farhan Akhtar concert. That specific ticket now becomes non-fungible because of its unique history and association with a particular event and person. Whether or not that ticket is valuable in the market is determined by the demand for such unique items.

In both ERC-721 and ERC-1155, the role of trust remains crucial. The blockchain provides a verifiable link between the digital asset and its unique identifier, ensuring that the item is what it claims to be. However, just like in the traditional art world, the true value comes from the story, the rarity, and the trust that collectors and the market place in the item.

Bitcoin NFTs

Bitcoin, unlike Ethereum, does not have its own smart contract platform, which means that NFTs are not native to the Bitcoin network. However, there have been attempts to introduce a form of non-fungibility to Bitcoin through a concept known as **colored coins**. Colored coins essentially add a distinguishing feature to a set of bitcoins, making them unique within the blockchain. The

term "colored" comes from the idea of adding a metaphorical "color" to certain bitcoins, which helps to differentiate them from the rest.

Think of colored coins as a way of tagging or earmarking certain bitcoins with additional information, thereby giving them a unique identity or purpose. This could be used to represent assets like stocks, bonds, or other types of property within the Bitcoin network. Although not as versatile as Ethereum's NFTs, colored coins represent an early attempt to bring some level of non-fungibility to Bitcoin.

Some Rules for Successful NFTs:

For an NFT to succeed, especially within the context of future society builders, it should meet several key criteria:

Innovation: Is there something innovative about this NFT? Does it noticeably challenge expectations and demonstrate a new capability? The NFT should introduce something new to the table, whether it's a novel use of technology or a creative approach to digital ownership.

Social Flex: Does this NFT help express a social "flex"? In the digital world, much like in the real world, some assets are valuable because they serve as status symbols. An NFT that carries social prestige or signifies membership in an exclusive community can have significant value.

Utility: Does the NFT provide utility that creates intrinsic demand? For instance, some NFTs can be used in decentralized applications (dApps) or as access keys to exclusive content or experiences. The more useful the NFT, the more likely it is to be in demand.

Backing by Tangible or Intangible Value: Is the NFT backed by something else that has value, such as a renowned artist, a popular brand, or a widely recognized event? The backing could be tangible, like a real-world asset, or intangible, like a strong narrative or historical significance.

These rules are not just about creating valuable NFTs—they're about building trust in the digital world. For future society builders, understanding and applying these principles is essential. Trust in the authenticity, utility, and backing of NFTs is what will make them valuable in the long run, just as trust is the cornerstone of value in the broader financial and social systems.

As you explore the potential of NFTs, whether on Ethereum, Bitcoin, or other platforms, remember that trust is at the heart of all value. By focusing on innovation, social relevance, utility, and reliable backing, you can help shape a future where digital assets are not just speculative but genuinely valuable and trusted.

11. DAOs

Let's get rid of the guy at the top. Do we really need him?

We may be able to do that…in some cases. But have you tried herding cats?

As we move further into the crypto world, we come across one of the most powerful innovations: **Decentralized Autonomous Organizations**, or **DAOs**. In my view, DAOs are the most important advancement in the crypto space, even more than cryptocurrencies themselves. That's because DAOs change the way we organize ourselves.

Throughout history, human progress has relied on our ability to work together. Families, armies, universities, and corporations—all are examples of how we group people to achieve specific goals. Whether it's providing stability, winning battles, gaining knowledge, or making money, our ability to organize has led to amazing accomplishments, like landing on the moon.

As society has evolved, so has the way we organize. Corporations are one of the newest ways to manage large groups, using legal contracts to define how they operate with shareholders, employees, and customers. But while corporations have been effective, they have

their limits—especially when it comes to being transparent, scalable, and inclusive.

This is where **DAOs** come in. Built on smart contracts, DAOs offer a new way to organize that not only does what corporations do but improves on it. DAOs operate with trust built directly into the blockchain, making every action and decision transparent and governed by set rules. There's no need for a central authority, making the organization truly decentralized.

Why are DAOs better?
For one, they go beyond borders, making them scalable and accessible to anyone with an internet connection. DAOs are transparent, so everyone involved can see how things are managed—no secrets, no hidden agendas. DAOs can also allow anonymous participation, reducing the chance of discrimination based on physical or cultural factors.

As we discussed earlier, trust is key to any organization. Traditional organizations rely on legal contracts and leaders to build trust, but these systems aren't perfect. DAOs, on the other hand, embed trust into their operations through smart contracts, lowering the cost of trust and making organizations more efficient and fair.

In this chapter, we'll dive into DAOs, starting with their potential to eliminate the need for a central leader. We'll also look at how DAOs fit into today's legal system and explore how they are structured, governed, and run.

Understanding DAOs is crucial to realizing the full potential of blockchain technology. They offer a new way

to organize and work together, showing us a future where organizations aren't limited by borders, hierarchies, or traditional power structures, but are guided by the collective will and trust of their members.

DAOs and the Current Legal System

Currently, DAOs are pushing the boundaries of the existing legal system. The legal frameworks most of us are familiar with have remained largely unchanged for centuries. Even newer democracies, like India, still rely on legal contracts and mental models inherited from European monarchic traditions. As I like to say, we live in an age of rockets but are governed by laws designed for wooden ships.

This means that governments around the world are still trying to figure out how to deal with DAOs because they don't easily fit into existing legal precedents. Some progressive regions, like Wyoming in the United States, have begun to address this by allowing DAOs to register as LLCs (Limited Liability Corporations), giving them similar rights and responsibilities within that jurisdiction. However, for much of the rest of the world, the biggest question remains: who is liable for the actions of a DAO?

This is a crucial issue because if a traditional corporation causes harm—whether to individuals or the environment—there are established legal mechanisms to address it. But with a DAO, things get complicated. For instance, if a DAO were to cause harm or break the law, who would be held accountable? Take the example of the Nouns DAO: many of its members have not revealed their identities. If Nouns DAO were to violate the law, identifying who is legally responsible becomes a challenge.

The liability of DAOs in the real world is a serious matter that must be addressed. However, I'm optimistic that in tackling these challenges, legal systems will be spurred to innovate and adapt to the needs of the modern world—updating themselves from the age of wooden ships to the age of rockets.

The Anatomy of a DAO

The fundamental feature of any DAO is its ability to **propose** and **vote**. These are the first principles of a DAO, the core mechanisms that allow it to function. Every DAO must have a way to create proposals and a system to either pass or reject these proposals. Without these mechanisms, a DAO simply cannot operate. Period. Full stop.

The next key principle is **governance**. DAOs need a way to determine which proposals get approved and which do not. Governance is typically designed to encourage the approval of proposals that benefit the DAO as a whole. For instance, most DAOs restrict voting and proposal rights to those who hold the DAO's tokens. This means that members who propose and vote are often motivated to support initiatives that will increase the value of their tokens.

Let's break down the process of creating and passing a proposal within a DAO.

There are two primary motivations for making a proposal:

Maximizing Token Value: You own a significant amount of DAO tokens and you can propose an initiative that could substantially increase the value of those tokens.

Aligning Personal and DAO Interests: There is an activity that both overlaps with your personal interests and also has the potential to increase the value of the DAO's tokens.

If you examine voting patterns across various DAOs, you'll notice that most proposals fall into one of these categories. The design of a DAO's proposal and voting mechanisms often varies to ensure that the actions taken benefit the DAO and to discourage harmful or malicious proposals.

The proposal and voting mechanisms within a DAO are directly tied to the broader theme of trust. In traditional organizations, trust is often managed by central authorities who enforce rules and make decisions. In a DAO, trust is decentralized and embedded in the governance system itself. Token holders trust that the mechanisms of the DAO will ensure that decisions are made in the best interest of the community, as their own interests are aligned with the success of the DAO. This alignment of incentives reduces the cost of trust, making DAOs an efficient and fair way to organize collective efforts.

