waves Labs
RESEARCH

Blockchain Fundamentals I

Think Like A Web 3 Iconoclast

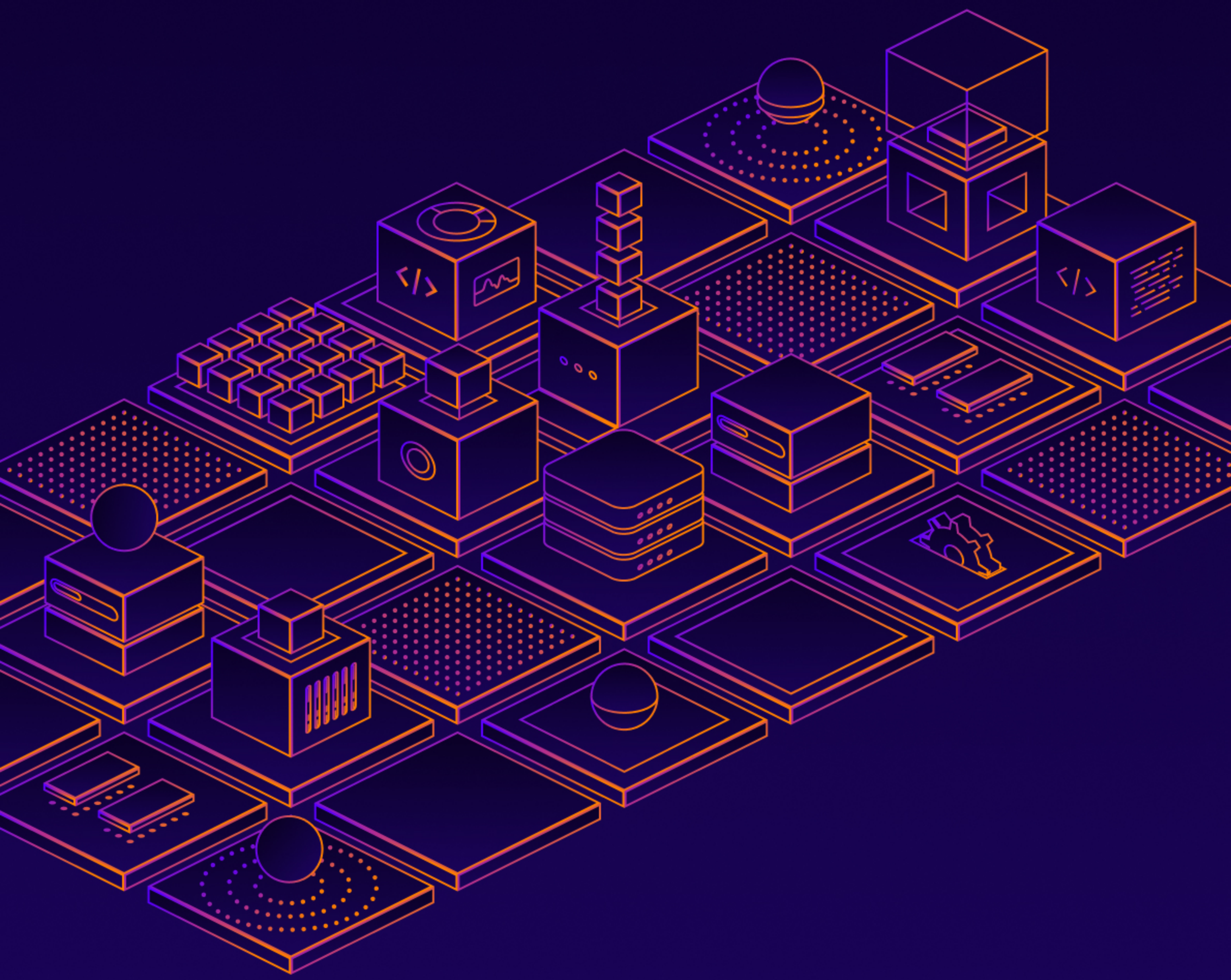


Table of Contents

Executive Summary

Blockchain Fundamentals I: Think Like A Web 3 Iconoclast explores the core values that motivate, guide, and inspire the developers and entrepreneurs who are building the next generation of decentralized applications.

