Journal of Computer Virology and Hacking Techniques
https://doi.org/10.1007/s11416-024-00525-1

ORIGINAL PAPER

Crypto-anarchy: a paradigm shift for society and the legal system

Alesia Zhuk[1]

Received: 25 October 2023 / Accepted: 4 May 2024

Abstract
This paper delves into the concept of crypto-anarchy, which has emerged in response to the growing dominance of governments and corporations over information and communication technologies. Crypto-anarchy advocates for individual freedom and autonomy in the digital realm through the use of encryption, anonymity, and decentralisation. By examining its historical development, philosophical foundations, and political implications, this article provides an in-depth overview of crypto-anarchy's significance for society and the legal system. It explores how crypto-anarchy challenges conventional legal frameworks and economic structures, while also examining its role in countercultural movements. Furthermore, the paper investigates the initiatives of crypto-anarchists and cypherpunks, highlighting their contributions to the advancement of encryption technology and digital activism. Through this comprehensive analysis, the paper argues that crypto-anarchy represents a paradigm shift for society and the legal system, aiming to foster a more democratic and decentralised digital world. The paper also suggests that for the future, establishing adaptive regulatory frameworks that balance innovation with effective oversight is crucial. This can be achieved by convening a collaborative task force comprising experts from various disciplines to ensure a comprehensive understanding of the complex issues at hand.

Keywords Crypto-anarchy · Decentralisation · Cryptography · Anonymity · Cypherpunks · Digital activism

1 Introduction

In the ever-evolving landscape of technological advancements, society has witnessed profound transformations across various spheres of daily life. From communication to finance, healthcare to governance, innovative technologies have reshaped traditional paradigms. Among these advancements, blockchain technology and cryptocurrencies have emerged as transformative forces, offering decentralised solutions with unprecedented security and transparency. Blockchain's distributed ledger system has revolutionised data management, ensuring immutable records and enabling secure transactions without the need for intermediaries. Cryptocurrencies, powered by blockchain, have disrupted the financial sector, introducing new forms of digital assets and facilitating peer-to-peer transactions on a global scale. As society continues to embrace digitalisation, the incorporation of blockchain and cryptocurrencies into everyday life is becoming increasingly prevalent, promising greater efficiency, accessibility, and democratisation across diverse sectors, heralding a new era of technological empowerment and innovation.

Blockchain technology and cryptocurrencies are deeply rooted in political ideology, particularly inspired by the "Crypto Anarchist Manifesto" of 1988. This ideology, known as cryptoanarchy, champions principles such as privacy, political freedom, and economic freedom. These technologies embody these ideals by decentralising control and enabling peer-to-peer transactions, reducing reliance on central authorities. Cryptocurrencies, in particular, offer secure and anonymous transactions, aligning with the values of privacy and individual liberty central to the cryptoanarchist movement. Consequently, they are reshaping discussions on governance and personal rights in the digital age, reflecting a broader shift towards decentralised systems and individual empowerment.

Recently, the emergence of crypto-anarchy has sparked considerable interest as a disruptive force in both societal and legal domains. This movement, rooted in the utilisation of cryptographic technology to challenge traditional power structures, presents a radical vision for reshaping social and economic organisation. At its core, crypto-anarchy advocates

✉ Alesia Zhuk
alesia.zhuk@ug.uchile.cl

[1] Law Department, Pompeu Fabra University, Barcelona, Spain

Published online: 23 May 2024

for decentralised governance, enabling secure and private transactions and communications without reliance on centralised authorities or intermediaries. Concrete examples of this paradigm shift include the proliferation of DeFi platforms like Ethereum, which allow individuals to engage in peer-to-peer financial transactions without the need for traditional banking institutions. Similarly, the rise of encrypted messaging applications like Signal and Telegram highlights the growing demand for secure and private communication channels outside the purview of centralised platforms.

Despite its growing significance, crypto-anarchy remains relatively unexplored within legal scholarship and practice, highlighting the need for a comprehensive examination of its theoretical underpinnings, historical evolution, and potential implications. This paper seeks to elucidate the foundational concepts and principles of crypto-anarchy and examine its potential ramifications for legal systems and governance. It is worth noting that this paper, originally written in 2019, has been thoroughly revised in 2024 to reflect the evolving landscape of academic research and the growing interest in the topic. Moreover, the focus of this study is on the initial ideas of crypto-anarchy rather than subsequent transitions, such as the emergence of cypherpunk.

This study aims to achieve several interconnected objectives. Firstly, it seeks to deepen our understanding of crypto-anarchy by exploring its historical roots, theoretical foundations, and contemporary manifestations. Furthermore, the research endeavours to critically analyse the philosophical and political underpinnings of crypto-anarchy, examining key concepts such as privacy, decentralisation, and individual autonomy. Moreover, the research seeks to explore practical applications of crypto-anarchy in diverse contexts, and assess their potential to disrupt traditional systems and empower individuals. Lastly, the study aims to identify and evaluate legal and regulatory challenges associated with crypto-anarchy, considering its implications for governance structures and legal frameworks. Through these objectives, the research seeks to contribute to a deeper understanding of crypto-anarchy and its broader impact on society, economy, and governance.

The research methodology employed in this study is characterised by a comprehensive and interdisciplinary approach. It encompasses a qualitative analysis of existing literature, historical inquiry, and critical examination of contemporary developments in the field of cryptography and decentralised technologies. This approach facilitates a holistic understanding of crypto-anarchy by drawing from diverse sources and methodologies. Additionally, the research methodology incorporates thematic analysis to identify key concepts and patterns across various sources, allowing for a nuanced exploration of the subject matter. By combining these methodological approaches, the study aims to provide a robust and well-rounded analysis of crypto-anarchy and its implications.

The paper unfolds in a structured manner, comprising six chapters that systematically explore the concept of crypto-anarchy from its historical roots to its contemporary implications.

Chapter 2 establishes the context for discussing crypto-anarchy, providing an overview of relevant literature and scholarly works. Chapter 3 explores the origins of the term "crypto-anarchy" and distinguishes it from the cypherpunk movement, setting a clear conceptual framework for subsequent analysis. These chapters lay the groundwork by outlining key themes and debates surrounding crypto-anarchy, facilitating a comprehensive exploration of its ideological and practical implications.

In Chapter 4, the paper delves into the philosophical and political foundations of crypto-anarchy in greater detail. It dissects key concepts such as privacy, anonymity, individual freedom, and autonomy, examining how these principles shape the design and implementation of cryptographic technologies like blockchain. By critically analysing the theoretical underpinnings of crypto-anarchy, this chapter sheds light on its broader implications for society, economy, and governance.

Chapter 5 focuses on the technological underpinnings of crypto-anarchy, centred on cryptography and blockchain technology. It explores how these technologies facilitate decentralised systems, secure transactions, and immutable records, laying the foundation for realising crypto-anarchist ideals. Additionally, this cahpter highlights core principles such as absence from government interference, economic freedom, and open-source collaboration, drawing insights from foundational literature and theoretical frameworks.

To demonstrate the real-world relevance of crypto-anarchy, Chapter 5 explores its practical applications and implications in contemporary contexts. It discusses how crypto-anarchist principles manifest in decentralised finance (DeFi) platforms and Decentralised Autonomous Organisations (DAOs), evaluating their potential to disrupt traditional financial systems and empower individuals. Furthermore, this chapter addresses legal and regulatory challenges associated with crypto-anarchy, offering insights into its complex relationship with existing legal frameworks and governance structures.

Finally, Chapter 6 synthesises key findings and insights from preceding sections, providing a critical discussion of crypto-anarchy's implications for society, governance, and technology. It offers a comprehensive summary of the paper's main arguments and contributions, highlighting areas for further research and exploration. By reflecting on crypto-anarchy's implications in light of current and future trends, this chapter provides valuable insights into potential trajectories of the crypto-anarchist movement and its broader impact on society.

2 Literature review on crypto-anarchy

Crypto-anarchy can be understood as a combination of two distinct but interrelated concepts: cryptography and anarchy. Cryptography refers to the science of encoding and decoding messages in order to maintain privacy and security, while anarchy refers to a state of society without government or law. Crypto-anarchy thus entails the use of cryptography to enable secure, private, and anonymous communication and transactions, as well as to undermine the authority and legitimacy of governments and other centralised institutions [51, 149, 190]. Some scholars characterize this as an ideology rather than merely a political or economic movement [27, 27, 28, 38].

A comprehensive understanding of crypto-anarchy necessitates grasping its fundamental principles. Academic literature from the early 2000s to late 2017 often lacked definitive definitions, instead relying on informal sources such as statements, manifestos, speeches, interviews, and other publicly available materials. However, with the growing popularity of cryptocurrencies, scholars began to delve deeper into this subject. Notably, scholars such as Chohan [51], García-Siñeriz [90], Swartz [190], Sajter [169], Hütten [108], Brunton [42], Groos [97], Jarvis [115], Swann [189], Brekke [39], Brekke and Alsindi [40], Jara-Vera [114], Brekhov [38] and Nabben [149] have significantly contributed to this investigation.

The discourse on crypto-anarchy has been significantly enriched by a diverse range of scholarly contributions. Nabben's [149] investigation traces the intellectual evolution of cryptoeconomics, shedding light on its progression from early conceptions of "Crypto Anarchy" to contemporary notions of governance within cryptographic systems.

Swartz [190] provides valuable insights into the techno-economic imaginaries surrounding Bitcoin, offering perspectives on its historical conceptualisation and future prospects. This analysis unveils the broader socio-economic implications embedded within the realm of crypto-anarchy.

Chohan [51] delves into the intersection of cryptoanarchism and cryptocurrencies, unraveling the ideological foundations shaping the adoption and evolution of digital assets. Through an exploration of these philosophical roots, Chohan enhances our comprehension of the political and economic ramifications of crypto-anarchy.

Brekhov's [38] scrutiny of crypto-anarchism as the underlying ideology of blockchain technologies delivers a critical viewpoint on the socio-political dynamics inherent in decentralised systems. By delving into the ideological underpinnings of blockchain, Brekhov deepens our understanding of how these technologies challenge established structures of authority and control.

Beltramini's [27, 28] research offers historical context by examining the influence of the cypherpunk movement on contemporary discussions surrounding crypto-anarchy. By situating the development of crypto technologies within broader socio-political movements, Beltramini underscores the ideological complexities intertwined with decentralised systems.

Swann [189] contributes to the discourse by exploring the nexus between anarchism and cybernetics, illuminating how decentralised technologies can harmonise with principles of political autonomy and self-governance. Through an examination of potential synergies between anarchism and decentralised systems, Swann broadens the theoretical framework for comprehending crypto-anarchy.

García-Siñeriz [90] explores the trust dynamics within blockchain technology, highlighting its potential to shift power dynamics towards decentralised structures. By examining the trust mechanisms inherent in blockchain, García-Siñeriz provides insights into how crypto-anarchy intersects with notions of trust and authority.

Sajter [169] investigates the untapped potentials of blockchain technology, shedding light on its capacity to disrupt traditional economic paradigms. Through an examination of blockchain's transformative potential, Sajter contributes to our understanding of how crypto-anarchy can reshape economic systems.

Hütten [108] critically analyses the governance structures within blockchain networks, highlighting the pitfalls of technological utopianism and emphasising the need for robust governance frameworks. By scrutinising the governance dynamics of blockchain, Hütten offers perspectives on the socio-political implications of crypto-anarchy.

Brunton [42] uncovers the historical roots of cryptocurrency development, tracing its origins to a diverse array of anarchist, utopian, and technological movements. Through an exploration of cryptocurrency's historical antecedents, Brunton enriches our understanding of the ideological foundations of crypto-anarchy.

Groos [97] delves into the sociotechnical imaginaries of governance within blockchain-based technologies, examining the socio-political implications of decentralised systems. By analysing the sociotechnical imaginaries surrounding blockchain, Groos contributes to our understanding of how crypto-anarchy intersects with broader governance paradigms.

Jarvis [115] provides a political history of digital encryption, tracing the evolution of the crypto wars and their implications for privacy in the digital age. Through an examination of the political dynamics surrounding digital encryption, Jarvis offers insights into the broader socio-political implications of crypto-anarchy.

Jara-Vera [114] explores new directions in crypto-politics, investigating emerging trends and developments within the field of crypto-anarchy. By examining the evolving landscape of crypto-politics, Jara-Vera contributes to our understanding of the dynamic nature of crypto-anarchic movements.

Nabben [149], in addition to his intellectual history of cryptoeconomics mentioned earlier, provides further insights into the governance aspects of crypto-anarchy. By examining the governance mechanisms within cryptographic systems, Nabben enhances our understanding of how crypto-anarchy operates within decentralised networks.

Together, these scholars deepen our comprehension of crypto-anarchy by elucidating its ideological underpinnings, historical trajectories, and socio-political implications. Their collective contributions enrich the discourse surrounding decentralised technologies and pave the way for further exploration into the transformative potential of crypto-anarchist principles.

All of the aforementioned sources trace back to the same initial origins where the term 'crypto-anarchy' first appeared. One pivotal starting point is the work of Timothy C. May, regarded as the founder of the crypto-anarchist movement. In November 1992, he released his 'Crypto Glossary,' a compilation of fundamental definitions concerning cryptography intended for public consumption. This glossary was co-developed with Eric Hughes, another influential figure in the genesis of the crypto-anarchist movement, who is also recognised as a cypherpunk.

Hughes and May define crypto-anarchy as "the economic and political system after the deployment of encryption, untraceable e-mail, digital pseudonyms, cryptographic voting, and digital cash" [106]. This definition highlights the two main changes that crypto-anarchy aims to establish: economic and political. The economic aspect involves a free market or market anarchism, which is similar to the libertarian free market ideology that promotes voluntary, uncoerced economic transactions [85]. The political aspect involves anarchy as the absence of government, in which groups may still have leaders, rulers, club presidents, elected bodies, etc. if they so desire [140].

The distinction between crypto-anarchy and the ideas of libertarians or anarchists lies in the technological means that are used to establish a new economic and political order. Specifically, crypto-anarchy employs anonymity and freedom of speech (encryption, untraceable e-mail, digital pseudonyms, cryptographic voting) as well as economic freedom and freedom of trade (voluntary economic transactions). Therefore, crypto-anarchy is an economic (free market) and political (non-governmental) system supported and enabled by cryptographic technology.

Hughes and May, as pioneers of the crypto-anarchist movement, defined crypto-anarchy as a radical ideology and practical framework [106, 140]. They envisioned it as the use of cryptographic technology to establish a decentralised social order characterised by anonymity, freedom of speech, and voluntary economic transactions. Subsequent authors have offered nuanced perspectives on crypto-anarchy, with some emphasising its ideological roots within broader movements such as anarchism or libertarianism [27, 42], while others focus on its practical applications and technological innovations [90, 169]. Overall, while there may be variations in the definitions and understandings of crypto-anarchy among different authors, the core principles of challenging centralised authority and promoting individual autonomy remain central to the discourse [38, 149, 190].