As future society builders, understanding the anatomy of a DAO is crucial. It's about more than just the technology—it's about how we can reimagine governance and collaboration in a way that is

transparent, decentralized, and aligned with the collective good.

12. Privacy

If you love me, you'll let me keep my secrets!

TMI - too much information

In *The Matrix*, human beings are mined for energy to power the world of machines. In the real world, humans are mined for data to fuel tech giants like Google, Facebook, Microsoft, and Amazon. Today, your data is considered the new oil, and everyone wants a piece of it. Almost every app and device you use is collecting your data, which is then sold to target you with ads, manipulate your behavior, and keep you hooked on consuming and spending. But this raises a critical question: is the cost of giving up your privacy worth the services you receive in return?

Just as we explored the concept of trust in the first chapter, we must now consider the value of privacy. Trust has a cost, and so does privacy. When you share your personal information, you usually do so in exchange for something—whether it's the convenience of using a free app or the emotional support you get from confiding in a friend. But as tech companies' profits soar, it's worth questioning whether we're paying too high a price with our privacy.

Tech companies argue that the free use of their applications is a fair trade for your data. But is it really? Just as we saw with the cost of trust, surrendering your privacy gives these companies enormous power—power that can be used to influence social opinions, shape behaviors, and even sway the outcomes of elections.

Privacy and Crypto

Knowledge of your financial data is power. If you're running a business, competitors can figure out your strategy and copy you. If you're simply a consumer, businesses can use it to target you with products and services, or deny you access to certain services. Crypto can help shield your financial data and give you more control over who can see it. But this is tricky. Due to Anti-Money Laundering (AML) laws and other government regulations designed to prevent terrorism financing, privacy in crypto is a sensitive topic.

We've all heard about the legal actions taken against Tornado Cash, a tool that became synonymous with bad crypto due to its association with money laundering and other illegal activities. Many also believe that Bitcoin is primarily used for ransomware and other online crimes. While some of this is true, it's important to note that far more US dollars are used for nefarious activities, and historically, the US dollar has probably been used for more illegal activities than any other currency.

This regulatory battle over privacy in crypto is one that needs to be fought. Governments and corporations

around the world, both for benign and self-serving reasons, would like to have access to every moment of your day, because it benefits them. However, it does not benefit you or society at large. In fact, it exacerbates the concentration of power and increases inequality.

Modern technology makes it easy to access all our data, and financial controls restrict how we can utilize our resources. This means you can only act in ways the government or powerful corporations deem acceptable, which is detrimental to both evolution and innovation. As we've seen throughout this book, innovation often involves challenging the establishment. If the establishment can control people completely, this stifles progress.

Encryption

In Chapter 3, we learned about how hash functions are foundational technologies behind crypto. Hash functions fall under the domain of cryptography, which also enables encryption—another key element of privacy tools today. Encryption protects us from malicious actors interfering with our online business. In fact, RSA encryption was central to the legal battle over the export of code that we discussed in Chapter 2.

Every crypto wallet has a public and private key, which can be used to encrypt and decrypt data, ensuring that only those you choose can see it. Moreover, you can monetize your data, getting paid every time someone uses it.

For instance, Keep Network, where I was part of the leadership team, launched a protocol to help people protect and monetize their privacy. Keep Network relied on strong encryption using complex mathematics developed by Princeton and Stanford, and it used a decentralized system of off-chain containers to store data, so no one could find where it was stored or corrupt it.

Keep Network was a pioneer in bringing privacy to public blockchains and was funded by Andreessen Horowitz. Although it was still early days and it didn't do as well as hoped, recent advances in cryptography and the proliferation of Ethereum and Bitcoin mean that solutions tackling data privacy and monetization are on the horizon.

Understanding privacy in the digital era is essential because, like trust, it is a valuable asset that can be exploited. As we explore the balance between convenience and privacy, we'll see how blockchain and encryption can help you regain control over your personal information, ensuring that you have the power to choose who gets to know your secrets. For future society builders, mastering these tools will be crucial in creating a more equitable and secure digital landscape.

13. The Metaverse, Web3 & Crypto

"This is the Oasis, it's a place where the limits of reality are your own imagination." - Ready Player One[54]

If you ask people about the Metaverse, Web3, and Crypto, you're likely to get a range of vague and uncertain answers. These are rapidly evolving and often misunderstood spaces. Yet, at their core, these concepts are about expanding the possibilities of human interaction and creating a new, decentralized digital world.

At a basic level, we can understand the Metaverse as a digital realm that seeks to enhance and transform the way we interact. For instance, when Meta held a courtroom trial in the Metaverse, it was an attempt to make complex social processes more accessible and efficient in a virtual space. This is just one example of how the Metaverse aims to blend the digital and physical worlds.

––––––––––––––––––––––––––

[54] *Ready Player One*. Directed by Steven Spielberg, performances by Tye Sheridan, Olivia Cooke, and Ben Mendelsohn, Warner Bros., 2018.

Web3 is even more perplexing to many. I've met people who claim to be part of Web3 but admit they don't really understand crypto. To me, that's oxymoronic. Why? Because crypto is integral to the vision of Web3. Web3 is supposed to be the decentralized internet—a place where trust is embedded in the technology itself, rather than in centralized institutions. And crypto, with its decentralized blockchain systems, is a fundamental part of that.

Remember our first chapter on trust? The internet is filled with anonymous interactions, and much of its speed and efficiency relies on the low barriers to entry. But anonymity comes with challenges, especially when it comes to trust. Crypto and blockchain technologies are critical for enabling trust in this decentralized world, where transactions can happen without the need for traditional intermediaries.

In this chapter, we'll dive into the Metaverse, Web3, and their connection to crypto. We'll explore how these concepts are reshaping human interactions, how scarcity is managed in the digital world of the Metaverse, and why crypto is essential for building a decentralized Web3. Understanding these connections is key to grasping the future of the internet and the role that trust, as enabled by crypto, will play in this new digital frontier.

Human Interactions and the Metaverse

Human interactions are complex, but our mental worlds are even more intricate. We communicate our inner thoughts and ideas through speech, writing, gestures, touch, video, music, and code. Our ability to use these various modes of communication has been key to our success as a species. The Metaverse can be seen as an aggregation and enhancement of all these communication modes, developed throughout our evolution.

Contrary to popular belief, the Metaverse is not owned by Facebook (now Meta) and is not a single place. Instead, it is a diverse group of virtual spaces, each with its own rules of interaction. The primary goal of these spaces is to enhance human interaction, often by addressing challenges that exist in the physical world.

For example, the Meta courtroom experiment solved the issue of physical proximity, allowing participants to interact as if they were in the same room, even though they were miles apart. This is just the beginning; future Metaverses may solve more fundamental barriers, such as trust in transactions. In places like India, where trust can be a significant hurdle in business and social interactions, crypto-based decentralized systems can facilitate low-trust interactions, where the protocol itself handles the trust element. We'll explore this further in the "Building Your Mental Model" section.

Scarcity in the Metaverse

In the Metaverse, creating digital scarcity is crucial for establishing value. For example, you could create one version of Mumbai in the Metaverse and then replicate it a hundred times with just a few clicks. However, this could lead to an oversupply of virtual land, diminishing its value. This is where crypto comes into play. By backing digital land with something scarce, like Bitcoin, you can create value and ensure that the land remains intrinsically scarce.

Crypto solves a major problem in the commercialization of the Metaverse by providing a way to create and maintain scarcity, a key element in establishing value in any economic system.

A Web3 Deep Dive

The internet was supposed to belong to the people, as we explored in Chapter 2. But currently, that is not the case. ISPs control the flow of information, and big tech companies like Google and Facebook have historically earned high profits at the expense of local businesses. These companies also act as gatekeepers, deciding which applications can be sold through their platforms. The goal of Web3 is to decentralize ownership of internet infrastructure and services, ensuring that it's not just a few companies that benefit at the expense of larger society.