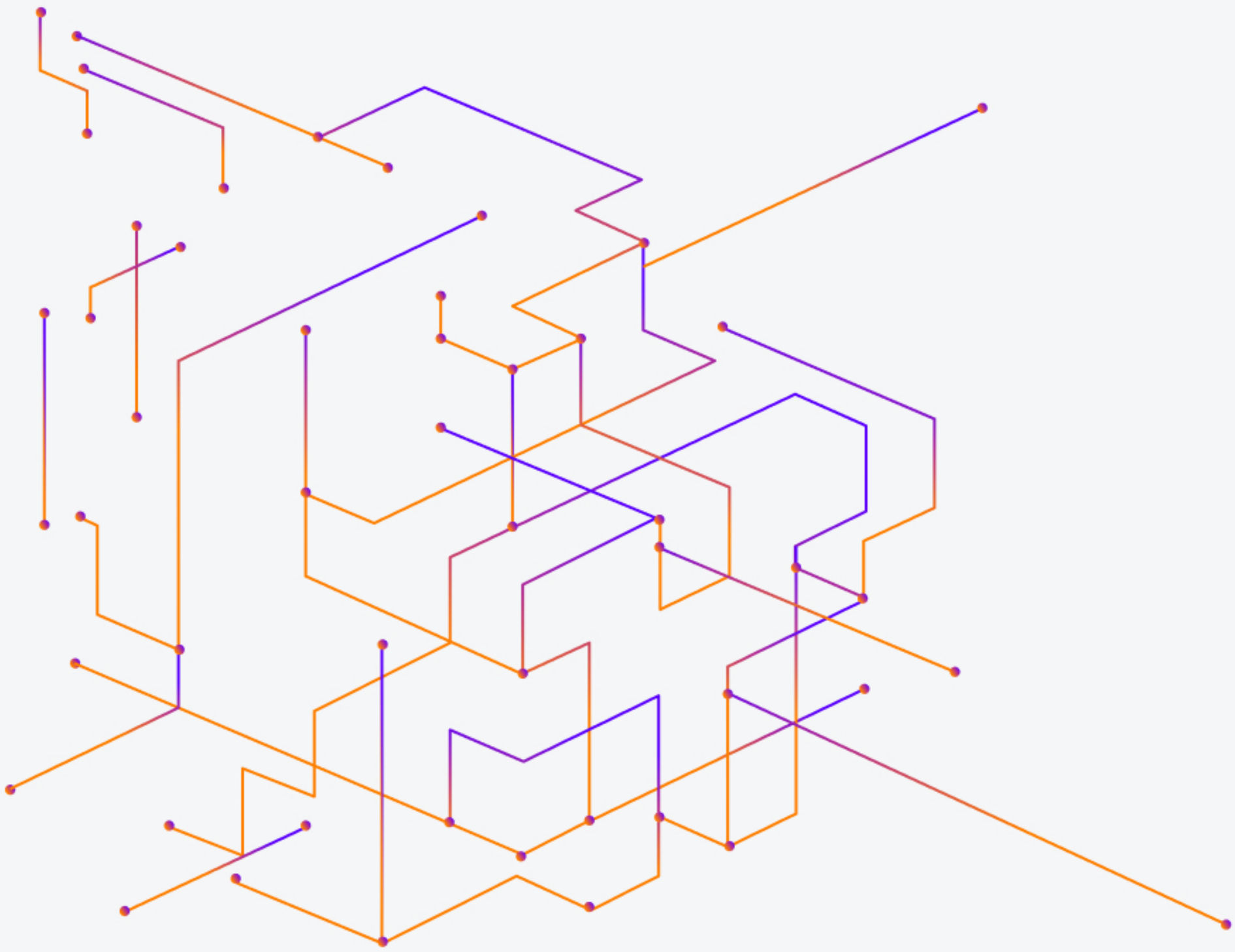
Blockchain technology sparked a paradigm shift in how individuals interact and exchange value in the digital world. The invention of the internet in the 1990s and the dominance of Web 2 tech giants transformed communication, information sharing and commerce at a global scale. However, a new breed of entrepreneur and developer is disrupting the Web 2 tech giants with innovative blockchain products, systems, and cryptoassets that reimagine how digital and financial products and systems work – and the purpose they serve. But how do they do it? What do they see that nobody else can?