Overall, crypto-anarchy can be defined as a radical socio-political ideology and practical framework that leverages cryptographic technology to establish decentralised governance, ensuring anonymity, freedom of speech, and voluntary economic transactions, ultimately challenging traditional forms of centralised authority and promoting individual autonomy within a new social order. In the subsequent section, an in-depth exploration of the historical evolution of crypto-anarchy will be conducted, with the aim of uncovering pivotal moments and key figures that shaped its trajectory. Specifically, the transition from the early conceptualisations of crypto-anarchy to the emergence of the cypherpunk movement and beyond will be scrutinised, shedding light on the ideological shifts, technological innovations, and socio-political contexts that have influenced its progression over time.

3 Summary

Crypto-anarchy merges the concepts of cryptography and anarchy, utilising cryptographic technology to facilitate secure, private, and anonymous communication and transactions while challenging the authority of governments and centralised institutions. A review of literature reveals that scholarly discourse on crypto-anarchy has evolved significantly, with contributions from various scholars shedding light on its ideological underpinnings, historical trajectories, and socio-political implications. The intellectual history of crypto-anarchy traces back to the pioneering work of Timothy C. May and Eric Hughes, who defined it as a radical socio-political ideology and practical framework enabled by cryptographic technology. Subsequent authors have provided nuanced perspectives, emphasising its ideological roots within broader movements such as anarchism or libertarianism, its practical applications, and technological innovations. Despite variations in definitions and understandings, the core principles of challenging centralised authority and promoting individual autonomy remain central to the discourse.

Author	Contribution
Timothy C. May	Pioneered the concept of crypto-anarchy and defined it as a radical socio-political ideology and practical framework
Eric Hughes	Co-founder of the crypto-anarchist movement, contributing to the foundational definition of crypto-anarchy
Enrico Beltramini	Explored the influence of the cypherpunk movement on contemporary discussions surrounding crypto-anarchy
Lana Swartz	Provided insights into the techno-economic imaginaries surrounding Bitcoin and its socio-economic implications
Gleb S. Brekhov	Scrutinised crypto-anarchism as the underlying ideology of blockchain technologies and its socio-political dynamics
Kelsie Nabben	Investigated the intellectual evolution of cryptoeconomics and governance aspects of crypto-anarchy within decentralised systems

4 Historical development of crypto-anarchy

The historical roots of crypto-anarchy stretch beyond the transformative decades of the late twentieth century, encompassing the core principles of anarchic philosophies. However, scholarly discourse presents differing perspectives on the relationship between crypto-anarchists and traditional anarchism. Brekhov [38] adamantly rejects any association, advocating for a complete divergence between crypto-anarchism and anarchism. In contrast, Malendowicz [136] explores the potential connection between the two ideologies but stipulates that it hinges on the centrality of freedom as a primary value.

Anarchy, as a political doctrine, advocates for the dismantling of centralised authority and hierarchical structures, favouring instead individual autonomy, voluntary collaboration, and reciprocal assistance [80, 156]. Throughout history, anarchism has manifested in diverse forms, ranging from the philosophical writings of Pierre-Joseph Proudhon and Mikhail Bakunin to the revolutionary actions witnessed in movements like the Paris Commune and the Spanish Civil War anarchists [130]. Anarchism is not necessarily defined by a complete absence of government or strict adherence to liberty as a value but rather as an endeavour to challenge prevailing power structures [148] and advocate for alternative modes of governance [205].

The term “crypto-anarchy” was introduced May in his later work titled "The Cyphernomicon" [141]. The word “crypto” originates from the Greek word κρυπτός, meaning "hidden" [140], while "anarchy" is derived from the Greek words ἀν "without" and ἄρχή "power, sovereignty, realm, magistracy" [133], literally translating to "having no ruler" [125]. May stressed that crypto-anarchy does not imply a society devoid of secrets but rather one where individuals safeguard their own secrets without relying on governments or corporations [140]. This foundational concept underscores the ideology of crypto-anarchy, depicting a decentralised governance paradigm where individuals uphold autonomy and privacy through cryptographic mechanisms. Such a notion resonates with the broader philosophy of anarchism, which advocates for the absence of centralised authority while emphasising individual freedom and self-governance [51].

While some, like Hughes and May [106], promote crypto-anarchy as a separate political and economic system, Chohan [51] views it as an improved form of anarchism. He identifies crypto-anarchism as the cyber-spatial realisation and manifestation of anarchism, rooted in the philosophical thought of both the East and West. Referring to the etymology of the term, Chohan suggests that "κρυπτός" may allude to both anarchist politics founded on cryptographic methods and a form of anarchism that operates in secret.

Goldenfein and Hunter [92] describe crypto-anarchy as utilising cryptography to facilitate private contractual arrangements, advance individual liberty, and challenge the dominance of the nation-state. This definition presents crypto-anarchy as the strategic application of cryptographic methods with three main objectives: conducting contracts without dependence on third-party intermediaries (distinct from anonymity), advocating for individual freedom (distinct from freedom of speech and open to broad interpretation), and contesting the authority of nation-states (distinct from advocating for the absence of government).

In the late twentieth century, the principles of anarchism found renewed resonance within the cypherpunk movement [116], which later influenced the development of Bitcoin. This cryptocurrency was conceived by an anonymous entity or group known as Satoshi Nakamoto, drawing inspiration from the ideals of the cypherpunk movement and embodying the concept of crypto-anarchy [149]. This paradigm utilises cryptographic technologies to challenge centralised authority, promote privacy, and empower individuals in the digital realm [51, 90]. Pioneers such as May envisaged a society where cryptographic protocols facilitate free and anonymous interaction, laying the groundwork for the decentralised networks and cryptographic currencies that define crypto-anarchy today [110]. The cypherpunks, recognising cryptography as a means to realise their vision, developed encryption technologies like Pretty Good Privacy (PGP) and Secure Sockets Layer (SSL) to facilitate secure online communication and commerce [211]. Additionally, they engaged in political activism aimed at resisting government surveillance and censorship [211].

Philip Zimmermann's development of PGP in 1991, aimed at implementing encryption in computer technology, played a significant role in catalysing the crypto-activism movement, despite Zimmermann himself not aligning with the labels of crypto-anarchist or cypherpunk [131]. He viewed electronic mail as a regression in terms of privacy compared to traditional sealed letters and sought to rectify this by creating a digital seal for electronic communication [131]. Subsequent collaborations between individuals like Hughes and May contributed to the conceptual development of crypto-anarchy, as manifested in works like "The Crypto Anarchist Manifesto" and the formation of the cypherpunk movement, setting the stage for its evolution and impact on digital society.

The crypto-anarchism and cypherpunk movements have spurred various initiatives aimed at enhancing privacy, security, and freedom of expression. These initiatives span a broad spectrum, from the development of privacy-centric software to the establishment of decentralised networks and alternative currencies. One noteworthy instance is the involvement of Andy Müller-Maguhn, who underscores the significance of the Chaos Computer Club (CCC), a prominent hacker organisation recognised for its advocacy of freedom of information and transparency in technology [95, 207]. Founded in 1981, the CCC has emerged as a seminal figure in the field, providing insights into technical and societal issues such as surveillance, privacy, and hacktivism through its website [3, 207]. Notably, the CCC hosts the annual Chaos Communication Congress, a significant event in the domain, and disseminates publications addressing pertinent topics within its purview [3].

The Electronic Frontier Foundation (EFF), founded in 1990 by John Perry Barlow, John Gilmore and Mitch Kapor, is an organisation dedicated to safeguarding digital privacy, freedom of expression, and innovation [164]. Utilising a diverse range of methods including litigation, policy analysis, mass activism, and technology development, the EFF advocates for access to emerging technologies as a fundamental enabler of other freedoms [152]. Notably, the organisation has been involved in numerous human rights-related legal cases [164]. One prominent example concerns its conflict with Facebook regarding the platform's policy mandating users to provide authentic information about their identities, without consistently implementing mechanisms to address the proliferation of false accounts [74]. While such a policy may serve to curb abuse and uphold accountability, it can also hinder individuals who rely on anonymity, particularly political activists [75].

The Paralelní Polis project in Prague, Czech Republic, encompasses The Institute of Crypto-Anarchy, which serves as a physical hub for cypherpunk gatherings and connects to an international network of hackers [159]. The institute's mission is to facilitate the unrestricted dissemination of information online, foster parallel decentralised economies, promote cryptocurrencies, and advocate for the establishment of a free society in the twenty-first century [38]. It contends that censorship is a pervasive global phenomenon, with both state and corporate entities exerting control over information access and the processing of private communications and personal data [159]. Paralelní Polis endeavours to safeguard two fundamental digital rights: the right to access information and the right to privacy [159]. In the institute's view, crypto-anarchy denotes an unregulated online environment wherein unfettered data sharing and the cultivation of free markets are made feasible through the utilisation of anonymous tools such as decentralised currencies and anti-surveillance encryption [159].

CCC and the EFF are affiliated with the European Digital Rights (EDRi) association, founded in 2002 with the objective of safeguarding human rights and liberties within the digital realm [76]. EDRi acknowledges that while advancements in technology enhance the freedom of communication and democratic principles, they concurrently present risks to fundamental rights due to the potential for surveillance by both governmental entities and private enterprises [76]. Comprising 42 civil and human rights organisations, the association remains dedicated to addressing these challenges and advocating for the protection of digital freedoms [76].

Overall, the historical development of crypto-anarchy reflects a multifaceted discourse, encompassing divergent perspectives on its relationship with traditional anarchism and its core principles. May's conceptualisation of crypto-anarchy underscores its foundational principles of decentralised governance and individual autonomy, while Goldenfein and Hunter's definition emphasise its strategic use of cryptography to challenge centralised authority. The emergence of the cypherpunk movement and Bitcoin further exemplify its practical application in the digital realm. Initiatives such as the CCC, the EFF, and Paralelní Polis embody its principles, advocating for digital privacy and decentralised governance. Collectively, these contributions enrich discourse on crypto-anarchy's historical development and its implications for contemporary society. Looking ahead, the subsequent section will delve into the philosophical and political underpinnings of crypto-anarchy, exploring its theoretical foundations and societal implications.

5 Summary

The historical evolution of crypto-anarchy traces back to the late twentieth century, drawing upon anarchic philosophies. While some scholars reject associations with traditional anarchism, others explore potential connections, focusing on freedom as a core value. Coined by May, crypto-anarchy utilises cryptography to establish decentralised governance and individual autonomy. Scholars like Chohan view it as an evolved form of anarchism rooted in both Eastern and Western philosophical traditions. Goldenfein and Hunter describe it as strategic cryptography challenging centralised authority and nation-states. The emergence of cypherpunk movements and Bitcoin exemplify its practical application, while organisations like the CCC, the EFF, and Paralelní Polis embody its principles through advocacy for digital privacy and decentralised governance. These contributions enrich discourse on crypto-anarchy's historical development and contemporary implications.

6 Philosophical and political underpinnings of crypto-anarchy

In exploring the philosophical and political underpinnings of crypto-anarchy, it is imperative to examine its foundational concepts. At its core, crypto-anarchy champions principles such as anonymity for privacy, individual freedom encompassing freedom of speech and autonomy, the utilisation of cryptography and blockchain for decentralisation, and advocating for absence from governmental interference, promoting economic freedom, and fostering open-source collaboration [140]. These principles serve as the cornerstone of the movement, shaping its aspirations for a decentralised and autonomous society [97]. Anonymity enables individuals to engage in transactions and communications without divulging their identities, fostering trust and privacy in digital interactions (Ludlow 2001; [96]). Individual freedom, coupled with freedom of speech, highlights the significance of unhindered expression in an open and decentralised digital milieu, allowing diverse perspectives to thrive devoid of fear of repression or censorship (Ludlow 2001). Meanwhile, the absence of government interference promotes economic freedom and facilitates open-source collaboration, paving the way for a rejection of hierarchical power structures and envisioning a society where governance is decentralised, consensus-driven, and voluntary (Ludlow 2001; [16]). These principles establish the groundwork for a fairer and more democratic society, empowering individuals to engage in self-governing communities and networks facilitated by cryptography and blockchain technology.

In this section on the philosophical and political underpinnings of crypto-anarchy, the discourse will centre on foundational concepts such as anonymity, individual freedom, and freedom of speech, and the absence of government interference. Anonymity, besides safeguarding privacy, fosters trust and security in online transactions, facilitating economic activities free from surveillance or interference [178]. Likewise, individual freedom and freedom of speech empower individuals to express dissenting opinions and cultivate innovation and critical discourse within digital communities [18]. Moreover, the absence of government intereferecne offers avenues for experimenting with decentralised decision-making, promoting resilience and adaptability in addressing societal challenges [35]. These principles collectively contribute to a vision of a more inclusive, transparent, and equitable society enabled by cryptographic technologies.

6.1 Anonymity for privacy

Anonymity stands as a foundational principle within the ideology of crypto-anarchy, emphasising the liberation of individuals from surveillance and control mechanisms imposed by centralised authorities. This concept finds its roots in the ethos of the cypherpunk movement, where the pursuit of privacy and autonomy in digital interactions became paramount [27, 28]. The cypherpunks envisioned cryptographic technologies as tools to enable individuals to communicate and transact without the fear of being monitored or censored by governments or corporations [115].

Anonymity, within the framework of crypto-anarchy, serves as more than just a shield against surveillance; it represents a fundamental reimagining of power dynamics in the digital age [157]. The ethos of anonymity is deeply intertwined with the broader principles of individual sovereignty and resistance to centralised authority [165]. By concealing the identities of participants in digital transactions and communications, crypto-anarchy seeks to level the playing field, empowering individuals to interact on equal terms without the looming specter of surveillance capitalism or governmental overreach [115]. This principle aligns with the core tenets of anarchism [51, 90], which advocate for the decentralisation of power and the promotion of voluntary cooperation among autonomous individuals [80].

Moreover, anonymity fosters a culture of trust and openness, enabling individuals to freely express themselves and exchange ideas without fear of reprisal. In this regard, anonymity serves not only to safeguard privacy but also to cultivate dissent and innovation, pivotal components of a dynamic and democratic society [2]. However, it is important to acknowledge that anonymity carries a dual nature, akin to a double-edged sword. While it can facilitate the dissemination of diverse perspectives and protect vulnerable voices, it also presents avenues for the propagation of deceptive information and acts of harassment [2, 13, 14]. Ultimately, anonymity embodies a tool that can be wielded for both constructive and detrimental purposes, underscoring the need for vigilance and responsible use in our democratic discourse [61].

