Chapter III

Why Bitcoin?

"The most significant result of the sudden regulation of the once-mysterious and forbidden realm of cryptography and code by the grassroots class may have been the creation of a usable electronic currency." — "Out of Control" by Kevin Kelly

The Origins of Punk

Over forty years ago today, the Sex Pistols, a punk rock band, released their single "Anarchy in the UK," opening the door to the British punk movement.

During the grand celebration of Queen Elizabeth's 25th year on the throne, the Sex Pistols performed this infamous anti-royalty song, "God Save the Queen," on a boat. The lyrics went like this: "God save the queen, she isn’ t no human being, there is no future in England's dreaming... no future, no future, no future for you."

This act caused a tremendous uproar, leading to their arrest and banishment. Fleeing from the police, they left the UK in haste.

Ironically, their song reached the top of the BBC charts, and to quell the outrage, the BBC reluctantly moved their position to second place.

It was this group of defiant and talented young people who stood against everything conventional. The lead singer of the Sex Pistols once said they came together out of extreme frustration and despair, united by their inability to see hope. They refused to seek normal jobs because it was meaningless and nauseating.

They also said there was no way out for the world.

With not much emphasis on musical skills, simple and catchy melodies, and a few chords, the Sex Pistols were formed. They created "Anarchy in the UK," and with it, they embodied the spirit of punk.

In their lyrics, the Sex Pistols proclaimed, "I wanna be anarchy, I wanna be anarchy, oh what a name, and I wanna be an anarchist, get pissed, destroy!"

Although no one can truly define punk, the act of negating and destroying the established conservative norms, followed by rebuilding, undeniably lies at its core.

The expression and embodiment of the punk spirit later extended from music to fashion, architecture, film, literature, and eventually, cryptography.

The Three Cyberpunk Offshoots Beyond Space and Time

In the evolution of the punk spirit throughout subsequent eras, numerous branches emerged, with steampunk, dieselpunk, and cyberpunk being among the more popular ones. They represent the past future, present future, and the future itself, primarily distinguished by their attitudes towards technology and sources of energy.

Steampunk works often rely on a hypothetical new technology to create an alternate worldview parallel to the Western world of the 19th century. The novel "The Difference Engine" can be considered an early source of steampunk, as game developers constructed a whole new world filled with greasy machines and billowing smoke.

Dieselpunk themes are often set in the interwar years, around 1950 to 1960, a period when the world was buried in the aftermath of horrifying nuclear warfare. It depicted an environment where everyone had to be constantly vigilant amidst the

collapse of surroundings, order, and spirits. The game "Command & Conquer" is a prime example of dieselpunk.

Cyberpunk, on the other hand, is a subgenre of science fiction that revolves around themes related to computers or information technology and typically involves a plot where societal order is disrupted. Cyberpunk works often feature a monochromatic color palette, along with gloomy and damp weather. The scenes in "Blade Runner" are a quintessential example of the cyberpunk style.

While steampunk and dieselpunk are based on fictional and reimagined historical eras, cyberpunk is firmly rooted in a technological theme and often leans towards a more realistic portrayal.

Cyberpunk emerged during the turbulent post-Cold War era.

In 1984, American science fiction writer William Gibson depicted an advanced digital realm in "Neuromancer," which later became known as "cyberspace," paving the way for cyberpunk thought.

One of the defining features of cyberspace is that it allows participants to transcend physical limitations, enabling the interaction of consciousness with a virtual world. The classic science fiction film "The Matrix" accurately replicated this concept.

In the novel, the protagonist Case is tasked with infiltrating multinational corporations to steal confidential information. By connecting his nervous system to the global computer network, he navigates a digital space constructed by computers, engaging in the theft of classified data and participating in information warfare.

Cyberpunk, a fusion of "cyber" (referring to computers) and "punk," created a new subgenre centered around the "control of computer networks" and imbued with a "dystopian spirit and tragic undertones." It encompasses topics like hacking, virtual reality, artificial intelligence (AI), urban sprawl, wealth disparity, and more.

Thus, through its strong spirit of resistance and the use of technology as a weapon, cyberpunk reshapes society and human relationships in a whole new way. Michael Benedikt, a professor of architecture at the University of Texas at Austin, was particularly interested in this newly constructed virtual world and the novel social relations it entailed.