First, the report traces the origins of the **cypherpunk values** to the practice of cryptography as established in ancient times, through to modern history as implemented by militaries during the World Wars. It examines Public Key Cryptography and Merkle Tree Cryptography as classified technologies that once made public, became technical expressions of the values of **trustless security** and **self-sovereignty**. Next, it shows the decades of legal battles to legitimate cryptography against the US Government as enshrining and the values of **censorship resistance** and **permissionlesness**. Then, it examines how innovations like untraceable email inspired the collective organization of the early cypherpunk community, enacting the values of **decentralization** and **privacy**.

Finally, this report unpacks the importance of distributed systems and how the invention of Bitcoin in the wake of the 2008 financial crisis represents a watershed moment for blockchain technology. It also looks toward what far-reaching impacts a decentralized monetary system may have on the world.

By defining and tracing core cypherpunk values through their early innovations, this report shows developers and entrepreneurs where decentralized blockchain technology insight originates. And from that perspective, how to find an original approach aligned with those values to disrupt centralized products and systems. The opportunity to help develop Web 3 is significant for builders looking to solve problems caused by centralization. Problems like systems that have a single point of failure, a lack of user privacy, insufficient transparency, inadequate accountability, or limited scalability.

The values guiding Web 3 technologists have been battle-tested through experimentation, litigation and activism over decades. Understanding them at their core is what differentiates developers and entrepreneurs in this industry, from those in legacy tech. After reading this report, you will understand what makes Web 3 so vital to humanity's future, and why encoding these values into tomorrow's solutions is one of the most rewarding technical challenges of our time.



Web 3 technologists are using decentralized technologies like blockchain and peer-to-peer networks to build the next evolution of the internet. Building in Web 3 gives users more control over their data and online identity, while increasing transparency, security, and privacy.

However, the builders and founders of today's successful Web 3 projects learned from the engineers, activists, and underground cypherpunks that came before them. Thriving Web 3 projects embody **cypherpunk values**, and understand cryptography, game theory design and Bitcoin at a fundamental level.

Blockchain technology bundles a series of technological innovations to create sustainable distributed systems without centralized decision-makers encroaching on individual freedoms. The fundamental values of the crypto space envision a world where average people have innate economic rights and are free from authoritarian governments and corporations.

Web 3 represents something far more powerful than many yet appreciate. It is an open space of ideas where brilliant developers and industrious entrepreneurs are already changing the world. The technology may be intimidating at first, but it is designed to be transparent and open to the public, not hidden or privatized.

The story of blockchain and Web 3 starts with the underground cypherpunk movement, and its technological and social innovations. To understand how to build a successful decentralized application (dApp), system or project, we need to start by understanding the actions and motivations of the original Web 3 pioneers.

Cypherpunk Values For A Digital Age

"Real punk is DIY — do it yourself." —Henry Rollins

TLDR

The seeds of today's Web 3 growth were planted decades ago. The cypherpunk values of decentralization, trustless security, privacy, permissionlessness, censorship resistance and self-sovereignty echo throughout crypto space today. These values are the foundation on which entrepreneurs and developers discover creative solutions to Web 1 and 2 era problems.

The cypherpunks were a community of activists interested in cryptography as a way to protect privacy and promote individual liberty. The cypherpunk movement took its name from the words "cipher" (a method of encryption) and "punk" (the counterculture and anti-establishment ethos). The movement eventually became an active community and played a key role in the development of cryptocurrency.

```
From: Eric Hughes <hughesNsoda.berkeley.edu>
Date: Mon, 21 Sep 92 22:47:51 PDT
To: cypherpunks@toad.com
Subject: No Subject
Message-ID: <9209220543.AA25094@soda.berkeley.edu>
MIME-Version: 1.0
Content-Type: text/plain



Welcome to the cypherpunks mailing list.

We have a real mailing list now, and not just a mail alias on my
account.  Thanks to John Gilmore for space on hoptoad and Hugh Daniel
for setting things up.

Mail to the list members at

        cypherpunks@toad.com

Request additions or deletions, talk to the list maintainer (me, Eric
Hughes) at

        cypherpunks-request@toad.com

Tell your friends about the list and have them join if they wish, and
have them do the same, but please do not post the list address yet.
We'd like to have a core group working before we advertise to avoid
diffusion of interest at the outset.
```

The cypherpunk community interacted online via the cypherpunk email list started by Eric Hughes, Tim May and John Gilmore from 1992 through to 2014. The community consisted of individuals who shared a common set of values: decentralization, trustless security, privacy, permissionlessness, censorship resistance, and self-sovereignty.