The cypherpunk movement, with its emphasis on privacy-enhancing technologies like encryption and digital signatures, laid the groundwork for the development of crypto-anarchy by demonstrating the practical feasibility of anonymous communication and financial transactions [27]. By embracing anonymity as a guiding principle, crypto-anarchy seeks to challenge the hegemony of centralised institutions and create alternative spaces where individuals can exercise their rights to privacy, autonomy, and free expression [11].

At the heart of anonymity lies the fundamental idea of individual sovereignty (Solve 2010). Crypto-anarchists argue that in a truly free society, individuals should have the right to conduct their affairs without undue interference or scrutiny from external entities [107, 135, 139]. Anonymity, therefore, becomes a means of reclaiming personal autonomy in the digital realm, where privacy is increasingly eroded by pervasive surveillance and data collection practices [153, 189, 217].

One prominent academic discourse explores the role of anonymity in shaping the governance structures of digital currencies like Bitcoin. Beltramini [27] argues that Bitcoin's design embodies the crypto-anarchist commitment to anonymity by enabling pseudonymous transactions. Through the utilisation of cryptographic techniques such as public-key cryptography and blockchain technology, Bitcoin provides users with the ability to engage in financial transactions without revealing their true identities (Antonopoulos and Wood 2018; [7, 27]). This aspect of anonymity aligns with the broader goals of crypto-anarchy, which seeks to undermine the authority of centralised institutions by empowering individuals with greater privacy and autonomy in their interactions [107, 139].

Golumbia [93] further examines the ideological underpinnings of crypto-anarchism, emphasising the importance of anonymity as a means of resisting technocratic authoritarianism. By enabling individuals to conduct their affairs without the need for intermediaries or oversight, anonymity serves as a tool for challenging the hegemony of state power and fostering greater individual sovereignty [93, 202].

The concept of anonymity within crypto-anarchy extends beyond financial transactions to encompass all forms of digital communication and interaction (Ludlow 2001; [61, 153]). As Brunton [42] notes, the cypherpunks viewed cryptographic tools such as PGP as essential for safeguarding privacy in email correspondence and online messaging. By encrypting their communications, individuals can protect their personal information from unauthorised access or surveillance by third parties [10].

Privacy complements the concept of anonymity and advances the liberation of individuals from surveillance and control mechanisms imposed by centralised authorities [96, 153, 182]. Unlike anonymity, which pertains to the state of being unidentified or unidentifiable, privacy, in essence, denotes the right of individuals to govern their personal information and determine its collection, usage, and dissemination [56, 57]. The right finds recognition in various international conventions and legal frameworks [77, 197, 198], underscoring privacy as a fundamental human right crucial for autonomy and freedom [100, 167], as elaborated further in the subsequent section.

The intersection of privacy and anonymity reveals a complex interplay among individual rights, societal values, and technological capabilities. Academic discourse frequently explores the delicate balance between privacy and freedom of expression [19, 69, 102, 119]. While privacy safeguards personal information and autonomy, it can also present challenges to transparency, accountability, and the unrestricted flow of information [194]. Scholars meticulously examine the nuanced relationship between these two fundamental rights, analysing how privacy protections can empower individuals to express themselves freely while potentially limiting information dissemination [69, 102]. They probe scenarios where privacy interests conflict with the societal need for transparency and accountability, particularly in cases where individuals seek to withhold information of public interest [19, 119]. Furthermore, these discussions navigate the intricate landscape of privacy in the digital era, where the abundance of personal data and the ease of information dissemination pose unprecedented challenges to maintaining both privacy and freedom of expression [194].

Simultaneously, anonymity on the internet remains a contentious topic, reflecting the intricate interplay among technological affordances, social norms, and regulatory landscapes. Proponents argue that anonymity is not only possible but also essential for protecting individual privacy, fostering free expression, and promoting democratic participation in online spaces [184]. Central to this perspective is the idea that anonymity enables individuals to engage in sensitive or controversial discussions without fear of reprisal or social stigma. By concealing their identities, users may feel empowered to express dissenting opinions, explore diverse perspectives, and challenge prevailing norms and power structures [55]. Moreover, anonymity can serve as a safeguard against surveillance and censorship, allowing individuals to evade monitoring by governments, corporations, and other entities [204].

However, critics argue that anonymity on the internet is not absolute and can be easily circumvented or compromised through various means. Technologies such as cookies, device fingerprinting, and IP address tracking can be used to identify users and trace their online activities, undermining attempts to remain anonymous [153]. Furthermore, anonymity can facilitate harmful behaviors such as cyberbullying [20], harassment [63], and hate speech [143], creating challenges for law enforcement and regulatory authorities [176]. While anonymity can empower marginalised groups and protect individual privacy rights, it also raises concerns about accountability, transparency, and the enforcement of legal and ethical standards [40]. The tension between the positive and negative implications of anonymity underscores the need for a nuanced and context-sensitive approach to its regulation [97].

Biases in relation to anonymity are pervasive within the discourses of crypto-anarchy and cypherpunk ideologies, significantly influencing the interpretation and advocacy of anonymity within these communities. These biases, shaped by various factors, profoundly impact how anonymity is perceived and understood in practice [42, 173]. One prominent bias evident in these discourses is the technological bias, which tends to emphasise the capabilities and limitations of cryptographic technologies in achieving anonymity [27, 28, 59]. This bias often overlooks broader socio-political factors that can affect anonymity in real-world contexts. Additionally, a notable libertarian bias is prevalent, with both crypto-anarchy and cypherpunk ideologies prioritising individual freedom and autonomy over collective or societal considerations [59, 61, 83]. While advocating for individual privacy rights, this bias may lead to a narrow interpretation of anonymity solely as serving individualistic interests.

Moreover, an anti-authoritarian bias characterises these discourses, reflecting a deep-seated distrust of centralised institutions and a desire to subvert traditional power structures (Coleman 2014; [51]). While motivating resistance against government surveillance, this bias may downplay concerns about anonymity's potential for abuse or misuse. Cultural biases also influence the interpretation of anonymity within these discourses, shaped by the cultural backgrounds and lived experiences of individuals involved [42]. These biases may privilege certain perspectives while marginalising others, particularly those from historically underrepresented or disadvantaged groups [31, 200]. Furthermore, a utopian bias is apparent in discussions of anonymity, characterised by an idealistic belief in its transformative potential to create a more just and equitable society [59, 217]. While inspiring activism, this bias may lead to unrealistic expectations about anonymity's efficacy in addressing complex socio-political issues.

Overall, anonymity and privacy are fundamental pillars of crypto-anarchy, essential for liberating individuals from centralised control and fostering their autonomy. However, their interpretation is susceptible to biases, which shape how it is understood and championed within liberalist ideologies. While anonymity holds the potential to empower individuals and safeguard privacy, addressing these biases is imperative for establishing a balanced approach to its regulation. Moreover, the significance of anonymity and privacy closely intersects with the concept of freedom of speech. As explored in the subsequent section, freedom of speech plays a pivotal role in enabling individuals to express themselves freely, shielded from the fear of retaliation or censorship, thus serving as an integral element within the framework of crypto-anarchy.

Author	Main ideas
Beltramini [27]	Anonymity is a foundational principle of crypto-anarchy, liberating individuals from centralised control; it aligns with the ethos of the cypherpunk movement, advocating for privacy and autonomy in digital interactions
Owen [157]	Anonymity within crypto-anarchy challenges power dynamics, promoting individual sovereignty and resistance to centralised authority; it seeks to level the playing field and empower autonomous interactions without fear of surveillance
Preukschat and Reed [165]	Anonymity is deeply connected to broader principles of resistance to central authority, emphasising privacy and autonomy; it enables individuals to interact on equal terms and counters surveillance capitalism and governmental overreach
Brunton [42]	Anonymity fosters trust, openness, and free expression, crucial for a dynamic and democratic society; while it has a dual nature, it cultivates dissent and innovation, although it can also facilitate deceptive information and harassment
Golumbia [93]	Anonymity serves as a tool for resisting technocratic authoritarianism, challenging state power, and promoting individual sovereignty; it enables individuals to conduct affairs without intermediaries, fostering autonomy in digital spaces
Schneider [173]	Biases in discourses of crypto-anarchy and cypherpunk ideologies shape perceptions of anonymity; technological, libertarian, anti-authoritarian, cultural, and utopian biases influence its interpretation and advocacy, impacting how it is understood and championed within these communities

6.2 Individual freedom, freedom of speech, and autonomy

Central to the concept of crypto-anarchy is the notion of individual freedom [90], which encompasses the right of individuals to govern their own lives and make decisions free from external interference or coercion [140, 141]. This principle reflects a deep-seated belief in the inherent dignity and autonomy of every individual [27, 28, 114], regardless of their background or circumstances. In the digital age, where centralised authorities wield increasing power over individuals' lives, the principle of individual freedom takes on added significance [181]. Crypto-anarchists advocate for decentralised systems that empower individuals to control their own data, finances, and identities, thereby reclaiming their sovereignty in an increasingly interconnected world [202].

Individual freedom stands as a cornerstone of digital rights and civil liberties, representing the fundamental principle that individuals should have the autonomy to exercise their rights and express themselves freely in the digital realm [46, 124]. This concept is crucial for safeguarding personal privacy, promoting democratic values, and fostering a free and open society in the digital age [158].

In the context of digital rights, individual freedom encompasses the right to privacy and autonomy over one's personal data and online activities [153]. With the increasing digitisation of society, individuals are generating vast amounts of data through their online interactions, from social media posts to financial transactions. Protecting individual freedom in this context involves ensuring that individuals have control over how their data is collected, stored, and used by governments and corporations [217]. This includes measures such as encryption, anonymisation, and data protection regulations aimed at preserving personal privacy rights [183]. However, the challenge of maintaining individual freedom arises when considering its potential negative implications for societal cohesion and justice.

Individual freedom, celebrated as a pillar of democratic societies, embodies principles of autonomy, self-expression, and human dignity [41]. However, alongside its virtues, scholarly discourse reveals several significant negative aspects that warrant thoughtful consideration [9, 29, 33, 83, 137, 155]. One primary concern revolves around the potential conflict between individual freedom and the public interest or common good [9, 155]. While individuals should enjoy the liberty to pursue personal interests, unrestrained freedom may result in actions detrimental to societal well-being [137]. This tension between individual autonomy and collective welfare has been a central theme in philosophical and political debates since John Stuart Mill's [142] seminal work "On Liberty". Mill argued for the importance of individual freedom but also acknowledged the need for limits when actions harm others or infringe upon their rights.

Moreover, an excessive emphasis on individual freedom can threaten social cohesion and solidarity, particularly in diverse or pluralistic societies [29, 83]. When individuals prioritise personal interests over community welfare, it can weaken social bonds and hinder cooperation for the greater good [104]. Putnam's [166] work on social capital and civic engagement highlights the importance of collective action and shared values in maintaining vibrant, cohesive communities. This raises questions about the potential consequences of prioritising individual freedom in ways that undermine collective well-being.

Unrestricted individual freedom may also enable harmful behaviors that infringe upon the rights and well-being of others. Instances of hate speech [143], discrimination [193], and actions perpetuating social injustice [1] highlight the need to balance individual freedom with ethical considerations and responsibilities towards fellow members of society. Philosopher Isaiah Berlin's [33] concept of negative liberty emphasises the importance of preventing individuals from harming others while preserving their autonomy. Thus, while individual freedom is essential, it must be accompanied by a recognition of its limitations and the broader societal context in which it operates.

In contexts marked by power imbalances, the pursuit of individual freedom may exacerbate exploitation and oppression [94, 98]. Certain groups or individuals with greater resources and social capital may exploit their freedom at the expense of marginalised populations, perpetuating systems of injustice and domination [31, 154]. Iris Marion Young's [215] work on the social connection model of responsibility highlights the complex interplay between individual agency and structural constraints in perpetuating social inequalities. This underscores the need to critically evaluate the implications of individual freedom, particularly within systems that perpetuate existing power differentials.

Furthermore, external forces such as manipulation, coercion, or social pressure can constrain the exercise of individual freedom. In today's digital age, individuals are susceptible to sophisticated forms of manipulation through advertising, social media algorithms, and political propaganda, limiting their autonomy and ability to make truly independent choices [187, 217]. This highlights the challenges inherent in maintaining individual freedom in environments where external influences exert significant control over individuals' decision-making processes. Thus, while individual freedom remains a fundamental principle, its realisation requires careful consideration of the broader social, political, and technological dynamics at play. Paradoxically, the unchecked pursuit of individual freedom may pave the way for tyranny or authoritarianism [24, 71]. When individuals prioritise personal liberty above all else, they may inadvertently create conditions conducive to the rise of autocratic leaders or oppressive regimes promising security and order in exchange for relinquishing certain freedoms [24]. Philosopher Erich Fromm's [86] exploration of the escape from freedom warns against the dangers of individuals surrendering their autonomy in pursuit of security and conformity.

The freedom of speech, a cornerstone of individual liberty, serves as more than just a legal entitlement; it stands as a foundational element of democratic societies [18]. Essential for the exchange of ideas, the functioning of a free press, and the advancement of knowledge, it enables individuals to express themselves, challenge authority, and engage in public discourse without fear of censorship or reprisal [147]. In the digital era, individuals enjoy unprecedented avenues for expression and participation in public discourse through social media, blogs, forums, and other online platforms [158, 218]. The widespread adoption of digital communication also introduces challenges [145, 196] akin to those associated with individual freedom.

One primary concern regarding unrestricted freedom of speech in the digital realm is its potential for harm. It can propagate misinformation, hate speech, and propaganda, posing significant threats to vulnerable individuals and marginalised communities [196, 218]. Additionally, the dominance of certain groups in digital public discourse can exacerbate social inequalities and power imbalances, marginalising minority perspectives [31, 154]. Unrestricted speech also fosters polarisation and extremism, particularly in echo chambers where individuals are exposed only to content that reinforces their existing beliefs [187]. This phenomenon challenges democratic values and underscores the need to limit speech that incites violence or directly harms others, aligning with Mill's harm principle [142].

Moreover, structural barriers such as socioeconomic status, race, and gender can restrict individuals' ability to fully participate in digital discourse, perpetuating inequality [154, 200]. In contexts where freedom of speech is weaponised to suppress dissent, it can paradoxically lead to censorship and repression, undermining the very principles it purports to uphold [15]. The unchecked proliferation of harmful speech online, including cyberbullying and harassment, poses additional threats to individuals' well-being, necessitating legal and technological solutions to protect their rights and dignity [196]. Balancing the preservation of free speech with the need to combat harmful content and ensure the integrity of public discourse requires thoughtful regulation and innovative technological solutions [91]. Furthermore, the emergence of censorship-resistant technologies like blockchain-based platforms presents new avenues for safeguarding freedom of speech while mitigating centralised control and censorship [66, 213].