Web3 can accomplish this through shared ownership, which is free, open, and permissionless. Using

crypto-based decentralized systems, Web3 can incentivize large groups of people to provide services to the internet economy. Ethereum is one example, where decentralized validators replace the centralized, trusted servers of internet payment processors.

How Crypto Enables Web3

If anyone says they believe in Web3 but don't understand crypto, then they don't really understand Web3. Crypto is to Web3 what the battery is to an electric car. The decentralized global infrastructure, where people can participate in value transfer and ownership in a free, open, and permissionless way, is the foundation for the more equitable world Web3 aims to create.

Ethereum is a prime example of Web3 in action. It fits perfectly into the idea of what Web3 is trying to accomplish. The ownership of Ethereum is decentralized through the ownership of ETH. Ethereum tokens are essential to the functioning of the system, and ETH owners earn rewards by participating in the protocol through staking. Most importantly, anyone, anywhere in the world can own ETH and participate in the Ethereum ecosystem.

DAOs built on Ethereum are another great example of Web3 built on crypto infrastructure. DAOs provide shared ownership in an organization, guaranteed by Ethereum smart contracts on the immutable and tamper-resistant Ethereum blockchain. DAOs also transact with others on the web through the crypto they

hold in their treasuries, which are effectively Ethereum accounts. They can store wealth they generate in the form of NFTs or other derivatives and earn returns on their wealth by participating in DeFi protocols like Compound.

In short, the Web3 we all want cannot exist without crypto. Understanding this is crucial for anyone looking to build the future of the internet and play a role in creating a more decentralized, trust-based digital world.

14. Interoperability and the Multi chain world

Moksha to you too!

Let's share the moksha. Why stick to one world when you and your stuff can move anywhere?

By now, you're familiar with the basics of blockchain, and you might be wondering: Why are there so many different blockchains? When Ethereum launched in July 2015, it set the stage for a new era of decentralized applications. But since then, the blockchain space has seen rapid innovation, leading to the creation of many new chains, each designed to address specific challenges and limitations of earlier platforms like Ethereum.

One of the key areas of innovation has been increasing the number of transactions that can be processed per second—a response to the growing demand on networks like Ethereum, which has sometimes struggled to keep up. When transaction volumes spike, gas fees can skyrocket, making it expensive to interact with the network. This is where newer chains and Layer 2 solutions come into play, offering improvements in speed, cost, and scalability.

For example, Cosmos addresses this issue by allowing applications to create their own unique blockchains, tailored to their specific needs, while borrowing security from the Cosmos Hub. Similarly, Layer 2 solutions within the Ethereum ecosystem are designed to process transactions faster and at a lower cost, while still relying on the security of the Ethereum main chain.

But beyond these individual improvements, there's a larger vision emerging in the blockchain world: interoperability. Interoperability is about enabling different blockchains to communicate and work together seamlessly. It's like achieving moksha—a state of liberation—where your assets and data can move freely between different chains without being confined to one single ecosystem.

In the first chapter, we explored the cost of trust and how blockchain technology reduces the need for centralized intermediaries. As the blockchain space grows, the need for trustless interactions between different blockchains becomes crucial. Interoperability extends the concept of decentralized trust across multiple chains, creating a more connected and flexible multi-chain world.

Borrowing Decentralized Security

Creating a successful decentralized blockchain ecosystem is hard. It took Bitcoin and Ethereum many years to create trust and spur innovation in their ecosystems. Newer chain ecosystems like Cosmos and Solana have struggled to reach the same level of

adoption even though they offer better and more up-to-date technology. Creating trust is hard.

However, new chain ecosystems do not have to build their own trust and security from scratch. They can borrow it from Bitcoin and Ethereum. For instance, Bitcoin and Ethereum Layer 2 solutions already leverage the main chain's security by reconciling transactions back to it.

Similarly, interoperability between distinct blockchain ecosystems helps new applications borrow decentralized security from Ethereum and Bitcoin. This is a game-changer, accelerating the development of everything from new decentralized applications to Web3 and the Metaverse. We'll explore this more in the "Building Your Mental Model" section.

The Evolution of Interoperability

Interoperability is still a new frontier in the blockchain world. Over the last few years, we've seen the emergence of cross-chain bridges that support the trustless transfer of assets between distinct chain ecosystems. For example, you can have wrapped Bitcoin on Ethereum without needing a central trusted custodian.

For many years, WBTC (Wrapped Bitcoin) was the only way to use Bitcoin on Ethereum, but it required a company like BitGo to lock up Bitcoin on the BTC chain and mint WBTC on Ethereum. This system worked

because the market trusted entities like BitGo to ensure that the locked Bitcoin was not double-spent.

However, TBTC, launched by the Keep Network, was one of the first trustless bridges that wrapped Bitcoin without relying on a trusted intermediary. TBTC and other trustless wrapped Bitcoins remove the need for a centralized intermediary like BitGo, but they also open up the space for more interoperable applications. All of these trustless applications borrow their trust and decentralized security from established and highly decentralized chains like Bitcoin and Ethereum.

Using similar mechanisms to trustlessly wrap Bitcoin, interoperable platforms can provide other services that can be made available across multiple blockchain ecosystems. One major area of development is censorship-resistant middleware, which is essential for truly decentralized applications.

In this evolving multi-chain world, interoperability is not just a feature—it's a necessity. As we build towards a more interconnected future, the ability to move assets and data freely across chains without losing trust or security will be vital. This is the next step in our journey towards a decentralized and connected global economy, where the limits of one blockchain no longer constrain innovation.

15. Crashes & Bull runs

Shiva is life, Shiva is death; Shiva is growth, Shiva is destruction.

Forest Fires can cleanse, and fasting can make people healthier. Crypto crashes can help find reality.

The crypto market is known for its extreme volatility, with at least one significant bull run and one major crash almost every year. Despite these ups and downs, the overall trajectory of the crypto market has been upward as more people discover, use, and build on these digital assets. While some view this volatility as a major risk, fearing sudden losses, it's crucial to step back and understand the dynamics from first principles.

Crypto volatility is often driven by speculation, followed by corrections as the market adjusts asset values in response to rapidly changing information. Unlike traditional financial markets, which have set trading hours, crypto markets operate 24/7, 365 days a year. This continuous flow of information means the market is always reacting, contributing to its fast-paced and often unpredictable nature.

If we compare this to the stock market, we see similarities—big market crashes have occurred there too, with the 2008 financial crisis being one of the most significant in recent history. The stock market also experiences volatility, but it tends to follow longer cycles. Ray Dalio has spoken about these larger cycles, explaining that in traditional markets, information is often hidden, allowing problems to build up over time. When these hidden issues finally surface, they result in massive crashes.

In contrast, the transparency of blockchain technology makes it harder to keep secrets in the crypto world. On-chain activities can be observed and analyzed by anyone, and algorithms and dashboards make it easier to draw inferences from this data. This transparency leads to quicker market reactions, which might seem chaotic but can actually be beneficial. Instead of large, catastrophic shocks every decade, crypto experiences smaller, more frequent corrections. These regular corrections help build a more resilient financial system where participants are better prepared for the inevitable ups and downs.

In the first chapter, we discussed the cost of trust and how blockchain technology reduces the need for centralized intermediaries. In the context of market volatility, this reduced need for trust in opaque institutions means that information flows more freely and corrections happen more quickly. While this creates a more volatile environment, it also means that the system can adapt and recover faster, potentially leading to a

healthier, more sustainable financial ecosystem in the long run.

In this chapter, we'll explore the dynamics of crypto markets, including the forces behind bull runs and crashes. We'll discuss key events like the Bitcoin Halvening, the Ethereum Flippening, and the impact of figures like Elon Musk. We'll also delve into the concept of "Crypto Winter," major crashes in recent history, and how these events have shaped the current state of the market.