In the summer of 1989, Benedikt began planning a grand Cyber-Space Conference. Notable guests included William Gibson, the author of "Neuromancer," and Bruce Sterling, a science fiction writer who had twice received the Hugo Award.

The Cyber-Space Conference took place as scheduled in May 1990. At the Fraunhofer Center in Austin, participants engaged in intense discussions and brainstormed various imaginative ideas around the theme of cyberspace.

John Perry Barlow, an active member of the WELL website, also attended the conference. In the years leading up to the event, Barlow had become anxious about the invasion of cyberspace after FBI agents "broke into" his home due to his online discussions, exposing him to potential hackers.

Perhaps inspired by the conference, he founded the Electronic Frontier Foundation (EFF) with the goal of "extending the Constitution to cyberspace." In 1996, he released the "Declaration of the Independence of Cyberspace," asserting that "the

Internet is an independent world, free from the jurisdiction of any political powers." Independence and freedom from any external control are the hallmarks of cyberpunk. On the Reddit cyberpunk forum, you can find the phrase "high tech, low life." The flourishing high-tech world juxtaposed with a spiritually desolate and hungry existence serves as the crucible of cyberpunk.

Cryptopunks, advocating "no privacy, no freedom," are indeed emblematic of their origins.

The Rise of Crypto Pioneers and the Birth of Bitcoin

Let's rewind to 1992, when Timothy May, a former senior scientist and electronic engineer at Intel, typed the final line of code in his California home, giving birth to the crypto anonymous mailing list. This revolutionary platform brought together 1,400 geeks who engaged in anonymous discussions, writings, and fearless expressions of their ideas in an unregulated digital wilderness.

Many of these individuals later became members of the Cypherpunk movement. Among them were prominent figures who would go on to exert significant influence in the later development of the Internet:

Tim May (Former Chief Scientist at Intel)

John Gilmore (Prominent employee at Sun Microsystems)

David Chaum (Influential figure in cryptography)

Phil Zimmermann (Developer of PGP technology)

Julian Assange (Founder of WikiLeaks)

Adam Back (Known as Adam Back)

Wei Dai (Possibly of Chinese descent, held in high regard)

Hal Finney (One of the inventors of PGP encryption)

Sir Tim Berners-Lee (Inventor of the World Wide Web)

John Perry Barlow (Cyber-libertarian political activist)

Nick Szabo (Inventor of BitGold and pioneer of smart contracts)

In this organization of crypto enthusiasts, there was another individual we are intimately familiar with—Satoshi Nakamoto. Although there were no direct evaluations of Satoshi within the mailing list, he emerged as a rising star in this community. Through the extensive research conducted by those who followed his footsteps, we can glean insights into Satoshi Nakamoto's status among these cyberpunks:

Hal Finney, one of the inventors of PGP encryption, served as an early collaborator with Satoshi Nakamoto.

In 2011, during Julian Assange's WikiLeaks campaign supporting Bitcoin donations, Satoshi Nakamoto made his last public appearance on the forum, where he cautioned against this move. Subsequently, WikiLeaks did not pursue further Bitcoin donations.

Kevin Kelly's portrayal of David Chaum, a pioneer in cryptographic currencies, in "Out of Control" from 20 years ago, underscores the importance of individuals in the field. Satoshi Nakamoto's status arguably exceeded even that of David Chaum.

Satoshi Nakamoto joined forces with these crypto pioneers, constantly influencing and reshaping the world. The rest of the story is well-known to all of us—the

emergence of Bitcoin, a technology that swiftly spread worldwide, incorporating elements of cryptography, distributed storage, and more.

Rome was not built in a day, and the history of cypherpunks follows a similar pattern, leaving footprints along the course of time. These rebels of the new world, transitioning from the era of cyberpunk to cypherpunk, fought for freedom and a better world, as expressed in the "Cypherpunk Manifesto":

"Our task is to build an open society from the ruins of the failed utopia. We will never go back to the shadows again."