Autonomy stands as a core value of crypto-anarchy, emphasising individuals' right to self-governance and self-determination ([43, 66, 139]; Ludlow 2001). In a world where centralised institutions increasingly dictate the terms of our existence, autonomy represents a radical departure from the *status quo* [145, 217]. Crypto-anarchists envision decentralised systems that empower individuals to make their own choices and shape their own destinies, free from external control or manipulation [139]. This principle extends beyond finance and technology to encompass broader aspects of human existence, including personal relationships, creative expression, and political activism [186].

As a fundamental aspect of individual freedom, autonomy empowers individuals to govern their own lives, make independent decisions, and assert control over their personal information and resources [54]. In the context of crypto-anarchy, autonomy is amplified through decentralised technologies that enable peer-to-peer transactions, secure communication, and self-sovereign identity management [11, 66, 151]. Cryptocurrencies like Bitcoin and Ethereum provide individuals with financial autonomy, allowing them to conduct transactions without the need for intermediaries such as banks or governments [151], Antonopoulos 2018). Similarly, decentralised identity solutions empower individuals to manage their digital identities securely and privately, reducing reliance on centralised identity providers and enhancing user control [201]. By decentralising control and distributing power among network participants, crypto-anarchist principles of autonomy challenge traditional hierarchies and promote individual sovereignty in the digital domain [11, 66].

The discourse on autonomy delves into the complex interplay between individual freedom and external constraints, acknowledging that while individuals aspire to act according to their own will, various social, political, and economic forces often limit their autonomy [160, 217]. With the advent of digital technologies, new challenges to autonomy have emerged, as individuals navigate algorithmic decision-making systems and data collection practices that shape their digital lives [60, 160, 217]. This concept of "algorithmic autonomy" underscores the importance of individuals retaining control over their personal data amidst growing concerns about surveillance and data manipulation [103]. Moreover, autonomy intersects with social justice, with scholars like Fraser [83] and Benhabib [30] exploring how systemic barriers based on factors like gender, race, and class impede individuals' ability to exercise self-determination. Overall, the discourse on autonomy underscores the need to empower individuals to resist encroachments on their autonomy in both physical and digital realms, ensuring their ability to participate fully in society.

Overall, individual freedom, including freedom of speech and autonomy, plays a pivotal role in shaping digital society and the philosophy of crypto-anarchy. It empowers individuals to express themselves openly, challenge authority, and engage in public discourse, both online and offline. However, discussions about individual freedom require nuance, considering both its virtues and limitations. While fundamental, it's not absolute; some restrictions may be necessary to prevent harm or maintain social cohesion. By leveraging digital tools like cryptography and blockchain, individuals can safeguard their privacy, autonomy, and freedom of expression in an increasingly digital world. These technologies enable secure communication and decentralised systems, prioritising individual sovereignty and upholding fundamental rights and principles.

Author	Main ideas
García-Siñeriz [90]	Individual freedom is central to crypto-anarchy, emphasising autonomy regardless of background
Beltramini [27]	Individual freedom ensures control over data, finances, and identity in decentralised systems
Klang and Murray [124]	Digital individual freedom safeguards privacy and promotes democracy amid increasing centralisation
Mill [142]	Balancing individual freedom with societal well-being requires thoughtful regulation and consideration
Benhabib [29]	Excessive emphasis on individual freedom may undermine social cohesion and collective welfare
Berlin [33]	Individual freedom must recognise limitations to prevent harm and erosion of democratic values
Bartlett [24]	Unchecked pursuit of individual freedom may lead to tyranny, necessitating vigilance against encroachments
Balkin [18]	Freedom of speech is crucial but requires measures to balance expression with combatting harmful content
Putnam [166]	Social cohesion and shared values are essential for democracy, requiring a balance between freedom and welfare
Young [215]	Autonomy intersects with social justice, challenging power differentials and enabling equitable participation

6.3 Cryptography and blockchain for decentralisation

In the realm of crypto-anarchy, cryptography and blockchain stand as indispensable pillars, driving decentralisation, individual sovereignty, and privacy in the digital domain. Through cryptographic techniques and decentralised ledger technology, individuals can safeguard their personal information, engage in confidential transactions, and participate in decentralised networks that operate free from external control or censorship [11, 151]. Cryptography, with its sophisticated encryption algorithms, ensures the confidentiality and integrity of data transmission, enabling individuals to communicate securely over digital channels [79, 174]. Additionally, blockchain technology, pioneered by Bitcoin, provides a decentralised ledger that records transactions transparently and immutably, eliminating the need for intermediaries and fostering trust in peer-to-peer interactions [150, 191].

Crypto-anarchists and liberalists uphold the belief that cryptography, the art and science of secure communication, plays a crucial role in preserving privacy and autonomy in digital interactions. Through the use of cryptographic techniques such as encryption, hashing, and digital signatures, individuals can safeguard the confidentiality, integrity, and authenticity of their data and communications [79, 174]. Within the framework of crypto-anarchy, cryptography emerges as a potent tool for protecting personal information and enabling anonymous transactions, thereby bolstering individual freedom and autonomy [11, 89].

Central to the philosophy of crypto-anarchy is the preservation of privacy, a function served adeptly by cryptography. Through end-to-end encryption mechanisms, individuals can ensure that their communications remain confidential and beyond the reach of unauthorised parties, including governments and corporations [151]. This level of privacy proves vital for safeguarding sensitive information, preserving anonymity, and mitigating the threats of surveillance and censorship [79, 151].

Moreover, cryptography facilitates anonymous transactions and financial interactions, granting individuals the ability to engage in commerce and economic activities without disclosing their identities [150, 188]. Cryptocurrencies like Bitcoin, leveraging cryptographic algorithms to secure transactions and regulate the creation of new units, offer a decentralised alternative to conventional financial systems [89, 188]. By decentralising control and eliminating the necessity for intermediaries, cryptocurrencies empower individuals to reclaim sovereignty over their finances and exert greater authority over their economic destinies [11, 151].

Furthermore, cryptography enables the establishment of digital identities and authentication mechanisms that are resilient to tampering and forgery [12, 120]. Through cryptographic protocols such as digital signatures and public-key infrastructure (PKI), individuals can assert their identities and authenticate their digital interactions without depending on centralised authorities [89, 120]. This decentralisation of identity management enhances individual autonomy and reduces reliance on centralised identity providers, granting individuals enhanced control over their personal data and online identities [66, 89].

Blockchain technologymis lauded as a distributed ledger that securely records transactions across a network of computers, ensuring transparency and integrity [150]. This technology relies heavily on cryptographic principles to achieve its security goals. Cryptographic hash functions, such as SHA-256, are utilised to generate unique identifiers for each block in the chain, ensuring the immutability and integrity of the ledger [188]. Digital signatures, another cryptographic technique, are employed to authenticate transactions, ensuring that they are authorised by the rightful owner of the assets being transferred [191]. Through mechanisms like proof-of-work and proof-of-stake, blockchain networks use cryptography to establish consensus among participants, preventing malicious actors from tampering with the ledger and ensuring the validity of transactions [43]. This interplay between blockchain and cryptography forms the foundation of the technology's security and trustworthiness.

In the realm of crypto-anarchy, blockchain technology facilitates decentralised governance and consensus-driven decision-making, eliminating the need for centralised authorities [191]. Through consensus algorithms like proof-of-work and proof-of-stake, participants in blockchain networks collectively validate transactions and agree on protocol changes without the intervention of central entities (Antonopoulos and Wood 2018). This decentralised governance model fosters trust among participants, enhances network resilience, and ensures that no single entity holds undue control over the network [43].

Furthermore, blockchain technology offers a transparent and immutable record of transactions, bolstering accountability and reducing the risk of fraud and corruption (Antonopoulos and Wood 2018). By decentralising data storage and verification, blockchain mitigates the risk of data tampering and provides a reliable source of truth for all network participants [188]. This transparency and immutability are vital for instilling trust in decentralised systems and enabling secure and reliable transactions [150].

Moreover, blockchain technology facilitates the creation of decentralised applications (dApps) and smart contracts, which execute automatically based on predefined conditions [191]. Smart contracts, coded using blockchain's scripting capabilities, enable trustless interactions between parties, eliminating the need for intermediaries and reducing transaction costs [43]. By automating contract execution and removing human intervention, smart contracts enhance efficiency and reduce the potential for fraud and disputes (Antonopoulos and Wood 2018).

In the realm of crypto-anarchy, while cryptography and blockchain are lauded as cornerstones of decentralisation and individual sovereignty, they also face significant criticism and challenges that impede their efficacy and adoption. Despite cryptography's role in safeguarding privacy and autonomy, concerns persist regarding its potential misuse by malicious actors for illicit activities such as cybercrime, terrorism, and money laundering [126]. The very anonymity and untraceability it offers can facilitate nefarious activities, raising ethical and regulatory dilemmas surrounding its ethical use and regulation [219]. Moreover, cryptographic systems are not immune to vulnerabilities and exploits, as evidenced by historical incidents of cryptographic attacks and weaknesses that compromise data security and integrity [44, 109].

Similarly, blockchain technology, while celebrated for its transparency and decentralisation, faces scalability limitations and environmental concerns associated with its energy-intensive consensus mechanisms, such as proof-of-work [214]. The scalability challenges inherent in blockchain networks hinder their ability to handle a high volume of transactions efficiently, leading to delays and increased transaction costs, thus limiting their practicality for widespread adoption [195, 214]. Furthermore, the decentralised nature of blockchain networks poses governance challenges, as the absence of centralised authority complicates decision-making processes, protocol upgrades, and dispute resolution, potentially leading to fragmentation and forks within the network [144].

Moreover, blockchain's immutability, while ensuring the integrity of transaction records, also presents challenges in correcting errors or addressing fraudulent transactions, as transactions once recorded cannot be easily altered or reversed [163]. This lack of flexibility can be problematic in cases of erroneous transactions, smart contract bugs, or regulatory compliance requirements, raising concerns about accountability and legal recourse [163]. Additionally, the pseudonymous nature of blockchain transactions, while offering a degree of privacy, can also hinder regulatory compliance and anti-money laundering efforts by obscuring the identities of transacting parties [45, 105].

Overall, within the domain of crypto-anarchy, cryptography and blockchain serve as indispensable pillars of decentralisation, individual sovereignty, and digital privacy. While they offer transformative benefits such as secure transactions and transparent record-keeping, they also face notable criticism regarding potential misuse for illicit activities, scalability limitations, governance challenges, and immutability drawbacks. Cryptography and blockchain facilitate decentralisation, which in turn fosters governmental non-interference and economic freedom. Together with open-source collaboration, they form the backbone of digital autonomy and empowerment.

Author(s)	Main ideas
Narayanan et al. [151]	Cryptography and blockchain promote decentralisation, individual sovereignty, and privacy by safeguarding personal information and enabling anonymous transactions
Antonopoulos and Harding [11]	Cryptography ensures privacy and autonomy in digital interactions, protecting personal data and enabling anonymous transactions within the framework of crypto-anarchy
Nakamoto [150]	Blockchain technology, exemplified by Bitcoin, fosters trust in peer-to-peer transactions, empowering individuals to control their finances without intermediaries
Tapscott and Tapscott [191]	Blockchain enables decentralised governance, transparent record-keeping, and efficient smart contract execution, enhancing accountability and reducing fraud
Garay et al. [89]	Cryptography and blockchain technologies together promote individual sovereignty, trust in decentralised systems, and empowerment in the digital domain through secure transactions and resilient identities
Buterin [43]	Blockchain consensus mechanisms ensure transaction validity and decentralised decision-making, fostering trust and resilience within the network
Tschorsch and Scheuermann [195]	Scalability challenges and governance issues in blockchain networks limit practicality and may lead to network fragmentation, hindering widespread adoption
Politou et al. [163]	Blockchain's immutability ensures transaction integrity but poses challenges in correcting errors and addressing regulatory compliance, hindering accountability and regulatory efforts

6.4 Absence from government interference, economic freedom, and open-source collaboration

In the realm of crypto-anarchy, the pursuit of absence from government interference, economic freedom, and open-source principles intertwines to form a robust foundation that underpins decentralised systems and fosters individual empowerment [23, 43, 139]. Advocates seek autonomy and sovereignty in digital interactions, leveraging decentralised networks and cryptographic tools to communicate, transact, and govern without intermediaries or regulatory oversight [16]. This pursuit reflects a fundamental aspiration for individual freedom and self-determination in the digital realm, emphasising mutual aid and community resilience as key tenets of the crypto-anarchist ethos [210].

Crypto-anarchists envision a world where individuals have the freedom to transact and interact without interference from governments or other centralised authorities [140, 141]. This vision is grounded in the belief that centralised institutions often serve to concentrate power and limit individual freedoms, stifling innovation and hindering economic progress [16, 85, 140, 141]. By advocating for absence from government interference, crypto-anarchists seek to create a digital landscape where individuals have the autonomy to govern their own affairs and interact with others on their own terms (Ludlow 2001).

Economic freedom naturally emerges as a consequence of this pursuit, offering individuals avenues to participate in open and permissionless economic systems that resist censorship and manipulation [7, 11, 208]. Cryptocurrencies and DeFi platforms serve as vehicles for this economic liberation, enabling global transactions with minimal barriers and circumventing traditional banking systems and government regulations [11]. This democratisation of finance fosters financial inclusion and empowerment on a global scale, providing opportunities for wealth creation and financial independence without dependence on centralised intermediaries (Popper 2015; [179, 191, 203]).

Open-source principles are integral to advancing the goals of absence from government interference and economic freedom within crypto-anarchy, providing the foundation for collaborative, and community-driven development [82, 210]. By making source code freely accessible for inspection, modification, and redistribution, open-source projects promote trust and accountability, guarding against hidden vulnerabilities or backdoors that could be exploited by governments or malicious actors [209]. Moreover, open-source communities foster collaboration and knowledge-sharing, driving innovation and accelerating the evolution of decentralised technologies [50, 209]. This also promotes inclusivity and accessibility, inviting individuals from diverse backgrounds to contribute to the shaping of digital society.

The interconnected nature of these three principles underscores the holistic approach of crypto-anarchy, where absence from government interference, economic freedom, and open-source collaboration are seen as interdependent components of a larger vision for a more equitable and resilient society (Ludlow 2001; [21]).

Despite the foundational ideals championed by crypto-anarchists, a significant body of critique challenges the notion of complete absence from government interference, arguing that unchecked autonomy from government oversight may lead to a lack of accountability and potential abuse within decentralised systems [66, 210]. Scholars such as De Filippi have highlighted the importance of regulatory frameworks in ensuring consumer protection, preventing fraud, and maintaining market stability [34, 65, 66]. Moreover, critics argue that the absence of government interference may create opportunities for illicit activities such as money laundering, tax evasion, and terrorist financing [151]. However, an opposing viewpoint suggests that weak governance structures or even governments themselves are the root causes of such criminal activities. This perspective argues that these activities thrive due to inadequate national or bilateral responses from governments to address the issue effectively [113]. On the other hand, advocates of crypto-anarchy argue that government interference stifles innovation and limits individual freedom. They point to the resilience of blockchain networks in withstanding censorship and attacks, highlighting their potential to offer a more robust and transparent alternative to centralised systems [191].