Bull Runs

Bitcoin often serves as the leading indicator of broader crypto market bull runs. Since Bitcoin and Ethereum are the largest cryptocurrencies by market cap, they gain the most during a bull run. Historically, all major bull runs have occurred in a low-interest rate environment, which has been prevalent since the 2008 financial crisis. During this period, there have been three significant bull runs closely linked to the Bitcoin Halvening.

The Bitcoin Halvening

As discussed in the Bitcoin chapter, the Bitcoin Halvening occurs approximately every four years. Historically, this event has triggered a general crypto market bull run. One reason is that it increases the cost of mining a single Bitcoin, so miners are less likely to sell for less than their production costs. Additionally, the

reduced supply of new Bitcoins entering the market often leads to higher prices.

Elon Musk

Elon Musk briefly influenced the crypto market in 2021 when Tesla announced it would accept Bitcoin payments. His endorsement brought significant visibility to Bitcoin, attracting new investors. However, the excitement was short-lived when Musk reversed his position due to concerns about Bitcoin's high carbon footprint and his involvement with Dogecoin.

The Ethereum Flippening

For most of crypto's history, Ethereum has been the second-largest cryptocurrency by market cap, generally following Bitcoin's lead in bull and bear cycles. Many in the crypto community believe that because of Ethereum's higher utility and its role as the platform for innovations like decentralized exchanges (DEXs) and NFTs, it will eventually surpass Bitcoin in market cap—a moment known as "The Flippening." Some argue that this has already happened if you consider the total value of assets locked on Ethereum in addition to the value of ETH itself. If Ethereum becomes the dominant cryptocurrency, future bull cycles may look very different.

Crypto Winter

The period between bull runs is known as Crypto Winter. This is when the market is down, and only the strongest projects survive. For many builders in the space, Crypto Winter is a time to weed out weak projects. You can think of it as a forest fire that clears out the old to make way for new growth. Projects that survive Crypto Winter often have real utility and value, making them strong contenders in the next bull run.

Crypto Winter is also an integral part of crypto business strategy. It's inevitable. Businesses that plan for Crypto Winter are better positioned to thrive when the next bull run arrives. Companies that enter Crypto Winter with healthy balance sheets can buy out failing projects and hire talent from poorly managed ones at a discount. For savvy operators, Crypto Winter is an opportunity, not a threat.

Major Crashes in Recent History

While Crypto Winter dominates most of the time in the crypto world, there are also significant crashes that either trigger Crypto Winter or create temporary downturns during a bull market. These crashes often involve major players in the crypto space, but external factors like Fed interest rate hikes have also contributed to bear markets.

Terra Luna

The Terra Luna crash was one of the most catastrophic in the crypto world. It led to the collapse of an entire blockchain ecosystem, Terra, due to the failure of its stablecoin UST to maintain its peg to the dollar. The crash triggered a chain reaction, causing major names in the space like Voyager and Celsius to file for bankruptcy, and leading to the liquidation of 3 Arrows Capital.

FTX

The FTX saga is a cautionary tale in the crypto world. Sam Bankman-Fried (SBF), the CEO of FTX, used customer funds for other business purposes. When the market downturn triggered by Terra Luna hit, he couldn't reconstitute the funds needed to fulfill customer obligations fast enough, leading to the collapse of the company and the loss of customer and investor funds. This was a classic bank run scenario, but in the crypto world. It's important to note that FTX was a centralized company without crypto safeguards like smart contracts or DAO governance. Its collapse helped cleanse the ecosystem of other such entities.

Fed Interest Rate Hikes

At the time of writing this book, interest rates are high. The US Fed's efforts to control inflation by raising interest rates have led to less risk capital globally, including in the crypto space. This has significantly depressed crypto asset prices. The global impact of the

Fed's decisions illustrates the need for a more decentralized financial system.

Past crypto bull cycles have occurred in a low-interest-rate environment, but the current high-interest-rate environment presents new challenges for the market.

Part 4: Where is this going?

17. Artificial Financial Intelligence

Outsourcing finance to Machines

Let's stop wasting time on finance, there's more important things that need solving !

Artificial intelligence (AI) is transforming society at an unprecedented rate, and its intersection with crypto could usher in a financial singularity—a moment in history that fundamentally changes how we think about saving, investing, and managing money. This singularity might bring about changes so profound that they are beyond our current ability to fully comprehend.

But how can we begin to imagine a future that is, by its very nature, unimaginable? One way is to apply first principles thinking to the combination of AI and crypto:

What do we know for sure about AI?

- AI is becoming more intelligent every year.
- AI can process and make decisions based on vast amounts of information, far more than any human could manage.

- AI can generate solutions that humans might never consider.

And what do we know for sure about crypto?

- Crypto is decentralizing financial operations, removing the need for traditional intermediaries.
- Crypto can be used pseudonymously, offering privacy and security.
- Crypto can be accessed by anyone with an internet connection, making financial systems more inclusive.

By applying these first principles, we can start to project the possible futures of an AI-crypto singularity. The scenarios range from the benevolent—where AI and crypto create a more equitable and efficient financial system—to the potentially concerning, where control over finances could become overly automated or concentrated in the hands of a few.

In the first chapter, we discussed the cost of trust and how blockchain technology helps reduce this cost by decentralizing power. Now, as we consider the implications of merging AI with crypto, the concept of trust becomes even more crucial. How do we trust machines with our financial decisions? How do we ensure that these systems remain transparent, fair, and aligned with human values?

This chapter will explore the potential of Artificial Financial Intelligence (AFI), starting with the idea of outsourcing financial management to machines. We'll discuss how this could lead to concepts like Universal

Basic Income (UBI) and AI-driven financial governance. We'll also examine the role of AI in managing investments, banking, and the broader implications for the future of finance.

Universal Basic Income (UBI)

In today's society, we trust investors to allocate resources to maximize profits. The belief is that by focusing on profit, the pie grows for everyone. However, the reality is more complex—climate change, deforestation, pollution, and the rising costs of housing and food show that profit maximization alone ignores many critical factors. Humanity seems to be losing ground in many areas.

With AI's ability to consider multiple variables simultaneously, it could potentially allocate capital more effectively than traditional investors. In this scenario, Wall Street's excessive profits could be unjustifiable, as AI might focus on optimizing wealth distribution across various dimensions, not just profit. AI could ensure that everyone on the planet has access to basic needs like food and housing, while rewarding those who contribute positively across multiple aspects of life, not just financial gain.

AI could also be instrumental in implementing Universal Basic Income (UBI). By managing and distributing resources efficiently, AI could ensure a more equitable distribution of wealth, potentially leading to a society where everyone enjoys a decent standard of living.

AI Governance

Wealth distribution is only one aspect of governance. It's possible that in the future, AI could take on roles as governors, CEOs, or directors. Since finance plays a significant role in politics and leadership selection, the intersection of AI and crypto could allow AI entities to influence large groups of people through capital allocation. This influence could easily transition into our current systems of government, where financial power often determines political outcomes.

AI-driven governance could potentially lead to more efficient and fair decision-making processes. However, this raises important questions about accountability, transparency, and the potential for bias in AI-driven systems.

AI-Based Financial Management

AI-based financial management is one of the most benign and beneficial use cases. We already have robo-advisors managing investment portfolios, and AI is likely to take this to the next level. Competing AI systems may strive to achieve the best returns for their investors, potentially leading to a more efficient and dynamic market.

However, the possibility of AI-driven competition raises deeper questions. Could AI traders significantly alter market dynamics? We've seen how human traders can manipulate markets—like in the GameStop saga. Imagine swarms of AI-driven traders pumping and

dumping stocks to maximize returns for their investors. This scenario could be less benign, potentially leading to market instability.

AI Banking

Why would you ever need a personal banker again? A highly reliable AI that manages your money and ensures you're making the most of available financial services could outperform any human banker. Moreover, since AI isn't human and doesn't benefit from stealing your money, it could be more trustworthy—and cheaper to run.