This manifesto, penned in 1993, anticipated concepts like anonymous transactions, secure communications, digital signatures, and electronic cash—all of which would play pivotal roles in the development of Bitcoin and the broader cryptocurrency movement.

The 1993 manifesto was truly ahead of its time, touching upon concepts like anonymous transactions, anonymous communications, cryptographic signatures, and electronic cash:

"In an open society, privacy requires anonymous transaction systems of some sort. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system enables individuals to reveal their identity when and only when they choose to; this is the essence of privacy."

As time marches forward, the Cypherpunks are advancing in stride with the changing times, alongside their cyberpunk predecessors.

Cyberpunks indulged day after day in fantasies, imagining that they could achieve fame and fortune with cutting-edge and astonishing technology. In reality, they could often be found in their daily lives, logging into chat tools and engaging in discussions—a lifestyle reminiscent of 20th-century geeks.

Being a "geek" is not necessarily pejorative; many modern tech geniuses proudly self-identify as "geeks" because they prefer staying indoors and are known to enjoy their favorite drink, cola, often referred to as "geeky happiness water."

Tech enthusiasts, while sipping their geeky happiness water, diligently type away at their keyboards. Fueled by an immense passion for technology, they are unwilling to be constrained by the limits of the real world, yearning for a space of freedom.

"Freedom or Death."

When technological shackles restricted the tide of freedom, someone had to step forward to break the deadlock.

In the 1970s, cryptographic technology seemed like a "canary in a cage," imprisoned and controlled by the U.S. military, with cryptographers falling under its authority.

A turning point occurred in 1976 when cryptographic experts Whitfield Diffie and Martin Hellman introduced a groundbreaking form of asymmetric encryption and published the popular science book "New Directions in Cryptography." This technology is the cornerstone of modern internet security.

The lifting of encryption technology restrictions triggered fervent public debates. Should it be freely used, or should it be strictly controlled? This debate reached its peak in the late 1980s.

There was no definitive answer, but that did not mean the story came to an end. Another story quickly unfolded, giving birth to a new future.

The new story unfolded in 1992, as described at the beginning, when the gathering of the Cypherpunk organization—a meeting that would significantly influence the history of blockchain—echoed like thunder on flat ground, impacting generations to come.

Amateur cryptography enthusiasts questioned every assertion, and the storytellers patiently explained the issues repeatedly until consensus was reached.

Amid these ongoing discussions, they embarked on one project after another. A distributed computing tool was born, and a component previously concealed under the veil of military secrecy found its way onto the open internet, laying the early foundation of the internet.

After the formation of the Cypherpunk group, they directly experienced the achievements of public key encryption and PGP encryption in controlling access to digital information.

The encryption program PGP (Pretty Good Privacy), born in 1991, was a significant milestone in the history of encryption technology. This entirely free program greatly expanded the public's awareness of encryption technology.

However, governments worldwide were concerned that this newfound freedom might jeopardize their control over information and declared their intention to restrict the widespread dissemination of these encryption tools.

Timothy May realized that encryption would fundamentally alter the nature of business and government intervention in economic activities. After this small private discussion, the participants came up with a cool name for their group: Cypherpunks—a name symbolizing the defense of citizens' privacy in the digital world.

One week later, one of the participants, Eric Hughes, wrote a program that implemented the functionality of "receiving encrypted emails, erasing all identity markers, and sending them back to the user list." This program became the means of communication among members of the Cypherpunk group, which numbered around 1400 individuals.

The pursuit of anonymity and privacy by the Cypherpunks aligns with the independence and decentralization principles of Bitcoin. However, this transition was not without its challenges.

As one of the early members of the Cypherpunks, Satoshi Nakamoto, who appeared nearly 17 years later, incorporated these ideas into the concept of Bitcoin. This transformation was influenced by foundational technologies, specific historical contexts, and economic environments.

According to Kevin, there was even a small group that initiated an activity called the "Information Liberation Front." They searched expensive (and hard-to-find) journals

for academic papers on cryptographic technology, scanned them using computers, and then anonymously posted them online, liberating them from copyright restrictions.

Such actions, if attempted today, might face copyright infringement issues. However, during that time, they used these "unlawful" means to enable more people to learn about cryptographic technology, further driving the development of the Cypherpunk movement.