Similarly, the concept of economic freedom is subject to critique and support within academic discourse [72]. Critics argue that the unregulated nature of DeFi platforms may expose users to financial risks such as volatility, fraud, and market manipulation [22, 84]. They contend that without proper safeguards and oversight, individuals may fall victim to scams or Ponzi schemes, undermining trust in decentralised systems [49]. Moreover, critics question the scalability and efficiency of DeFi platforms, pointing to high transaction fees and network congestion as barriers to widespread adoption [118].

In contrast, proponents of economic freedom underscore the limitations of centralised banking systems, advocating for DeFi platforms as a solution (Swam 2015). They argue that traditional banking systems exclude underserved communities from financial opportunities. Cryptocurrencies offer a bypass to these limitations, providing access to financial services for the unbanked and underbanked populations [93]. Additionally, decentralisation democratises access to capital, enabling small businesses and entrepreneurs to raise funds without relying on traditional intermediaries [191]. By eliminating barriers to entry and reducing transaction costs, DeFi platforms pave the way for new avenues of wealth creation and economic growth [43].

Finally, critics argue that open-source projects may lack accountability and quality control, leading to security vulnerabilities and software bugs [44]. They point to historical incidents of open-source software being exploited by malicious actors, highlighting the need for robust governance mechanisms and security protocols [6]. Moreover, critics question the sustainability of open-source development models, noting that volunteer-driven projects may struggle to attract long-term contributors and funding [32]. However, proponents of open-source collaboration argue that the benefits of transparency and community-driven innovation outweigh the potential risks [175]. They highlight the success of open-source projects such as Linux and Apache in powering critical infrastructure and driving technological advancements [123].

Overall, the realm of crypto-anarchy embodies a dualistic landscape where every coin has two sides. While the pursuit of absence from government interference, economic freedom, and open-source collaboration offers promising avenues for innovation and autonomy, it also exposes vulnerabilities that require diligent attention. It is imperative to acknowledge that complete exclusion of government oversight may not always yield the desired outcomes, as evidenced by ongoing challenges. Therefore, striking a delicate balance between innovation and regulation is paramount to navigating this evolving digital terrain effectively. The subsequent section will thoroughly explore the practical applications of crypto-anarchist principles within the technological domain, with a particular emphasis on decentralised governance structures and cryptocurrencies operating within the financial system. This examination will extend to scrutinising their broader implications for the legal framework surrounding emerging digital innovations.

Author(s)	Main ideas
May [139]	Absence from government interference, economic freedom, and open-source collaboration form the foundation of crypto-anarchy, fostering individual empowerment and autonomy in digital interactions
Buterin [43]	Advocates for decentralised systems envision a world where individuals can transact and govern without interference from centralised authorities, promoting economic freedom and open-source collaboration
Barreiro [23]	Decentralised networks and cryptographic tools enable autonomous communication and governance, reflecting a desire for individual freedom and self-determination, with open-source collaboration as a key tenet
Atzori [16]	Pursuit of autonomy via decentralised networks embodies principles of absence from government interference and economic freedom, promoting interaction without intermediaries or regulatory oversight
Werbach [210]	Decentralised systems emphasise absence from government interference, economic freedom, and open-source collaboration, fostering trust and resilience in digital communities
Ludlow (2001)	Crypto-anarchists advocate for absence of government interference to promote economic freedom and open-source collaboration, enabling individuals to govern their affairs and interact freely
Weber [208]	Economic freedom is enabled by participation in permissionless economic systems via cryptocurrencies and DeFi platforms, fostering financial inclusion and empowerment globally
Frank and Strecker [82]	Open-source collaboration promotes trust and innovation by making code accessible for inspection and modification, fostering inclusivity within digital communities

7 Summary

The chapter explored the foundational principles and technologies of crypto-anarchy, focusing on individual freedom, freedom of speech, and autonomy as central tenets. It delved into how cryptography and blockchain serve as essential tools for decentralisation, empowering individuals to control their data, finances, and identities. The core principles of crypto-anarchy, including privacy preservation and decentralisation, were highlighted alongside the pursuit of absence from government interference, economic freedom, and open-source collaboration. Despite the transformative potential, challenges such as misuse, scalability limitations, and governance issues were discussed, underscoring the need for a balanced approach to innovation and regulation.

Key elements	Description
Anonymity	Ensures the concealment of individuals' identities and personal information, facilitating anonymous transactions and communications
Privacy	Protects individuals' personal data and information from unauthorised access or surveillance, ensuring confidentiality and security
Individual freedom, freedom of speech	Fundamental principles advocating for individuals' rights to self-governance, autonomy, and free expression, essential for preserving civil liberties and democratic values
Autonomy	Represents individuals' right to self-determination and control over their personal lives, decisions, and digital identities, promoting sovereignty in both physical and digital realms
Cryptography	Utilises encryption techniques to secure communication, data transmission, and privacy, ensuring confidentiality and integrity in digital interactions
Blockchain	Decentralised ledger technology that records transactions transparently and immutably, eliminating the need for intermediaries and fostering trust in peer-to-peer interactions
Decentralisation	Promotes the distribution of power and control away from centralised authorities, enabling peer-to-peer networks and systems that operate independently of external influence or censorship
Absence from government interference	Advocates for autonomy in digital interactions without governmental oversight, fostering economic freedom and innovation through decentralised finance (DeFi) platforms and cryptocurrencies
Economic freedom	Emphasises open and permissionless economic systems, enabling global transactions, financial inclusion, and empowerment, bypassing traditional banking systems and government regulations
Open-source collaboration	Encourages collaborative, community-driven development of digital technologies through transparent and freely accessible source code, promoting innovation, trust, and inclusivity

8 Practical applications and implications of crypto-anarchy

This section delves into the practical applications and broader implications of crypto-anarchy, with a particular focus on governance innovations and DeFi platforms. DAOs represent a significant aspect of this exploration, illustrating how blockchain technology can automate decision-making processes and resource allocation without the need for intermediaries [66, 170, 203]. Despite their potential for democratising governance, DAOs encounter security vulnerabilities and legal uncertainties.

Additionally, the discussion extends to cryptocurrencies and DeFi platforms, which epitomise financial liberation by bypassing traditional intermediaries and enabling peer-to-peer transactions [52, 171]. Cryptocurrencies like Bitcoin and Ethereum offer solutions to economic instability and limited banking infrastructure in regions experiencing hyperinflation or lacking banking infrastructure [52, 134]. However, these innovations face challenges such as price volatility, market manipulation, and scalability limitations [70, 162]. Understanding the practical applications and implications of DAOs and DeFi platforms is essential for comprehensively analysing the impact of crypto-anarchy on governance and finance.

Lastly, the section examines the legal and regulatory challenges arising from the decentralised nature of crypto technologies, which present complexities in jurisdictional compliance and regulatory enforcement. Overall, acknowledging the potential benefits and risks of crypto-anarchy is essential for developing effective regulatory responses and harnessing the full potential of decentralised technologies.

8.1 Governance innovations and decentralised systems

The rise of decentralised systems and cryptographic technologies has ushered in a new era of governance innovation, challenging traditional centralised authority structures and paving the way for novel approaches to decision-making and resource management [66]. One of these innovations is DAOs, which represent a radical departure from conventional organisational structures, leveraging blockchain technology to automate decision-making processes and allocate resources without the need for intermediaries or central oversight [66, 170, 203]. From a technical standpoint, DAOs operate through smart contracts, self-executing code stored on a blockchain, which enables members to vote on proposals and execute transactions autonomously [203].

While DAOs hold promise for democratising governance and enhancing organisational efficiency, they also face issues related to security and legal status. Smart contract vulnerabilities, such as the infamous DAO hack of 2016, underscore the need for robust security protocols and dispute resolution mechanisms [117]. The DAO was a venture capital fund built on the Ethereum blockchain, designed to operate as a decentralised investment platform where investors could contribute funds and vote on which projects to fund [170]. It raised over $150 million worth of Ether, making it one of the largest crowdfunding projects at the time (Santos, & Kostakis). However, in June 2016, an unknown attacker exploited a vulnerability in The DAO's smart contract code, allowing them to siphon off approximately one-third of the funds, totaling around $50 million worth of Ether [36].

The hack exploited a flaw in the DAO's code related to the "split function," which allowed users to split their investment into smaller parts and withdraw their Ether. The hack led to a contentious debate within the Ethereum community about how to respond. Some advocated for a hard fork of the Ethereum blockchain to reverse the transactions and recover the stolen funds, while others argued that doing so would undermine the immutability and decentralisation principles of blockchain technology [108]. Ultimately, the Ethereum community decided to implement a hard fork, leading to the creation of Ethereum Classic (ETC), a separate blockchain that retained the original transaction history without reversing the DAO hack [68]. Meanwhile, the majority of Ethereum users migrated to the new blockchain, now known as Ethereum (ETH), which implemented the hard fork to recover the stolen funds [68].

The DAO hack served as a wake-up call for the cryptocurrency industry, highlighting the importance of robust security practices and thorough code audits when developing smart contracts and decentralsed applications [108]. It also sparked discussions about governance, consensus mechanisms, and the role of community decision-making in decentralised systems [170].

In addition to security challenges, the legal status of DAOs remains uncertain, with regulators grappling with questions of liability, accountability, and jurisdiction in the absence of traditional legal entities [37]. In many jurisdictions, DAOs operate in a legal gray area due to their decentralised nature and the lack of clear regulatory frameworks tailored to govern them. Traditional legal frameworks often struggle to categorise DAOs, as they do not fit neatly into existing legal classifications such as corporations, partnerships, or cooperatives [37].

Despite these struggles, DAOs have garnered interest across various industries, including finance, supply chain management, and content creation due to their unique nature. Projects like Aragon and DAOstack are pioneering the development of DAO frameworks tailored to specific use cases, offering customisable governance modules and community-driven decision-making processes [161]. Aragon, an open-source platform built on the Ethereum blockchain, provides a comprehensive suite of tools and infrastructure tailored for the creation and operation of DAOs [78]. Launched in 2016, Aragon's modular architecture allows users to customise their DAOs according to their specific needs, selecting from a range of pre-built modules or developing custom ones using Aragon's development framework [78].

This modular approach enables flexibility and adaptability, empowering users to design governance mechanisms, conduct voting processes, manage finances, and define membership criteria within their DAOs. Central to Aragon's functionality is its native token, the Aragon Network Token (ANT), which serves as a governance token within the ecosystem, allowing holders to propose and vote on changes to the protocol [172].

DAOstack, founded in 2017, is another pioneering platform in the DAO space, offering a comprehensive toolkit for the creation and management of decentralised organisations and applications [78]. Built on Ethereum, DAOstack emphasises collective decision-making and coordination among large groups of participants without centralised control [78]. At the core of DAOstack is the Arc.js framework, a set of tools and libraries that enable developers to build complex DAO structures and decentralised applications (DApps) [64]. This framework includes modules for governance, voting, reputation management, and more, providing developers with the building blocks necessary to create sophisticated organisational structures ("DAOstack Arc.js," 2018). DAOstack's unique governance mechanism, known as Holographic Consensus, incentivises active participation and contribution by rewarding users with reputation tokens. These tokens grant holders influence over decision-making processes within the DAO, fostering a dynamic and responsive governance system [73, 78].

Moreover, the transformative potential of blockchain-based voting systems extends beyond organisational governance, promising to revolutionise electoral processes by enhancing transparency, integrity, and accessibility [26, 111]. Technically, blockchain voting systems utilise distributed ledger technology to record and validate votes securely and transparently, mitigating the risks of tampering and fraud associated with traditional voting systems [185].

One practical example of DAOs' application is their potential to play a pivotal role in local, national, or even global movements by facilitating the allocation of resources in a manner that is both fair and effective [138]. For example, small local organisations, which often spearhead action within these movements, can leverage DAOs to streamline the management of funds. By allowing members to participate in decision-making processes, DAOs enable these organisations to determine resource allocation based on the specific needs and priorities of the movement [138].

It is important, however, to understand that the widespread application of DAOs is still far from being implemented in states, at least on a local level. Due to potential problems with technical equipment, system changes that require resources, legal problems associated with regulation, and subsequent ethical problems related to fairness, transparency, inclusivity, and accountability. Despite all this, DAOs appear as a promising step and have potential.

Overall, DAOs are based on crypto-anarchy principles, embodying decentralisation, autonomy, privacy, anonymity, and resistance to censorship. This model holds promise for revolutionising governance structures by empowering communities to make collective decisions and manage resources autonomously. However, potential issues such as susceptibility to security vulnerabilities, regulatory challenges, must be carefully considered and addressed to realise the full potential of DAOs in practical applications.

8.2 Cryptocurrencies and decentralised finance

Cryptocurrencies and DeFi platforms represent a paradigm shift in the concept of access to financial services, assets managment, and money and value exchange [53, 171]. Unlike traditional fiat currencies controlled by central authorities, cryptocurrencies operate on decentralised networks, enabling peer-to-peer transactions without intermediaries [58]. Bitcoin, the first and most well-known cryptocurrency, introduced the concept of digital scarcity and censorship-resistant money, challenging the traditional banking system's dominance [128]. Subsequent cryptocurrencies, such as Ethereum, expanded the possibilities by introducing smart contracts and programmable money, enabling a wide range of decentralised applications and financial services ([43], Antonopoulos and Wood 2018).

DeFi platforms build upon the principles of cryptocurrencies to create open and permissionless financial ecosystems. These platforms enable users to access a wide range of financial services, including lending, borrowing, trading, and yield farming, without relying on traditional financial intermediaries [17, 99]. Smart contracts and blockchain technology automate and secure these transactions, reducing counterparty risk and enhancing transparency [171]. DeFi platforms also enable users to earn passive income through liquidity provision, staking, and yield farming, further democratising access to financial opportunities [99].

Several case studies highlight the real-world implications of cryptocurrency adoption for economic freedom, financial inclusion, and global financial systems [168]. In countries experiencing hyperinflation or economic instability, such as Venezuela and Zimbabwe, cryptocurrencies like Bitcoin provide a hedge against currency devaluation and capital controls, enabling citizens to preserve their wealth and access international markets [52, 53, 134]. In regions with limited banking infrastructure, such as sub-Saharan Africa and Southeast Asia, cryptocurrencies and mobile-based wallets offer a lifeline for the unbanked and underbanked populations, enabling them to participate in the global economy and access financial services previously out of reach [168].