AI-driven banking could offer personalized financial services at scale, providing tailored advice and management that adapts to each individual's unique circumstances. This could democratize access to high-quality financial services, making them available to everyone, not just the wealthy.

18. The network state

How do you form a new country in the future? Maybe it starts in the metaverse….

In an era where creating a new country seems nearly impossible without colonizing a new planet or engaging in significant conflict, Balaji Srinivasan offers a visionary alternative: the Network State[55]. This concept reimagines how societies and communities are formed, moving beyond the constraints of traditional nation-states and physical borders.

The idea of the Network State is anchored in the transformative power of digital technologies. Srinivasan envisions a future where communities first emerge online, not bound by geography but united by shared ideals, interests, and digital interactions. These "cloud communities" represent more than just online forums; they are the seeds of new forms of social and political organization, capable of creating their own systems of governance, economy, and culture independent of existing nation-states.

---

[55] *The Network State*. https://thenetworkstate.com/. Accessed 18 Aug. 2024.

As these digital-first communities mature, they might choose to establish physical territories, challenging and redefining our traditional understanding of sovereignty and citizenship. Unlike the static nature of current countries, these network states could offer dynamic, decentralized governance models, inspired by technological advancements. They might experiment with direct democracy, real-time policy adjustments, and decentralized decision-making structures, allowing for more responsive and adaptive governance.

For individuals, the rise of network states means a future of enhanced mobility and choice. People could "subscribe" to or "exit" from these entities based on their evolving preferences, values, or opportunities. In this digital age, allegiance to a community might become more about ideological alignment than birthplace, creating a more adaptive and personalized global landscape.

If we consider this in the context of the themes explored in the first chapter—trust and decentralization—the network state represents a natural evolution. As we've seen throughout this book, blockchain technology, crypto, and AI are reshaping the foundations of trust in society. The network state takes these innovations to the next level, offering a new way to organize human societies where trust is decentralized and built into the very fabric of the community.

In this chapter, we'll explore how the network state could emerge, starting in the metaverse, and how cryptocurrencies could serve as enablers for these digital-first communities. We'll also discuss the role of AI

in facilitating the governance and operation of network states, providing the tools for these new entities to function effectively and efficiently.

Understanding the network state is essential as we look to the future of society, governance, and global interactions. This concept, though still in its infancy, could redefine what it means to be part of a community, a nation, or a world.
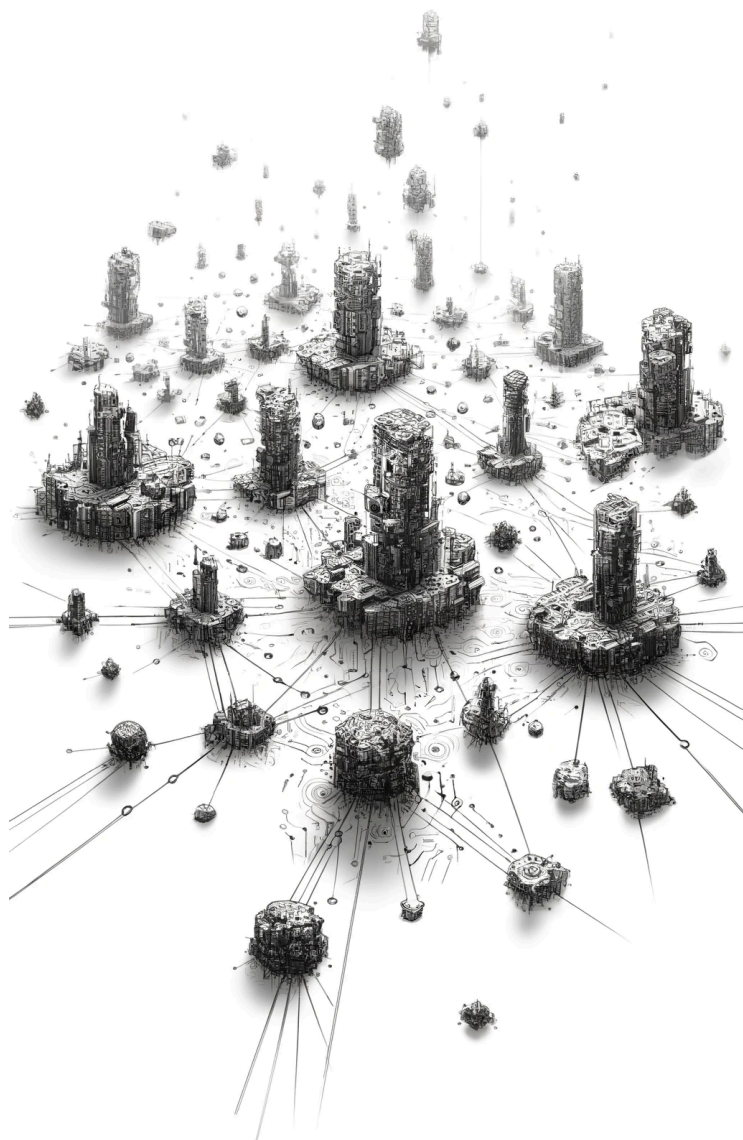
Cryptocurrency as an Enabler of the Network State

Cryptocurrencies and blockchain technology present a transformative toolkit for actualizing Balaji Srinivasan's vision of the "network state." At their core, these decentralized systems redefine governance and autonomy. Smart contracts, for instance, spawn decentralized autonomous organizations (DAOs), empowering communities to self-govern without traditional centralized oversight. This decentralized framework extends to the economy as well. Cryptocurrencies can act as the lifeblood of these digital-first communities, offering a borderless and independent financial system beyond the confines of traditional banks or fiat currencies.

The blockchain doesn't just reshape governance and economics; it offers foundational pillars for identity and property. Decentralized identities can birth a novel form of digital citizenship, granting rights and privileges in a network state without reliance on centralized entities. Alongside this, tokens, especially non-fungible tokens (NFTs), encapsulate property rights in the digital realm, providing immutable, transparent proof of ownership. This crystal-clear record-keeping intrinsic to blockchains underpins the entire structure, ensuring every transaction, governance choice, and community interaction is transparent and irreversible.

Furthermore, the inherent borderless nature of cryptocurrencies champions global interaction within these network states. While fiat currencies are confined

by national borders and policies, crypto transactions flow seamlessly across global digital communities. This, combined with the technology's ability to incentivize community-driven behaviors and its inherent security features, crafts a robust and resilient framework. In this light, cryptocurrencies and blockchain don't just support the idea of a network state; they might very well be the linchpin to its tangible manifestation.

AI as an Enabler of the Network State

Artificial Intelligence (AI) can be a pivotal enabler for the "network state" by reshaping governance, infrastructure, and security. First, in the realm of governance, AI's capability for data-driven decision-making offers an analytical approach to policy formulation. By sifting through vast datasets, AI can model potential outcomes of different policies and even assist in liquid democracy systems, ensuring informed and efficient decisions at every turn.

Secondly, the network state's digital infrastructure can be optimized and autonomously maintained by AI. From managing digital resources to deploying chatbots for citizen interactions, AI ensures seamless operation and enhanced user experience. Its adaptability ensures that the digital backbone of the network state remains robust, responding in real-time to the demands of its digital citizenry.

Lastly, security, a cornerstone for any state's stability, gets a formidable ally in AI. Through real-time monitoring, threat detection, and predictive analytics, AI

safeguards the network state from cyber threats and vulnerabilities. Simultaneously, its prowess in identity verification ensures genuine participation, thwarting malicious actors. In a nutshell, while blockchain may form the skeletal structure of the network state, AI emerges as its responsive nervous system, making the concept more dynamic and sustainable.

In understanding the network state, we see a future where trust is decentralized and managed by advanced technologies like blockchain and AI. This concept ties back to the central theme of this book: the cost of trust. By reducing this cost, the network state promises to offer a new model for organizing human societies in a way that is more flexible, equitable, and adaptive to the complexities of the modern world.