In the late 1990s, David Chaum, a luminary in the field of cryptography and a member of the Cypherpunks, invented the Ecash electronic cash system. This system aimed to address the flaw in traditional debit cards, where centralized banks controlled transaction data. David's Ecash system allowed secure and anonymous internet payments. However, a genius's inherent suspicion and incompatibility with established systems prevented this system from gaining widespread global adoption.

In March 1997, members of the Cypherpunk mailing list received an announcement about the formal implementation of the "hash cash postage scheme." The sender was Adam Back, a fellow member of the Cypherpunk organization and a 26-year-old cryptographer. He later earned the title "Father of Hashcash," and the importance of hash algorithms for Bitcoin represents the accumulation and inheritance of technology.

Afterward, nearly every year witnessed critical technological milestones that brought history closer to Bitcoin.

In 1998, Wei Dai proposed the b-money distributed anonymous cash system. This project had a significant impact within the Cypherpunk community. However, it ultimately did not achieve the level of adoption commensurate with its reputation. One key reason was the design flaw in b-money that prevented it from addressing the "open cost calculation and agreement on a uniform price" issue among miners. Nevertheless, Wei Dai undeniably set a good precedent. The sparks of ideas generated by this thought would invisibly create some form of traction.

By 1999, peer-to-peer (P2P) technology had matured and become widely popular, as seen in technologies like BitTorrent (BT) downloads. From its definition – "participants in a network share some of their hardware resources (processing power, storage capacity, network connectivity, printers, etc.), these shared resources are used to provide services and content through the network, and they can be directly accessed by other peer nodes without the need for intermediate entities" – P2P essentially laid the framework for Bitcoin.

Six years later, Hal Finney, another creator of the PGP software, designed the "Reusable Proof of Work" (RPOW), a mechanism for achieving distributed consensus on cash transactions. The well-known Bitcoin Proof of Work (POW) mechanism, which became the basis for the concept of mining, also had its roots here.

With these developments, the theoretical foundation for Bitcoin was complete, awaiting the arrival of the hero who would perfect it. In this temporal context of

2008, Satoshi Nakamoto emerged amidst the global financial crisis, characterized by his mystery, wisdom, and ability to build upon the work of his predecessors. This made both him and Bitcoin a enigmatic technological phenomenon, leading to all the consequences we see today regarding Bitcoin's impact on blockchain.

From hash algorithms, b-money, and RPOW, or tracing back to even earlier history—the birth of the Cypherpunk organization—members of these circles, whether intentionally or unintentionally, participated in shaping Bitcoin.

Following this, another member of the Cypherpunk organization, Nick Szabo, further refined these ideas in an article called "Bit gold," which was published again in 2008. This article marked a significant milestone in the formation of Bitcoin's philosophical framework and the history of the development of digital property rights.

The first core attribute of "Bit Gold" is proof of work, starting with a "candidate string" that is essentially a random number.

Anyone can mathematically combine this string with another newly generated random number - a "hash." Due to the nature of hash collisions, the result will be a new, seemingly random string of numbers: the hash value. The only way to know what this hash value looks like is to create it in practice - otherwise, you cannot calculate or predict it.

For those familiar with Bitcoin, this text will sound familiar. It was the ideas of Dai and Nick Szabo that greatly influenced Satoshi Nakamoto.

Later that year, he anonymously published an article on a forum: "Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System," which had a groundbreaking impact on the world of the internet.

Some say that Satoshi Nakamoto is the Neo-Saintly of the digital age, bringing the aura of a cyberpunk creator from the Matrix, the savior of citizen privacy in the high-speed information flow of the internet.

The significance of cryptography to society is akin to the importance of the invention and improvement of the printing press in medieval Europe. The rise of the printing press altered the power structure of the medieval church, and cryptography is poised to fundamentally change the nature of businesses and arbitrary interference in economic transactions.

After the widespread dissemination of the printing press in the Middle Ages, people could freely read the Bible, and incendiary writings against the church could quickly spread among the masses.

Today, the rise of cryptography provides digital equivalents for interpersonal relationships in the real world. Cypherpunks freely distribute these tools, giving people the opportunity for free signatures and online anonymity, liberating them from imprisonment and surveillance. They are immersed in a utopia they are reluctant to leave.