Despite the beneficial characteristics of cryptocurrencies and DeFi, there are several points of concern that warrant attention. One of the primary weaknesses of cryptocurrencies is their inherent volatility and speculative nature (Tan et al. 2020; [70]). Cryptocurrency markets are known for their extreme price fluctuations, which can be driven by factors such as market sentiment, regulatory news, and technological developments [8]. For instance, in 2017, Bitcoin witnessed an extraordinary escalation in valuation, peaking at nearly $20,000 per coin [192]. However, this surge was short-lived, as its value rapidly declined by more than 50% within a few weeks [192]. This volatility poses significant risks for investors and undermines cryptocurrencies' viability as stable stores of value and mediums of exchange [212]. The consequential price fluctuations may entail substantial financial setbacks for investors and participants, thereby undermining their trust in the reliability of cryptocurrencies as a dependable means of exchange and reservoir of value [67].

Another weakness of cryptocurrencies is their susceptibility to market manipulation and fraudulent activities [4, 22]. Due to the relatively low liquidity and unregulated nature of crypto markets, they are vulnerable to price manipulation schemes such as pump and dump schemes, wash trading, and spoofing [48]. These manipulative practices can distort market prices and erode investor confidence, leading to reputational damage for the entire crypto ecosystem [88]. For example, a study analysing suspicious trading activity on the Mt. Gox Bitcoin exchange, where approximately 600,000 bitcoins (BTC) valued at $188 million were fraudulently acquired, found that the USD-BTC exchange rate rose by an average of four percent on days when suspicious trades took place, compared to a slight decline on days without suspicious activity [88]. This indicates the significant impact of market manipulation on cryptocurrency prices. Additionally, the pseudonymous nature of cryptocurrencies makes it challenging to identify and prosecute perpetrators of fraudulent activities, further exacerbating the problem [62].

Scalability is another major challenge facing cryptocurrencies and blockchain networks, including DeFi platforms [47]. The current generation of blockchain platforms, such as Bitcoin and Ethereum, face scalability limitations that restrict their capacity to process transactions quickly and cost-effectively at scale [162]. Network congestion and high transaction fees can impede the usability of cryptocurrencies for everyday transactions, limiting their adoption as a mainstream payment method [25].

Overall, cryptocurrencies and DeFi platforms embody principles of crypto anarchy, including decentralisation, autonomy, and resistance to censorship. Pioneered by cryptocurrencies like Bitcoin and Ethereum, they usher in a paradigm shift in currency and finance. Operating on decentralised networks, they eliminate intermediaries and facilitate peer-to-peer transactions. DeFi platforms, stemming from cryptocurrencies, extend this decentralisation to financial services, enabling users to access a broad range of offerings without relying on traditional financial institutions. This restructuring of financial systems challenges existing power dynamics, granting individuals greater control over their assets and transactions. However, vulnerabilities in blockchain technology may impact DeFi platforms, potentially resulting in financial losses and eroding trust. Additionally, the volatility of cryptocurrencies poses a barrier to their wider acceptance and adoption.

Legal challenges associated with DAOs, cryptocurrencies, and DeFi platforms encompass various complex issues, including regulatory ambiguity, jurisdictional conflicts, and concerns about investor protection and consumer rights. These complexities warrant special attention and will be thoroughly examined in the subsequent section, which aims to illuminate the future trajectory of legal developments in these domains.

8.3 Legal and regulatory challenges

The rise of crypto-anarchy's principles, as exemplified by technologies such as DAOs, cryptocurrencies, and DeFi, presents profound legal and regulatory challenges [132]. Decentralised systems and cryptographic technologies disrupt traditional notions of jurisdiction, compliance, and enforcement by eroding the authority of central entities and introducing novel mechanisms for governance and transactions [112]. This shift challenges existing legal frameworks designed for centralised systems, necessitating adaptation and innovation in regulatory approaches to address the complexities of decentralised networks and their implications for governance and accountability [132].

One of the fundamental challenges posed by crypto tehcnologies in the legal domain is the ambiguity of jurisdiction in a borderless digital environment [5]. Traditional legal frameworks are ill-equipped to address transnational transactions and interactions facilitated by decentralised networks and cryptographic technologies [101]. Jurisdictional disputes arise when legal entities operate across multiple jurisdictions, raising questions about which laws and regulations apply to their activities [121, 146]. The decentralised nature of blockchain networks further complicates matters, as nodes and users can operate from anywhere in the world, beyond the reach of traditional regulatory authorities [87].

Compliance with existing regulations presents another significant challenge for participants in crypto systems [66]. Financial institutions, exchanges, and other entities involved in cryptocurrency transactions must navigate a complex web of regulatory requirements, including anti-money laundering (AML), know your customer (KYC), and counter-terrorism financing (CTF) regulations [127]. However, the pseudonymous nature of cryptocurrency transactions and the lack of intermediaries make it difficult for regulators to enforce compliance and monitor illicit activities [45, 105]. Moreover, regulatory frameworks vary widely between jurisdictions, leading to regulatory arbitrage and inconsistencies in enforcement [121, 146].

One prominent legal dispute that underscores the complexities of regulating crypto technology is the case between the United States Securities and Exchange Commission (SEC) and Ripple Labs regarding the classification of XRP, the native cryptocurrency of Ripple [199]. The United States Securities and Exchange Commission (SEC) alleges that Ripple Labs engaged in the unlawful offer and sale of securities, violating Sect. 5 of the Securities Act of 1933 [199]. The core issue is whether XRP should be considered a security under US securities laws. The outcome of this case could have significant implications for the regulation of cryptocurrencies and the broader crypto ecosystem [180].

Regulating crypto technology requires a nuanced understanding of the complexities of decentralised systems and cryptographic technologies [206]. Traditional top-down regulatory approaches may not be suitable for regulating decentralised networks, which are designed to operate autonomously and resist censorship and control [216]. Instead, regulators must adopt a collaborative and adaptive approach that balances innovation with consumer protection and financial stability. Regulatory sandboxes, pilot programs, and stakeholder consultations can facilitate experimentation and innovation while allowing regulators to monitor risks and develop tailored regulatory frameworks [81].

To conclude, in considering the future trajectory of crypto-anarchy and its implications for the legal system, it is crucial to acknowledge both the potential benefits and risks that accompany this technological innovation. While crypto-anarchy presents opportunities for decentralisation, autonomy, and resistance to censorship, it also poses significant challenges for regulatory frameworks and traditional institutions. One concrete recommendation is to establish a collaborative task force dedicated to studying the impact of crypto technologies on the legal system and developing adaptive regulatory frameworks [129]. This task force could comprise experts from various fields, including law, technology, economics, and cybersecurity, to ensure a comprehensive understanding of the complex issues at hand. Additionally, leveraging technological solutions such as blockchain analytics and AI-powered compliance tools can enhance regulatory oversight and enforcement capabilities in the crypto space [122, 129]. Implementing smart contracts and decentralised governance mechanisms within regulatory frameworks can also streamline compliance processes and improve transparency and accountability [177].

9 Summary

The chapter explored the practical applications and broader implications of crypto-anarchy, with a particular focus on governance innovations and DeFi platforms. It delved into how DAOs leveraged blockchain technology to automate decision-making and resource allocation, highlighting their potential for democratising governance despite encountering security vulnerabilities and legal uncertainties. Additionally, the discussion extended to cryptocurrencies and DeFi platforms, showcasing their role in financial liberation by enabling peer-to-peer transactions and addressing economic instability and limited banking infrastructure in certain regions. However, these innovations faced challenges such as price volatility, market manipulation, and scalability limitations. The chapter underscored the importance of understanding these practical applications and challenges for developing effective regulatory responses and harnessing the full potential of decentralised technologies in governance and finance.

10 Discussion

The exploration of crypto-anarchy in this research represents a comprehensive investigation into the transformative potential of decentralised technologies. By delving into the foundational principles of crypto-anarchy, including anonymity, freedom of speech, absence of government interference, and decentralisation, insights that extend far beyond the realm of technology alone have been uncovered. This final section aims to initiate a discussion and synthesise the key findings of the research, elucidate their profound implications for society and the legal system, acknowledge the inherent limitations, and propose avenues for future research.

The analysis has underscored the fundamental role of crypto-anarchy in enabling cryptography and blockchain technology, empowering individuals to reclaim control over their data, finances, and identities. Through the exploration of practical applications such as DAOs and DeFi platforms, how these technologies serve as catalysts for democratising governance and revolutionising financial systems have been demonstrated. By leveraging smart contracts and decentralised networks, DAOs automate decision-making processes and resource allocation, while DeFi platforms facilitate peer-to-peer transactions and access to a wide range of financial services. These practical manifestations of crypto-anarchy not only challenge traditional power structures but also offer viable alternatives for fostering economic liberation and collaborative innovation.

The implications of crypto-anarchy extend across societal and legal domains, presenting both opportunities and challenges. From a societal perspective, decentralised technologies hold the promise of fostering greater individual autonomy, economic empowerment, and creative expression. However, from a legal standpoint, the rise of crypto-anarchy introduces complexities that demand innovative regulatory responses. Jurisdictional ambiguity, regulatory compliance, and investor protection emerge as pressing concerns, highlighting the need for adaptive legal frameworks that strike a delicate balance between fostering innovation and safeguarding public interests.

While the present research has shed light on the transformative potential of crypto-anarchy, it is essential to acknowledge certain limitations inherent in our analysis. Firstly, the rapidly evolving nature of decentralised technologies presents challenges in keeping pace with regulatory developments and understanding emerging risks and opportunities. Additionally, governance challenges such as scalability limitations and environmental impacts associated with blockchain technology raise questions about the long-term sustainability and adoption of decentralised systems. Furthermore, the pseudonymous nature of cryptocurrencies and the potential for illicit activities pose challenges for regulatory enforcement and consumer protection.

To address these limitations and further advance our understanding of crypto-anarchy, future research endeavours should focus on several key areas. Interdisciplinary studies that integrate perspectives from technology, law, economics, and sociology are essential for developing comprehensive frameworks that account for the multifaceted nature of decentralised technologies. Comparative analyses of regulatory approaches across different jurisdictions offer valuable insights into effective strategies for navigating legal complexities and promoting innovation. Furthermore, research focused on enhancing scalability, security, and sustainability in blockchain networks will contribute to the long-term viability and societal acceptance of decentralised technologies.

11 Conclusion

This paper has sought to enrich the academic discourse surrounding crypto-anarchy, shedding light on its significance in parallel with more established cypherpunk ideals. While initially confined to the realm of technological literature upon its emergence in 1992, crypto-anarchy has since garnered increasing attention across diverse academic domains, particularly in light of the recent proliferation of crypto-based technologies like blockchain, cryptocurrencies, and associated innovations such as DAOs and DeFi.

This surge in scholarly interest underscores the profound ethical implications inherent in these technologies. Noteworthy scholars, including Chohan [51], García-Siñeriz [90], Swartz [190], Sajter [169], Hütten [108], Brunton [42], Groos [97], Jarvis [115], Swann [189], Brekke [39], Brekke & Alsindi [40], Jara-Vera [114], Brekhov [38], and Nabben [149], have explicitly grappled with and defined the concept of crypto-anarchy.

Furthermore, this paper has endeavored to elucidate the foundational philosophical and political tenets underpinning crypto-anarchy, such as the pivotal role of anonymity in safeguarding privacy, individual autonomy, and freedom of expression. Additionally, cryptography and blockchain technologies have emerged as linchpins of decentralisation, while principles like freedom from government intervention, economic liberty, and collaborative open-source development have assumed paramount importance.

By highlighting the nuanced interplay between these principles and their implications for crypto technologies, this paper has underscored the need for adaptive regulatory frameworks to navigate the evolving landscape. To this end, it is recommended that a collaborative task force be convened, comprising experts from diverse disciplines—including law, technology, economics, and cybersecurity—to undertake a comprehensive study of the impact of crypto technologies on the legal system and devise effective regulatory strategies that balance innovation with regulatory oversight.

Acknowledgements The author has no acknowledgements to declare.

Author contributions The author conducted an in-depth analysis of the sources and existing literature on crypto-anarchy, provided critical insights on the implications of crypto-anarchy on society and the legal system, and was responsible for writing and revising the manuscript.

Funding This research did not receive any funding.

Data Availability Not applicable. There is no data associated with this article.

Declarations

Ethical Approval Not applicable. This article does not contain any studies with human participants performed by any of the authors.

Informed Consent Not applicable. This article does not contain any studies with human participants performed by any of the authors.

Conflict of interest The author declares that there is no conflict of interest.