Part6: How do I become a future society builder?

19. How to innovate

You can't build the future without breaking some eggs!

You need first principles to cook up a great idea

At the foundation of every groundbreaking idea lies the power of **First Principles Thinking**. This problem-solving strategy requires us to break down complex ideas into their most basic, undeniable truths or elements. By doing so, we can then reconstruct concepts from the ground up, free from the constraints of traditional thinking. First principles allow us to look past conventional solutions and dive deeper into the fundamentals of a problem, leading to innovative and often unconventional outcomes.

Elon Musk, for example, famously applied first principles thinking to create more affordable batteries for Tesla. Instead of accepting the existing market prices and manufacturing methods, he questioned what batteries are fundamentally made of and how those elements could be sourced and assembled more efficiently. This approach enabled him to drastically reduce costs and revolutionize electric vehicles.

Now, let's apply first principles thinking to the concept of trust—something we've explored since the first chapter. **What should trust really cost?** At its core, the primary component of trust is the time it takes to establish. Therefore, the base value of trust should be the value of the time it takes for individuals to build it. This is why trust is so expensive—larger groups require even more time to establish trust, and for very large groups, it can be nearly impossible to achieve on a traditional scale.

This is where crypto and blockchain-based systems come into play. They lower the cost of trust by significantly reducing the time it takes to establish trust between large groups of people. By automating trust through decentralized technology, these systems make what was once impossible possible. As a result, the very fabric of society is being altered, opening up new avenues for innovation and collaboration.

In this chapter, we'll explore how to innovate effectively by applying first principles thinking to various challenges. We'll discuss the dangers of groupthink, the differences between incremental and zero-to-one innovation, and how first principles can lead to breakthroughs that reshape industries. We'll also look at India-specific innovations and how first principles thinking can be applied to create solutions tailored to unique cultural and societal contexts.

Innovation is key to building the future, but it requires a willingness to question everything, break old patterns, and approach problems from a fresh perspective. By understanding and applying first principles thinking, you

can become a true future society builder, ready to create the next wave of groundbreaking ideas.

Groupthink

Groupthink[56] is a psychological phenomenon where individuals in a group prioritize consensus over the

---

[56] Park, Won‑Woo. "A review of research on groupthink." *Journal of behavioral decision making* 3.4 (1990): 229-245.

accuracy of decisions. This can stifle innovation, as it leads to conformity and discourages unique ideas. To truly innovate, it's essential to encourage diversity of thought and foster environments where contrarian viewpoints are welcomed.

Applying First Principles

To apply first principles thinking:

1. **Identify the Problem:** Clearly define the problem you are trying to solve.
2. **Break Down the Problem:** Deconstruct the problem into its fundamental truths or elements.
3. **Reconstruct the Solution:** With these basic truths in hand, brainstorm innovative solutions without being influenced by traditional methods.

Incremental Innovation

Incremental innovation focuses on making small improvements to existing products, services, or processes. Think of it as refining and enhancing what already exists. For instance, smartphone manufacturers releasing new models with better cameras or batteries are examples of incremental innovation. Although it might not be as groundbreaking as zero-to-one innovation, it's vital for the sustained success and competitiveness of an organization.

Zero-to-One Innovation

Coined by Peter Thiel in his book *Zero to One*, this term refers to creating something entirely new—going from nonexistence (zero) to existence (one). This kind of innovation often reshapes industries and creates new paradigms. An example would be the creation of the first iPhone, which fundamentally changed the smartphone industry.

India-Specific Innovation

Innovation doesn't exist in a vacuum. Regional and cultural contexts play a significant role in shaping the nature and direction of innovation. In the case of India, a term called 'Jugaad' encapsulates its spirit of innovation. Jugaad is a Hindi word that implies a clever, improvisatory style of innovation, driven by scarce resources. It's about making the most of what you have and finding unique, often unexpected solutions to problems.

The rise of affordable mobile phones in India and their impact on the rural economy, the development of the Tata Nano as a low-cost car, and the creation of low-cost sanitary products for women in rural areas are examples of India-specific innovations.

The Big Picture

Innovation is not just about grand ideas and revolutionary breakthroughs. It's as much about

understanding the core of problems, thinking out of the box, making continuous improvements, and adapting to the cultural and regional nuances of a place. Whether you're aiming for incremental changes or groundbreaking transformations, a deep understanding of the principles highlighted in this chapter will steer you in the right direction.

By leveraging first principles thinking, avoiding the traps of groupthink, and understanding the context in which you are innovating, you can create lasting impact and lead the charge in building the future.

20. Science fiction and the future

Boldy go!

….where some people have gone in their imagination

The realm of science fiction (Sci-Fi) has long served as more than just a playground for the imagination; it has often been a crystal ball into the future. From Jules Verne's early predictions of lunar voyages to the ethical dilemmas posed by Isaac Asimov's robot tales, Sci-Fi has a unique way of envisioning possibilities that eventually shape reality.

Throughout this book, we've discussed the transformative potential of technology, from blockchain and AI to the concept of the network state. But many of these ideas were first explored within the pages of science fiction, where authors and thinkers dared to imagine worlds far different from our own. Sci-Fi allows us to explore the implications of technological advancements before they happen, giving us a framework to understand and prepare for the future.

At the core of these imagined futures is the concept of trust. Whether it's the trust between humans and machines, the trust in a decentralized financial system,

or the trust in new forms of governance, Sci-Fi often challenges us to rethink how trust is established, maintained, and sometimes broken. Just as we've explored the cost of trust in the real world, Sci-Fi offers us a chance to explore it in worlds that don't yet exist but could very well become our reality.

In this chapter, we'll journey through some of the most iconic Sci-Fi visions, from *Brave New World* to *Star Trek*, and examine how these stories have influenced and been influenced by technological advancements. We'll delve into the portrayal of AI, the concept of a world without money, and the promise of value beyond traditional financial systems. We'll also explore how Sci-Fi has inspired ideas about incentivizing a shift away from finance as we know it, and the possibility of a future where finance doesn't rely on banks or governments.

Understanding the visions of Sci-Fi helps us see where we might be headed and challenges us to consider the ethical, social, and technological implications of the innovations we're building today. By drawing on these imaginative works, we can better prepare ourselves to create a future that aligns with our values and aspirations.

Brave New World[57]

Aldous Huxley's *Brave New World* offers a chilling portrayal of a future where society has traded freedom and individuality for stability and control. Set in a world

---

[57] Huxley, Aldous. *Brave new world*. DigiCat, 2022.

where humans are genetically engineered, socially conditioned, and kept docile through a drug called soma, the novel explores the consequences of a society that prioritizes collective order over personal freedom.

For future society builders, *Brave New World* serves as a stark warning about the cost of trust when it is manufactured and enforced by a powerful elite. In this world, trust is not earned but imposed through conditioning and propaganda. The people trust their government because they are engineered to do so, not because it has proven itself worthy of trust. This artificial trust leads to a society where individual thought and innovation are stifled, and true human potential is never realized.

In the context of our exploration of decentralized technologies, *Brave New World* challenges us to consider what happens when trust is monopolized and controlled by a few. It prompts us to think about the dangers of centralization—whether in governance, technology, or social systems—and the importance of maintaining spaces where individuals can think freely, question authority, and innovate. As we build new systems based on blockchain and AI, we must ensure that these technologies empower individuals rather than subdue them, fostering genuine trust that is earned rather than imposed.

Huxley's vision is a cautionary tale for those who seek to build the future. It reminds us that while technology can offer solutions to many of society's challenges, it can also be used to control and oppress if not guided by ethical principles. As we develop new technologies, we

must be vigilant to ensure they promote freedom, innovation, and human dignity.

Star Trek

Star Trek[58] represents a more optimistic vision of the future, one where humanity has overcome many of its challenges and is united in the pursuit of knowledge and exploration. The series, created by Gene Roddenberry, envisions a future where technology has advanced to the point where material scarcity is no longer an issue, and society is organized around principles of equality, diversity, and cooperation.