Kevin Kelly once said, "The future has already arrived, it's just not evenly distributed in society yet."

Since Tim Berners-Lee invented the HTTP protocol, the internet has continuously surged like a tidal wave, covering the entire world. Over the past few decades, data collection and privacy breaches have become common topics on the internet, far from the "free, equal, and open" internet that Berners-Lee envisioned initially.

The cypherpunk movement's promotion of cryptography provides privacy to ordinary people who were once exposed to the public eye. Rooted in the internet, peer-to-peer encryption is tightly linked with electronic payments and is closely integrated with daily business transactions.

Bitcoin emerged in response to these developments.

Crypto Punk: Punk Art in Pictures

Even though Bitcoin had emerged, the heyday of the cypherpunks had passed.

One of the founders, John Gilmore, declared the dissolution of the cypherpunk organization around the turn of the millennium. In a public email, he stated, "This organization has been declining for a long time, but I don't know why more than 500 people are still receiving emails."

This chapter of passionate cypherpunk history slowly faded away in the deconstruction of time. As T.S. Eliot once said, "This is the way the world ends, not with a bang but a whimper."

The cypherpunk organization faded away quietly, like tiny snowflakes melting before spring. Those who had yearned for spring took it upon themselves to put an end to the last budding shoots.

At the North American Bitcoin conference, former cypherpunk members, rarely seen

in public, spoke of their journey. They said, "Our current success and progress come from developers, not Lamborghinis or noisy markets. You can't find Lamborghinis at a hackathon."

It's hard to imagine that such a conference took place in a strip club.

The collision of strip clubs, Lamborghinis, and crypto geeks is like a massive dyeing agent, each element rubbing off on the other, settling and neutralizing.

"We were destined to live in this era," Czesław Miłosz once gave Shakespeare's line to himself, writing it at the beginning of his memoirs. At this moment, I also want to give it to the cypherpunks of the past. Their era has come to a close, their figures shining conspicuously in the fading sunlight, gradually fading into the twilight.

In 2017, founders Matt Hall and John Watkinson of Larva Labs, a New York-based software company, created a software program capable of generating thousands of unique and peculiar-looking characters.

Initially, they thought the characters they created might have features of a smartphone app or a game. However, what they eventually got was a change model that could alter the norms of the digital art market and challenge the concept of ownership itself.

Inspired by the London Punk scene of the 1970s, many of these "Punks" have mohawks or wildly unconventional hairstyles.

Explaining further, Noah Davis, an expert in post-war and contemporary art at New York's Sotheby's, said, "CryptoPunks are a major component of the CryptoArt movement, and this auction is historic."

In March 2022, Yuga Labs, the creator of Bored Ape Yacht Club, acquired both CryptoPunks and Meebits. Through this acquisition, Yuga Labs expressed its intention to foster a "builder community" centered around these two projects, creating derivative works.

As Joe Corré once said, "Today's punk has become a part of commercialization and mainstream values."

BTCs: Enlightening On-Chain Assets for the Punk Era

The development of blockchain has extended and expanded most cryptographic technologies, but it has also become a fearful dark forest.

When everything can be easily manipulated by conspirators, there is no safe haven left.

Centralized exchanges (CEX) manipulation leaves no future for blockchain!

Project promoters using pickup artist (PUA) tactics leave no future for blockchain!

Rug pulls by malicious actors leave no future for blockchain!

Fraudulent schemes create a toxic environment that leaves no future for blockchain!

With anger and resistance, we shall destroy all false pretenses of decentralization.

A new era of asset punk movement begins!

Why BTCs and not something else?

Inheriting the bloodline of Bitcoin, BTCs is more than just an interesting experiment, unlike ordi. BTCs embodies the punk spirit of Bitcoin and criticizes the various malicious behaviors that harm the true blockchain ethos, establishing true fairness,

security, and decentralization in the realm of cryptocurrency.

As people awaken, everything is just beginning.

The arrival of BTCs is like V from "V for Vendetta," emerging from the hidden, digital, underground darkness to tell everyone:

"Tomorrow, a different world will begin!"