References

1. Aanestad, M., Kankanhalli, A., Maruping, L., Pang, M.S., Ram, S.: Digital technologies and social justice. MIS Q. **17**, 515–536 (2021)
2. Akdeniz, Y.: Anonymity, democracy, and cyberspace. Soc. Res. Int. Q. **69**(1), 223–237 (2002)
3. Akmut, C.: European hackers: source documents for the history of the Chaos Computer Club, its magazine, its conference (2022)
4. Alexander, C., Cumming, D. (eds.): Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation. Wiley, Hoboken (2022)
5. Allah-Rakha, N.: Rethinking digital borders to address jurisdiction and governance in the global digital economy. Int. J. Law Policy 2(1) (2024)
6. Altinkemer, K., Rees, J., Sridhar, S.: Vulnerabilities and patches of open source software: an empirical study. J. Inf. Syst. Secur. **4**(2), 3–25 (2008)
7. Ammous, S.: The Bitcoin Standard: The Decentralized Alternative to Central Banking. Wiley, Hoboken (2018)
8. Anamika, A., Subramaniam, S.: Do news headlines matter in the cryptocurrency market? Appl. Econ. **54**(54), 6322–6338 (2022)
9. Anderson, E.: Private Government: How Employers Rule Our Lives (and why we don't talk about it). Princeton University Press, Princeton (2017)
10. Anderson, R.: Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, Hoboken (2020)
11. Antonopoulos, A.M., Harding, D.A.: Mastering Bitcoin. O'Reilly Media Inc (2023)
12. Ao, W., Fu, S., Zhang, C., Huang, Y., Xia, F.: A secure identity authentication scheme based on blockchain and identity-based cryptography. In: 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET) (pp. 90–95). IEEE (2019)
13. Asenbaum, H.: Anonymity and democracy: absence as presence in the public sphere. Am. Polit. Sci. Rev. **112**(3), 459–472 (2018)
14. Asenbaum, H.: The Politics of Becoming: Anonymity and Democracy in the Digital Age. Oxford University Press, Oxford (2023)
15. Ash, T.G.: Free Speech: Ten Principles for a Connected World. Yale University Press, New Haven (2016)
16. Atzori, M.: Blockchain Technology and Decentralized Governance: Is the State Still Necessary?. SSRN 2709713 (2015)
17. Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., Victor, F.: The Technology of Decentralized Finance (DeFi). Bank for International Settlements, Monetary and Economic Department (2023)
18. Balkin, J. M.: Digital speech and democratic culture: a theory of freedom of expression for the information society. In: Law and Society Approaches to Cyberspace, pp. 325–382. Routledge (2017)
19. Barendt, E.: Balancing freedom of expression and privacy: the jurisprudence of the Strasbourg Court. J. Med. Law **1**(1), 49–72 (2009)
20. Barlett, C.P.: Anonymously hurting others online: The effect of anonymity on cyberbullying frequency. Psychol. Pop. Med. Cult. **4**(2), 70 (2015)
21. Barlow, J.P.: A declaration of the independence of cyberspace. Duke L. Tech. Rev. **18**, 5 (2019)
22. Barnes, P.: Crypto currency and its susceptibility to speculative bubbles, manipulation, scams and fraud. J. Adv. Stud. Finance JASF **9**(2), 60–77 (2018)
23. Barreiro, M. F.: The power of Blockchain: decentralization (2022).
24. Bartlett, J.: The People Vs Tech: How the Internet is Killing Democracy (and how we save it). Random House, New York (2018)
25. Basu, S., Easley, D., O'Hara, M., Sirer, E.G. Towards a functional fee market for cryptocurrencies. arXiv:1901.06830 (2019)
26. Baudier, P., Kondrateva, G., Ammi, C., Seulliet, E.: Peace engineering: the contribution of blockchain systems to the e-voting process. Technol. Forecast. Soc. Chang. **162**, 120397 (2021)
27. Beltramini, E.: Against technocratic authoritarianism: a short intellectual history of the cypherpunk movement. Internet Hist. **5**(2), 101–118 (2021). https://doi.org/10.1080/24701475.2020.1731249
28. Beltramini, E.: The cryptoanarchist character of Bitcoin's digital governance. Anarchist Stud. **29**(2), 75–99 (2021). https://doi.org/10.3898/AS.29.2.03
29. Benhabib, S.: The Rights of Others: Aliens, Residents, and Citizens. Cambridge University Press, Cambridge (2004)
30. Benhabib, S.: Situating the Self: Gender, Community, and Postmodernism in Contemporary Ethics. Routledge (2020)
31. Benjamin, R.: Race after Technology: Abolitionist Tools for the New Jim Code. Polity Press, Cambridge (2019)
32. Benkler, Y.: The Wealth of Networks: How Social Production Transforms Markets and Freedom. Yale University Press, New Haven (2006)
33. Berlin, I.: Two concepts of liberty. In: Liberty Reader, pp. 33–57. Routledge (2017)
34. Bodó, B., De Filippi, P.: Trust in context: the impact of regulation on blockchain and DeFi. In: Blockchain and Society Policy Research Lab Research Nodes, vol. 1 (2022)
35. Bodó, B., Brekke, J.K., Hoepman, J.H.: Decentralisation: a multidisciplinary perspective. Internet Policy Rev. **10**(2), 1–21 (2021)
36. Bose, P., Das, D., Chen, Y., Feng, Y., Kruegel, C., Vigna, G.: Sailfish: Vetting smart contract state-inconsistency bugs in seconds. In: 2022 IEEE Symposium on Security and Privacy (SP), pp. 161–178. IEEE (2022)
37. Boss, S.: DAOs: Legal and empirical review. In: Blockchain and Society Policy Research Lab Research Nodes, vol. 2 (2023)
38. Brekhov, G.S.: Crypto-anarchism: the ideology of blockchain technologies. RUDN J. Polit. Sci. **24**(3), 393–407 (2022)
39. Brekke, J.K.: Hacker-engineers and their economies: the political economy of decentralised networks and 'cryptoeconomics.' New Polit. Econ. **26**(4), 646–659 (2021). https://doi.org/10.1080/13563467.2020.1806223
40. Brekke, J.K., Alsindi, W.Z.: Cryptoeconomics. Internet Policy Rev. **10**(2), 1–8 (2021). https://doi.org/10.14763/2021.2.1553
41. Brennan, A., Lo, Y. S.: Two conceptions of dignity: Honour and self-determination. In: Perspectives on Human Dignity: A Conversation, pp. 43–58. Springer, Dordrecht (2007)
42. Brunton, F.: Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency. Princeton University Press (2020)
43. Buterin, V.: A next-generation smart contract and decentralized application platform. White Paper **3**(37), 2–1 (2014)
44. Butun, I., Österberg, P., Song, H.: Security of the internet of things: vulnerabilities, attacks, and countermeasures. IEEE Commun. Surv. Tutor. **22**(1), 616–644 (2019)
45. Campbell-Verduyn, M.: Bitcoin, crypto-coins, and global anti-money laundering governance. Crime Law Soc. Chang. **69**, 283–305 (2018)
46. Cannataci, J. A., Zhao, B., Torres Vives, G., Monteleone, S., Bonnici, J. M., & Moyakine, E.: Privacy, Free Expression and Transparency: Redefining Their New Boundaries in the Digital Age. Unesco Publishing (2016)

47. Chauhan, A., Malviya, O. P., Verma, M., Mor, T. S.: Blockchain and scalability. In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 122–128. IEEE (2018)
48. Chen, W., Xu, Y., Zheng, Z., Zhou, Y., Yang, J. E., Bian, J.: Detecting "Pump & Dump Schemes" on cryptocurrency market using an improved Apriori Algorithm. In: 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), pp. 293–2935. IEEE (2019)
49. Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P., Zhou, Y. Detecting Ponzi schemes on ethereum: towards healthier blockchain technology. In: Proceedings of the 2018 World Wide Web Conference, pp. 1409–1418 (2018)
50. Chen, Y., Bellavitis, C.: Blockchain disruption and decentralized finance: the rise of decentralized business models. J. Bus. Ventur. Insights **13**, e00151 (2020)
51. Chohan, U. W.: Cryptoanarchism and cryptocurrencies. SSRN 3079241. (2017)
52. Chohan, U. W.: Cryptocurrencies and hyperinflation. In: Critical Blockchain Research Initiative (CBRI) Working Papers (2021a)
53. Chohan, U. W.: Decentralized finance (DeFi): an emergent alternative financial architecture. In: Critical Blockchain Research Initiative (CBRI) Working Papers (2021b)
54. Christman, J.: The Politics of Persons: Individual Autonomy and Socio-Historical Selves. Cambridge University Press, Cambridge (2009)
55. Christopherson, K.M.: The positive and negative implications of anonymity in internet social interactions: "on the internet, nobody knows you're a dog." Comput. Hum. Behav. **23**(6), 3038–3056 (2007)
56. Chua, H.N., Ooi, J.S., Herbland, A.: The effects of different personal data categories on information privacy concern and disclosure. Comput. Secur. **110**, 102453 (2021)
57. Ciocchetti, C.: Just click submit: the collection, dissemination, and tagging of personally identifying information. Vand. J. Ent. Tech. L. **10**, 553 (2007)
58. Claeys, G., Demertzis, M., Efstathiou, K.: Cryptocurrencies and monetary policy (No. 2018/10). In: Bruegel Policy Contribution (2018)
59. Cohen, J.E.: Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale University Press (2012)
60. Cohen, J.E.: Between Truth and Power. Oxford University Press (2019)
61. Coleman, G.: Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. Verso Books, London (2015)
62. Corbet, S. (Ed.). Understanding Cryptocurrency Fraud: The Challenges and Headwinds to Regulate Digital Currencies (vol. 2). Walter de Gruyter GmbH & Co KG (2021)
63. Cross, K. A.: Ethics for cyborgs: On real harassment in an "unreal" place. Loading 8(13) (2014)
64. DAOstack Arc.js. (2018). npm. Retrieved March 1, 2024, from https://www.npmjs.com/package/daostack-arc-js
65. De Filippi, P., & Loveluck, B. (2016) The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. Internet Policy Rev. 5(4)
66. De Filippi, P., Wright, A.: Blockchain and the Law: The Rule of Code. Harvard University Press, Cambridge (2018)
67. De Filippi, P., Mannan, M., Reijers, W.: Blockchain as a confidence machine: the problem of trust and challenges of governance. Technol. Soc. **62**, 101284 (2020)
68. Dhillon, V., Metcalf, D., Hooper, M., Dhillon, V., Metcalf, D., Hooper, M. The DAO hacked. In: Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You, pp. 113–128
69. Docksey, C.: Four fundamental rights: finding the balance. Int. Data Privacy Law **6**(3), 195–209 (2016)
70. Doumenis, Y., Izadi, J., Dhamdhere, P., Katsikas, E., Koufopoulos, D.: A critical analysis of volatility surprise in Bitcoin cryptocurrency and other financial assets. Risks **9**(11), 207 (2021)
71. Dragu, T., Lupu, Y.: Digital authoritarianism and the future of human rights. Int. Organ. **75**(4), 991–1017 (2021)
72. Eigelshoven, F., Ullrich, A., Parry, D. A.: Cryptocurrency market manipulation: a systematic literature review. In: International Conference on Information Systems (2021)
73. El Faqir, Y., Arroyo, J., Hassan, S.: An overview of decentralized autonomous organizations on the blockchain. In Proceedings of the 16th International Symposium on Open Collaboration, pp. 1–8. (2020)
74. Electronic Frontier Foundation: Global Coalition to Facebook: "Authentic" Names Are Authentically Dangerous for Your Users. Retrieved February 16, 2024 from https://www.eff.org/es/deeplinks/2015/10/global-coalition-facebook-authentic-names-are-authentically-dangerous-your-users (2015)
75. Electronic Frontier Foundation: Anonymity. Retrieved February 16, 2024 from https://www.eff.org/es/issues/anonymity (n.d.)
76. European Digital Rights: Who we are. EDRi. Retrieved February 16, 2024 from https://edri.org/about-us/who-we-are/ (n.d.)
77. European Union:Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. Retrieved March 1, 2024, from https://eur-lex.europa.eu/eli/reg/2016/679/oj (2016)
78. Faqir-Rhazoui, Y., Arroyo, J., Hassan, S.: A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain. J. Internet Serv. Appl. **12**(1), 1–20 (2021)
79. Ferguson, N., Schneier, B., Kohno, T.: Cryptography Engineering: Design Principles and Practical Applications. Wiley (2011)
80. Fiala, A.: Anarchism (2017)
81. Finck, M.: Blockchains: regulating the unknown. Ger. Law J. **19**(4), 665–692 (2018)
82. Frank, U., Strecker, S.: Open reference models-community-driven collaboration to promote development and dissemination of reference models. Enterp. Modell. Inf. Syst. Architect. (EMISAJ) **2**(2), 32–41 (2007)
83. Fraser, N.: Scales of Justice: Reimagining Political Space in a Globalizing World, vol. 31. Columbia University Press, New York (2009)
84. Fratrič, P., Sileno, G., Klous, S., van Engers, T.: Manipulation of the Bitcoin Market: An Agent-Based Study. Financ. Innov. **8**(1), 60 (2022)
85. Friedman, D.D.: The Machinery of Freedom: Guide to a Radical Capitalism. Open Court Publishing Company, Chicago (1989)
86. Fromm, E.: The escape from freedom. In: An Introduction to Theories of Personality, pp. 121–135. Psychology Press (2014)
87. Frommelt, E.: Liability challenges in the blockchain ecosystem. UC Davis Bus. LJ **21**, 165 (2020)
88. Gandal, N., Hamrick, J.T., Moore, T., Oberman, T.: Price manipulation in the Bitcoin ecosystem. J. Monet. Econ. **95**, 86–96 (2018)
89. Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol: analysis and applications. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 281–310. Springer, Berlin (2015)
90. García-Siñeriz, M. P.: In blockchain they trust–now, power to the people or to the invisible hand (2018)
91. Gillespie, T.: Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media. Yale University Press (2018)
92. Goldenfein, J., Hunter, D.: Blockchains, orphan works, and the public domain. Colum. JL Arts **41**, 1 (2017)