For future society builders, *Star Trek* offers a powerful model of what a decentralized, trust-based society could look like. In the *Star Trek* universe, trust is not something that is imposed from above but is built through cooperation, mutual respect, and a shared commitment to common goals. The series emphasizes the importance of diversity—not just in terms of race, gender, and species, but in ideas, cultures, and perspectives.

In many ways, *Star Trek* anticipates the principles underlying decentralized technologies like blockchain and AI. The show's depiction of a moneyless society, where the pursuit of knowledge and self-improvement replaces financial ambition, resonates with the ideals of Web3 and the metaverse. In this future, technology

---

[58] Okuda, Michael, Denise Okuda, and Debbie Mirek. *The Star Trek Encyclopedia*. Simon and Schuster, 2011.

serves as a tool to enhance human potential, rather than as a means of control.

The series also challenges us to think about the role of governance in a decentralized world. In *Star Trek*, the United Federation of Planets is a cooperative alliance where decisions are made through consensus and dialogue, rather than through coercion or power. This vision of governance aligns with the principles of DAOs (Decentralized Autonomous Organizations), where decision-making is decentralized, transparent, and based on the collective will of the participants.

For future society builders, *Star Trek* offers both inspiration and a challenge. It inspires us to imagine a future where technology serves to elevate humanity, where trust is decentralized and earned through cooperation. At the same time, it challenges us to think critically about how we build this future, ensuring that our innovations promote equity, freedom, and the flourishing of all individuals. As we explore the potential of technologies like blockchain, AI, and the metaverse, *Star Trek* reminds us of the importance of staying true to these values, even as we boldly go into uncharted territories.

AI

Artificial Intelligence, once a fantastical element of Sci-Fi novels, has now permeated our daily lives. From smart assistants to predictive algorithms, AI impacts how we live, work, and play. Books like Philip K. Dick's *Do Androids Dream of Electric Sheep?* (the basis for the film *Blade Runner*) questioned what it means to be human in an age of sentient machines. Today, as AI continues to evolve, these questions become ever more pertinent. Are we on the cusp of creating true machine consciousness? And if so, what ethical considerations do we need to address?

The End of Money

The concept of the "end of money" is a recurring theme in both science fiction and forward-looking technological discourse. It suggests a future where traditional forms of currency—like physical cash or even digital fiat currencies—are replaced or rendered obsolete by more advanced systems of value exchange. This idea has profound implications for society, governance, and human interaction, and it challenges us to rethink the very nature of value and economy.

The Sci-Fi Perspective

In many science fiction works, the end of money is portrayed as part of a utopian or post-scarcity society, where technology has advanced to the point that material needs are effortlessly met, and the pursuit of

wealth is no longer the primary driver of human activity. *Star Trek* is one of the most famous examples of this, depicting a future where humanity has transcended the need for money, focusing instead on exploration, self-improvement, and the betterment of society as a whole[59].

In these narratives, the end of money often coincides with the elimination of poverty, inequality, and social strife—problems that are deeply intertwined with the current economic systems. Instead of competing for resources, individuals in these societies collaborate to achieve common goals, with technology providing the necessary tools to meet everyone's needs. The result is a society where the cost of trust is minimized because there is no need to engage in transactions that could exploit or disadvantage others.

The Real-World Implications

While the idea of a world without money may seem far-fetched, current trends in technology suggest that we might be heading in that direction, albeit in a different form. Cryptocurrencies, decentralized finance (DeFi), and blockchain technology are already challenging traditional financial systems by offering new ways to store, transfer, and create value without relying on central banks or traditional currencies.

In a future where decentralized systems dominate, money as we know it could be replaced by digital tokens

---

[59] Saadia, Manu. *Trekonomics: The Economics of Star Trek*. Inkshares, 2016.

that represent a wide variety of values—social contributions, environmental impact, personal achievements, and more. These tokens could be exchanged in decentralized marketplaces, with smart contracts ensuring that transactions are fair, transparent, and trustless.

For future society builders, the end of money offers both opportunities and challenges. On one hand, it could lead to a more equitable and just society, where value is created and shared based on contributions rather than wealth accumulation. On the other hand, it raises questions about how to measure value in a world without money. What will replace the dollar, the euro, or the yuan as the standard of exchange? How will we ensure that new forms of value are not manipulated or corrupted?

The Promise of Value Beyond Money

In this imagined future, the "promise of value" could be redefined in ways that go beyond mere economic exchange. Value might be tied more closely to individual and collective achievements, societal well-being, or even the preservation of the environment. For instance, a person's contribution to reducing carbon emissions or improving public health could be tokenized and rewarded in a way that incentivizes positive behavior and social good.

The move towards a post-money society also opens up possibilities for new forms of governance and social organization. Without the need for a centralized financial

system, communities could experiment with decentralized forms of governance, where decisions are made collectively and resources are allocated based on need, merit, or consensus.

Trust in a Post-Money World

The end of money would also fundamentally change the nature of trust in society. Today, much of our trust in financial transactions is mediated by banks, governments, and other institutions. In a world without money, trust would need to be built into the systems themselves—through transparent, immutable ledgers, decentralized networks, and community governance.

For future society builders, this means creating systems where trust is not an afterthought but a core principle. It requires thinking deeply about how to design protocols, incentives, and structures that foster trust and collaboration, rather than exploitation and division.

In conclusion, the end of money is more than just a futuristic fantasy—it's a concept that challenges us to rethink the foundations of our economy and society. By exploring this idea, we can begin to imagine new ways of creating and sharing value, and lay the groundwork for a future that is more just, equitable, and sustainable.

21. Building Together: Practical Steps for Future Society Builders

As we reach the culmination of this exploration into the future, it's time to transition from understanding to action. Throughout this book, we've delved into the profound impact of emerging technologies, the essential role of trust in all human interactions, and the ethical considerations that must guide us as we shape the societies of tomorrow. The journey has taken us through the complexities of decentralized systems, the potential of AI, and the transformative power of innovation when grounded in human values.

Now, as we stand at the threshold of this new era, the focus shifts to you—the future society builders. The insights and principles we've discussed are not just theoretical; they are a blueprint for action. The choices we make today, as individuals and as a collective, will determine the trajectory of our world for generations to come.

This final chapter is dedicated to practical steps you can take to contribute to building the future society we've envisioned. It's a call to engage with the technologies that are reshaping our world, to innovate with purpose, and to lead with ethics and integrity. The future is not something that happens to us—it's something we create together.

As we move forward, remember that the foundation of any thriving society is trust. Trust in the systems we build, trust in the people we work with, and trust in the values we hold dear. With this in mind, let's explore how we can each play a role in shaping a future that is just, inclusive, and innovative—a society where technology serves humanity, and where our collective efforts drive progress for all.

Reflecting on the Journey

As we look back on the journey we've taken through this book, a few key themes stand out. Trust has emerged as the foundational element of all human interaction, essential for cooperation, innovation, and progress. Without trust, the systems and societies we build cannot endure.

We've also explored the power of first principles thinking—breaking down complex problems to their most basic elements to find innovative solutions. This approach has guided our understanding of how emerging technologies like blockchain and AI can be leveraged to create more transparent, inclusive, and resilient societies.

Finally, the intersection of technology and human values has been a central focus. Technology alone cannot shape a better future; it must be guided by ethical principles that prioritize fairness, inclusivity, and respect for all individuals.

As we move forward, these themes will serve as our compass, guiding us in the practical steps we take to build the future society we envision—one grounded in trust and driven by ethical innovation.

Engage with Emerging Technologies

The future society we envision will be deeply influenced by the technologies we adopt and how we use them. To play an active role in shaping this future, it's essential to engage with emerging technologies like blockchain, artificial intelligence (AI), and decentralized platforms. These tools are not just transforming industries; they're redefining how we organize, govern, and connect as a global community.

Learn and Innovate

Start by educating yourself about the key technologies that are driving change. Whether it's understanding how blockchain enables transparent, decentralized transactions, or exploring the potential of AI to solve complex problems, continuous learning is vital. Apply first principles thinking to these technologies to uncover new ways to innovate within your field or community. Innovation is most impactful when it's rooted in a deep understanding of the fundamentals.

Participate in Decentralized Communities

Decentralized Autonomous Organizations (DAOs) and other decentralized platforms offer new models for governance and collaboration. These communities operate without traditional hierarchies, giving everyone a voice in decision-making processes. By participating in DAOs or similar platforms, you can contribute to shaping the governance models and economic systems of the future. Your involvement helps ensure that these systems are fair, inclusive, and aligned with the values we've discussed.

Use Technology Ethically

As we adopt and develop new technologies, ethical considerations must guide our actions. Advocate for the ethical use of technology in both your personal and professional life. This means supporting transparency, privacy, and fairness in all technological applications. Whether you're a developer, entrepreneur, or simply a user, your commitment to ethical standards helps build a future society where technology serves the common good, rather than exploiting vulnerabilities.

Engaging with emerging technologies is not just about keeping up with the latest trends—it's about actively participating in the creation of a better future. By learning, innovating, and advocating for ethical use, you become a builder of the society we aspire to create.

The Collective Vision: A Call to Action

As we conclude this journey, it's important to remember that the future we envision is not something that will be built by a few, but by all of us together. The collective efforts of individuals, communities, and organizations are what will shape the society of tomorrow. Now is the time to take action and contribute to the creation of a future that reflects our highest ideals.

Collaborative Effort

The challenges we face today—from climate change to social inequality—cannot be solved by isolated efforts. They require collaboration across borders, disciplines, and sectors. Whether you're working on a local project or participating in global initiatives, seek out opportunities to collaborate with others. By pooling resources, knowledge, and skills, we can tackle complex problems more effectively and create solutions that benefit everyone.

Innovate with Purpose

Innovation is the driving force behind progress, but it must be guided by purpose. As you engage in innovation—whether through technology, business, or social initiatives—ensure that your work aligns with ethical principles and contributes to the common good. Purpose-driven innovation not only solves immediate problems but also lays the foundation for a more just and sustainable society.

Shape the Future Together

Building a future society is not just about technology or policy; it's about creating a culture of trust, inclusivity, and respect. This culture starts with the actions we take every day, in our communities, workplaces, and personal lives. By fostering environments where diverse voices are heard, where transparency is valued, and where ethical considerations guide decisions, we collectively shape the future.

Your role in this collective vision is vital. Whether you're leading initiatives, contributing ideas, or simply supporting others in their efforts, your actions make a difference. The future is a shared responsibility, and together, we can create a society that is innovative, inclusive, and grounded in trust.

Final Thoughts

In this final chapter, the essence of everything we've discussed comes down to one central idea: the future is not predetermined; it's something we build together. Through the lens of trust, ethical innovation, and collaboration, each of us has the power to shape the society we want to live in. The steps outlined in this chapter are practical ways to begin this journey, offering a roadmap for anyone who aspires to be a future society builder.

As you move forward, remember that every action you take contributes to the larger tapestry of our shared future. The technologies we embrace, the values we

uphold, and the innovations we pursue will define the world for generations to come. Together, we have the opportunity to create a future that reflects our highest ideals—a future where technology serves humanity, trust is the foundation of all interactions, and innovation drives progress for all.

Copyright and Licensing

This book, along with all of its content, is a product of extensive research, original thought, and collaboration. Ensuring that we respect copyright and licensing requirements is fundamental to maintaining the integrity of this work.

Images and Visual Content

Most of the images used in this book were generated using OpenAI's DALL-E, an advanced AI tool designed to create images from text descriptions. These images are used under the terms of the DALL-E license, which allows for the generation and use of images under specific guidelines. This licensing ensures that all generated content is legally compliant and respects the intellectual property rights of others.

Wherever other images have been included, every effort has been made to correctly attribute the source and specify the licensing terms. This includes images from publicly available databases, creative commons licenses, and other content sources that permit usage under specified conditions. Proper attribution is not only a legal requirement but also a recognition of the creative work of others.

Textual Content and References

In the creation of this book, great care has been taken to ensure that all text, ideas, and references are original or appropriately credited. However, if any copyrighted material has been included unknowingly or without proper attribution, please reach out immediately. Any such content will be reviewed and either properly attributed or edited out of the book to comply with copyright laws.

Acknowledgements and Contact

We acknowledge the importance of respecting the intellectual property of others. If you believe that any content within this book infringes on your copyright or has been used without proper permission, please contact us directly. Your feedback is invaluable, and we are committed to addressing any issues promptly and responsibly.

This approach to copyright and licensing reflects our dedication to ethical practices and our respect for the creative community. Thank you for your understanding and cooperation in maintaining these standards.

Acknowledgements

The spark for this book was ignited by my mom and Dr. Rudrama Pagidipati in 2022. They not only planted the idea but also expressed the need for such a book, setting the foundation for what would become a deep exploration into the future of technology and society. Their vision and encouragement were instrumental in shaping this journey, and for that, I am profoundly grateful.

The final structure of this book was crafted through many conversations at Soho Houses around the world. These exchanges, filled with diverse perspectives and insightful discussions, were crucial in refining the concepts and themes presented here. I extend my heartfelt thanks to everyone who contributed their thoughts and ideas in these spaces.

My global talks and engagements have also greatly influenced the content of this book. Each event offered new challenges and opportunities for reflection, pushing me to deepen my understanding and articulate my ideas more clearly.

A special thanks to Vikram Rangala and Nirmika Singh, who took the time to read various versions of the manuscript. Their thoughtful feedback, keen observations, and valuable suggestions were pivotal in refining the final product. Their contributions have left a lasting imprint on this work.

To everyone who played a part in bringing this book to life—whether through direct involvement or through the inspiration you provided—thank you. This book is as much a reflection of your insights and support as it is of my own ideas.

About the Author

Prashanth Irudayaraj is an technologist, entrepreneur, and author with a deep passion for Artificial Intelligence (AI), blockchain technology, and renewable energy. Born in Mumbai, India, and raised in Dubai and the United States, Prashanth's diverse background has been instrumental in shaping his approach to technology and innovation. He is known for his significant contributions to various fields, including his pioneering work in decentralized systems and his commitment to leveraging technology for social good.

Prashanth's educational journey led him to the Georgia Institute of Technology, where he earned a Bachelor of Science in Mechanical Engineering in 2007, followed by a Master of Science in Mechanical Engineering in 2015, and an MBA from the Scheller College of Business in 2016. His time at Georgia Tech was marked by early exposure to AI and renewable energy, particularly through his leadership role in the Georgia Tech Solar Decathlon team.

Throughout his career, Prashanth has held key leadership positions in companies like Alcoa, Tesla, Keep Network, and ZebPay. At Keep Network, he served as CEO and Head of R&D, where helped launch privacy-focused infrastructure for public blockchains. At ZebPay, he spearheaded initiatives like the SolarBTC project, which empowered rural Indian women through Bitcoin mining powered by solar energy.

Prashanth's work is also deeply influenced by his love of science fiction, particularly Star Trek. The series' portrayal of a utopian society achieved through science and technology has inspired his techno-optimistic outlook and his desire to build a more equitable and abundant world.

As a prolific author, Prashanth has contributed extensively to Rolling Stone India, where he writes about the intersection of cryptocurrencies, AI, and their societal impacts. His thought leadership continues to influence and shape the conversation around emerging technologies and their role in building the future. Whether through his innovative projects, his writings, or his public speaking engagements, Prashanth Irudayaraj remains dedicated to pushing the boundaries of what's possible with technology, always with an eye toward creating a better, more inclusive future.