93. Golumbia, D.: The Politics of Bitcoin: Software as Right-Wing Extremism. University of Minnesota Press, Minneapolis (2016)
94. Grant, C.: Freedom and oppression. Polit. Philos. Econ. **12**(4), 413–425 (2013)
95. Greenberg, A.: This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cypherpunks Are Freeing the World's Information. Random House (2012)
96. Gritzalis, S.: Enhancing web privacy and anonymity in the digital era. Inf. Manag. Comput. Secur. **12**(3), 255–287 (2004)
97. Groos, J.: Crypto Politics: Notes on Sociotechnical Imaginaries of Governance in Blockchain Based Technologies. Data Loam, pp. 148–170 (2020)
98. Hamilton, T., Sharma, S.: Power, power relations, and oppression: a perspective for balancing the power relations. Peace Res. 21–41 (1996)
99. Harvey, C.R., Ramachandran, A., Santoro, J.: DeFi and the Future of Finance. Wiley (2021)
100. Henkin, L.: Privacy and autonomy. Columbia Law Rev. **74**, 1410 (1974)
101. Herian, R.: Regulating Blockchain: Critical Perspectives in Law and Technology. Routledge (2018)
102. Heyman, S.J.: Righting the balance: an inquiry into the foundations and limits of freedom of expression. BUL Rev. **78**, 1275 (1998)
103. Hildebrandt, M.: Smart Technologies and the End (s) of Law: Novel Entanglements of Law and Technology. Edward Elgar Publishing, Cheltenham (2015)
104. Hochschild, A.R.: Strangers in Their Own Land: Anger and Mourning on the American Right. The New Press, New York (2018)
105. Huang, C., Trangle, A.S.H.E.R.: Anti-Money Laundering and Blockchain Technology. Harvard University, Cambridge (2020)
106. Hughes, E., May, T. C.: Crypto Glossary | Satoshi Nakamoto Institute (1992). Retrieved March 1, 2024, from https://nakamotoinstitute.org/crypto-glossary/
107. Hughes, E.: "A Cypherpunk's Manifesto." Retrieved March 1, 2024, from https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt (1993)
108. Hütten, M.: The soft spot of hard code: blockchain technology, network governance and pitfalls of technological utopianism. Glob. Netw. **19**(3), 329–348 (2019)
109. Islam, M. R., Rahman, M. M., Mahmud, M., Rahman, M. A., Mohamad, M. H. S.: A review on blockchain security issues and challenges. In: 2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC), pp. 227–232. IEEE (2021)
110. Jacobetty, P., Orton-Johnson, K.: Blockchain imaginaries and their metaphors: organising principles in decentralised digital technologies. Soc. Epistemol. **37**(1), 1–14 (2023)
111. Jafar, U., Aziz, M.J.A., Shukur, Z.: Blockchain for electronic voting system—review and open research challenges. Sensors **21**(17), 5874 (2021)
112. Jafari, S., Vo-Huu, T., Jabiyev, B., Mera, A.: Cryptocurrency: a challenge to legal system. Reza, Cryptocurrency: A Challenge to Legal System (May 2, 2018) (2021)
113. James, M.: The other civil society: organised crime in fragile and failing states. Def. Stud. **12**(2), 218–256 (2012)
114. Jara-Vera, V.: New directions in crypto-politics. J. Libert. Stud. **25**(1) (2022)
115. Jarvis, C.: Crypto Wars: the Fight for Privacy in the Digital Age: A Political History of Digital Encryption. CRC Press, Cambridge (2020)
116. Jarvis, C.: Cypherpunk ideology: objectives, profiles, and influences (1992–1998). Internet Hist. **6**(3), 315–342 (2022)
117. Jiang, B., Liu, Y., Chan, W. K.: Contractfuzzer: Fuzzing smart contracts for vulnerability detection. In: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, pp 259–269 (2018)
118. Jiang, S., Li, Y., Wang, S., Zhao, L.: Blockchain competition: the tradeoff between platform stability and efficiency. Eur. J. Oper. Res. **296**(3), 1084–1097 (2022)
119. Jonason, P.: The right to be forgotten: the balance between the right to privacy and freedom of expression. Eur. Rev. Public Law 30(1) (2018)
120. Joux, A.: Introduction to identity-based cryptography. In: Identity-Based Cryptography, pp. 1–12. IOS Press (2009)
121. Kaal, W.A., Calcaterra, C.: Crypto transaction dispute resolution. Bus. Lawyer **73**(1), 109–152 (2017)
122. Kalenzi, C.: Artificial intelligence and blockchain: how should emerging technologies be governed? Front. Res. Metr. Anal. **7**, 801549 (2022)
123. Kelty, C.M.: Two bits: The cultural significance of free software. Duke University Press, Durham (2020)
124. Klang, M., Murray, A. (eds.): Human Rights in the Digital Age. Psychology Press (2005)
125. Kociatkiewicz, J., Kostera, M.: Creativity out of chaos: anarchy and organizing. Hum. Resour. Dev. Int. **1**(4), 383–398 (1998)
126. Kshetri, N.: Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun. Policy **41**(10), 1027–1038 (2017)
127. Kyles, D. L.: Centralised control over decentralised structures: AML and CTF regulation of blockchains and distributed ledgers. In: Financial Technology and the Law: Combating Financial Crime, pp. 121–150. Springer International Publishing, Cham (2022)
128. Lansky, J.: Cryptocurrency survival analysis. J. Alternat. Invest. **22**(3), 55–64 (2020)
129. Lescrauwaet, L., Wagner, H., Yoon, C., Shukla, S.: Adaptive legal frameworks and economic dynamics in emerging tech-nologies: navigating the intersection for responsible innovation. Law Econ. **16**(3), 202–220 (2022)
130. Levy, C.: Anarchism, internationalism and nationalism in Europe, 1860–1939. Aust. J. Polit. History **50**(3), 330–342 (2004)
131. Levy, S.: Crypto: How the code rebels beat the government—saving privacy in the digital age. In: Penguin Press Science Series. Penguin Publishing Group (2002)
132. Lianos, I., Hacker, P., Eich, S., Dimitropoulos, G. (eds.): Regulating Blockchain: Techno-Social and Legal Challenges. Oxford University Press, Oxford (2019)
133. Liddell, H. G., Scott, R., Jones, H. S.: A Greek-English Lexicon/Compiled by Henry George Liddell and Robert Scott (1940)
134. Lu, C.: Cryptocurrency and digital assets: A positive tool for economic growth in developing countries. Available at SSRN 4177415 (2022)
135. Ludlow, P., Godwin, M.: High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace Digital Communication. MIT Press, New York (1996)
136. Malendowicz, P.: Non-anarchist anarchisms and anarchisms of non-anarchist origin in contemporary political thought Athenaeum. Polskie Stud. Politol. **75**, 67–86 (2022)
137. Markus, H.R., Schwartz, B.: Does choice mean freedom and well-being? J. Consum. Res. **37**(2), 344–355 (2010)
138. Marquez, D. A.: An Attempt at Democratizing Resource Allocation for Social Movements Using Decentralized Autonomous Organizations (Doctoral dissertation, Massachusetts Institute of Technology (2021)
139. May, T. C.: The crypto anarchist manifesto. In: High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace (1992)
140. May, T. C. Crypto anarchy and virtual communities. Timothy C. May (1994a).

141. May, C. "The Cyphernomicon." 1994. Retrieved March 1, 2024, from https://nakamotoinstitute.org/static/docs/cyphernomicon.txt. (1994b)
142. Mill, J. S. (2023) On liberty. In: BoD-Books on Demand
143. Mondal, M., Silva, L. A., & Benevenuto, F. (2017). A measurement study of hate speech in social media. In: Proceedings of the 28th ACM Conference on Hypertext and Social Media (pp. 85–94).
144. Monrat, A.A., Schelén, O., Andersson, K.: A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019)
145. Morozov, E.: The Net Delusion: The Dark Side of Internet Freedom. PublicAffairs
146. Möslein, F. Conflicts of Laws and Codes: Defining the Boundaries of Digital Jurisdictions. SSRN 3174823 (2018)
147. Mounk, Y.: The people vs. democracy: Why our freedom is in danger and how to save it. In: The People vs. Democracy. Harvard University Press (2018)
148. Mueller, T.: Empowering anarchy: Power, hegemony, and anarchist strategy. Anarch. Stud. **11**(2), 122–149 (2003)
149. Nabben, K.: Cryptoeconomics as governance: an intellectual history from "Crypto anarchy" to "cryptoeconomics". Internet Hist. 1–23 (2023)
150. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. In: Decentralized business review
151. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press (2016)
152. Nhan, J., Carroll, B.A.: The offline defense of the internet: an examination of the electronic frontier foundation. SMU Sci. Tech. L. Rev. **15**, 389 (2011)
153. Nissenbaum, H.: Privacy in context: technology, policy, and the integrity of social life. In: Privacy in context. Stanford University Press (2009)
154. Noble, S.: Algorithms of Oppression: How Search Engines Reinforce Racism. New York University Press, New York (2018)
155. Nussbaum, M. C.: Frontiers of justice: disability, nationality, species membership. In: Frontiers of Justice. Harvard University Press (2007)
156. Onuf, N., Klink, F.F.: Anarchy, authority, rule. Int. Stud. Quart. **33**(2), 149–173 (1989)
157. Owen, T.: Disruptive Power: The Crisis of the State in the Digital Age. Oxford Studies in Digital Poli (2015)
158. Papacharissi, Z.: A private sphere: Democracy in a digital age. Polity (2010)
159. Paralelní Polis. Cryptoanarchy Institute. Retrieved February 16, 2024 from https://www.paralelnipolis.cz/koncepty/cryptoanarchy-institute/ (n.d.)
160. Pasquale, F.: The Black Box Society: The Secret Algorithms that Control Money and Information. Harvard University Press (2015)
161. Peña-Calvin, A., Saldivar, J., Arroyo, J., Hassan, S.: A categorization of decentralized autonomous organizations: the case of the Aragon platform. IEEE Trans. Comput. Soc. Syst. (2023)
162. Pierro, G. A., Tonelli, R.: Can solana be the solution to the blockchain scalability problem?. In: 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), pp. 1219–1226. IEEE (2022)
163. Politou, E., Casino, F., Alepis, E., Patsakis, C.: Blockchain mutability: challenges and proposed solutions. IEEE Trans. Emerg. Top. Comput. **9**(4), 1972–1986 (2019)
164. Postigo, H.: Capturing fair use for the YouTube generation: the digital rights movement, the electronic frontier foundation and the user-centered framing of fair use. Inf. Commun. Soc. **11**(7), 1008–1027 (2008)
165. Preukschat, A., Reed, D.: Self-sovereign identity. Manning Publications (2021)
166. Putnam, R. D.: Bowling Alone: The Collapse and Revival of American Community. Simon and Schuster (2000)
167. Rengel, A.: Privacy as an international human right and the right to obscurity in cyberspace. Gron. J. Int. Law **2**(2) (2014)
168. Rodima-Taylor, D., Grimes, W. W.: Cryptocurrencies and digital payment rails in networked global governance: perspectives on inclusion and innovation. In: Bitcoin and Beyond, pp. 109–132. Routledge (2017)
169. Sajter, D.: Unblocking blockchain potentials. Zbornik radova Međunarodne naučne konferencije o digitalnoj ekonomiji DIEC **2**(2), 13–20 (2019)
170. Santos, F., Kostakis, V.: The DAO: a million dollar lesson in blockchain governance. School of Business and Governance, Ragnar Nurkse Department of Innovation and Governance (2018)
171. Schär, F.: Decentralized Finance: On Blockchain-and Smart Contract-Based Financial Markets. FRB of St. Louis Review (2021)
172. Schmitz, A., & Rule, C.: Online dispute resolution for smart contracts. J. Disp. Resol. **103** (2019)
173. Schneider, N.: Thank You, Anarchy: Notes from the Occupy Apocalypse. University of California Press (2013)
174. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley, Hoboken (2007)
175. Schweik, C., Evans, T., Grove, J. M.: Open source and open content: a framework for global collaboration in social-ecological research. Ecol. Soc. **10**(1), (2005)
176. Serracino-Inglott, P.: Is it OK to be an anonymous?. In The Ethics of Information Technologies, pp. 243–270. Routledge (2020)
177. Shermin, V.: Disrupting governance with blockchains and smart contracts. Strateg. Chang. **26**(5), 499–509 (2017)
178. Shin, D.D.: Blockchain: the emerging technology of digital trust. Telemat. Inform. **45**, 101278 (2019)
179. Shin, L.: The Cryptopians: Idealism, Greed, Lies, and the Making of the First Big Cryptocurrency Craze. Hachette (2022)
180. Smith-Bishop, C.: A ripple-turned-tidal wave: SEC v. ripple labs as an inflection point in the regulatory approach to innovation in complex systems. Campbell L. Rev. **44**, 335 (2021)
181. Solove, D. J.: The Digital Person: Technology and Privacy in the Information Age (vol. 1). NyU Press (2004)
182. Solove, D.J.: Understanding Privacy. Harvard University Press (2010)
183. Spindler, G., Schmechel, P.: Personal data and encryption in the European general data protection regulation. J. Intell. Prop. Info. Tech. Elec. Com. L. **7**, 163 (2016)
184. Stieglitz, E.J.: Anonymity on the internet: how does it work, who needs it, and what are its policy implications. Cardozo Arts Ent. LJ **24**, 1395 (2006)
185. Sudharsan, B., MP, N. K., Alagappan, M.: Secured electronic voting system using the concepts of blockchain. In: 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 0675–0681. IEEE (2019)
186. Sundararajan, A.: The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism. MIT Press (2017)
187. Sunstein, C.: # Republic: Divided Democracy in the Age of Social Media. Princeton University Press (2018)
188. Swan, M.: Blockchain: Blueprint for a new economy. O'Reilly Media Inc (2015)
189. Swann, T.: Anarchist cybernetics. The Institute for Anarchist Studies. https://anarchiststudies.org/acybernetics/ (2021)
190. Swartz, L.: What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. Cult. Stud. **32**(4), 623–650 (2018)
191. Tapscott, D., Tapscott, A.: Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin (2016)

192. Taskinsoy, J.: Bitcoin could be the first cryptocurrency to reach a market capitalization of one trillion dollars. SSRN 3693765 (2020)
193. Taylor, L.: What is data justice? The case for connecting digital rights and freedoms globally. Big Data Soc. **4**(2), 2053951717736335 (2017)
194. Trask, A., Bluemke, E., Garfinkel, B., Cuervas-Mons, C. G., Dafoe, A.: Beyond privacy trade-offs with structured transparency. arXiv:2012.08347 (2020)
195. Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. **18**(3), 2084–2123 (2016)
196. Tufekci, Z.: Twitter and Tear Gas: The Power and Fragility of Networked Protest. Yale University Press, New Haven (2017)
197. United Nations: Universal Declaration of Human Rights. Retrieved March 1, 2024, from https://www.un.org/en/universal-declaration-human-rights/ (1948)
198. United Nations: International Covenant on Civil and Political Rights. Retrieved March 1, 2024, from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (1966)
199. United States District Court, Southern District of New York: Retrieved March 5, 2023, from https://www.nysd.uscourts.gov/sites/default/files/2023-07/SEC%20vs%20Ripple%207-13-23.pdf (2023)
200. Valdivia, A.N.: Algorithms of oppression: how search engines reinforce racism by Safiya Umoja Noble. Fem. Form. **30**(3), 217–220 (2018)
201. Van Rijmenam, M., Ryan, P.: Blockchain: transforming your business and our world. Routledge (2018)
202. Vigna, P., Casey, M. J.: The age of cryptocurrency: how bitcoin and digital money are challenging the global economic (2015)
203. Vigna, P., Casey, M. J.: The truth machine: The blockchain and the future of everything. Picador (2019)
204. Voorhoof, D.: Internet and the right of anonymity. In: Proceedings of the Conference Regulating the Internet, Belgrade, 2010, pp. 163–173. Center for Internet Development (2011)
205. Wachhaus, A.: Governance beyond government. Adm. Soc. **46**(5), 573–593 (2014)
206. Walch, A.: Deconstructing'decentralization': Exploring the core claim of crypto systems (2019)
207. Webb, M.: Coding Democracy: How Hackers are Disrupting Power, Surveillance, and Authoritarianism. MIT Press (2020)
208. Weber, B.: Bitcoin and the legitimacy crisis of money. Camb. J. Econ. **40**(1), 17–41 (2016)
209. Weber, S.: The Success of Open Source. Harvard University Press (2004)
210. Werbach, K.: The Blockchain and the New Architecture of Trust. MIT Press (2018)
211. West, S.M.: Survival of the cryptic: tracing technological imaginaries across ideologies, infrastructures, and community practices. New Med. Soc. **24**(8), 1891–1911 (2022)
212. Wilson, C.: Cryptocurrencies: the future of finance? In: Contemporary Issues in International Political Economy, pp. 359–394 (2019)
213. Wright, A., De Filippi, P.: Decentralized blockchain technology and the rise of lex cryptographia. SSRN 2580664 (2015)
214. Xie, J., Yu, F.R., Huang, T., Xie, R., Liu, J., Liu, Y.: A survey on the scalability of blockchain systems. IEEE Netw. **33**(5), 166–173 (2019)
215. Young, I. M.: Justice and the politics of difference. In: The New Social Theory Reader, pp. 261–269. Routledge (2020)
216. Zetzsche, D.A., Arner, D.W., Buckley, R.P.: Decentralized finance (defi). J. Financ. Regul. **6**, 172–203 (2020)
217. Zuboff, S.: The age of surveillance capitalism. In: Social Theory Re-Wired, pp. 203–213. Routledge (2023)
218. Zuckerman, E.: Rewire: digital cosmopolitans in the age of connection. WW Norton and Company (2013)
219. Zyskind, G., Nathan, O.: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops, pp. 180–184. IEEE (2015)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.