Through activism, entrepreneurship, and software development, cypherpunk principles evolved into the values that now guide the efforts of developers and entrepreneurs building today's Web 3 infrastructure.
To understand what makes a successful Web 3 project, you need to start by understanding the ethos of this pioneering movement — and the origin of that ethos is in the Cypherpunks actions and values.

The following is a summary of the core cypherpunk values described first in principle, and then in relation to blockchain technology.

1 Decentralization

In a decentralized system, power should be distributed across a majority of different individual stakeholders rather than centralized and under the control of one – or a select few.

Decentralized infrastructure is maintained by networks of miners or validators that share responsibility for keeping the network running. This design makes it very difficult for any one individual or group to seize control and eliminates the risk of a single point of failure.

2 Trustless Security

In a system with trustless security, individuals should not need to rely on third parties or intermediaries to facilitate transactions or interactions. Individuals should have full responsibility for the security of their information and transactions, and have the autonomy to decide how it is used, shared, or accessed.

Cryptocurrencies are often considered to be trustless because they allow for secure, direct, peer-to-peer transactions without the need for a trusted third-party.

3 Privacy

Any system used by individuals with civil liberties should preserve the user's right to privacy. Online, the use of strong encryption is the best way to protect this right at a technical level.

Cryptocurrencies by their nature, offer a high level of privacy, as transactions are often pseudonymous and can be made without revealing the identity of the counterparties involved.

4 Permissionlessness

Systems should be safe, freely available and accessible to the public. Individuals acting in good-faith should not be required to be granted permission to use it by any external actor.

Cryptocurrencies by their nature, are inclusive, transparent and enable the free flow of information and value. There is no administrator to assign database permissions in a decentralized system.

5 Censorship Resistance

In a censorship resistant system, individuals should be able to communicate and share information without fear of interference or censorship by external actors – no matter their power or influence.

Cryptocurrencies are often considered to be censorship-resistant because they allow users to transact economic value across the globe without any central authority being able to prevent it.

6 Self-sovereignty

In any self-custodial system, individuals should retain full control of their assets and information, without needing to trust a third-party intermediary.

Cryptocurrencies enable self-sovereignty by allowing individuals to hold and control their private keys, giving them full control over their assets.

Understanding where the cypherpunk movement came from will add depth to how each value evolved and will show how the actions of cypherpunks have put these values into practice, and in some cases, into laws.

Cryptography and Cypherpunk Prehistory

TLDR

Cypherpunk values developed over time with their spirit attributable to real world events. Trustless security and self-sovereignty developed out of the public research on private key cryptography. Censorship resistance and permissionlessness out of years of legal battles. Decentralization and privacy out of technical innovation and public experimentation.

Cypherpunk values emerged over decades of experimentation, activism and community action. Although Hughes (et. al)'s mailing is now defunct, it brought together people who continue to innovate Web 3 today. To really appreciate what makes successful Web 3 project founders
unique, we first need to understand the pre-history of the cypherpunk movement.
To understand the ethos that drove the early cryptopunks, we must look at the problems and creative solutions that they fought to build.

Cypherpunk prehistory starts with the academic breakthroughs of cryptography in the 1970s that made public, once-classified cryptographic techniques.[1] In the 1980s, there were critical attempts to build cryptographic digital money and other watershed experiments in privacy and decentralized systems.[2] Then in the 1990s, there were legal battles pleading the case for "cryptography as speech" that were fought – and won – by individuals from a then unknown, underground collective.[3]

Cryptography as we know it today, has its roots in the 1883 work of Auguste Kerckhoffs' six design principles for a secure cryptosystem: ease of use, key secrecy, key exhaustion, known attack resistance, portability and analyzability.[4] At its most basic level, cryptography is the practice of using techniques and tools to secure communication and protect data from unauthorized access or tampering. It involves the use of mathematical algorithms and protocols to encode and decode information, making it difficult for unauthorized parties to interpret or modify.

Cryptography has a long prehistory as a military technology, with the earliest known examples dating back to ancient civilizations like Egypt and Mesopotamia.[5] Cryptographic techniques and technology was also utilized heavily during both World Wars by all capable militaries to communicate without detection. Importantly, cryptographic techniques were historically kept classified, allowing some militaries a competitive advantage over others.

"Through activism, entrepreneurship, and software development, cypherpunk principles evolved into the values that now guide the efforts of developers and entrepreneurs building today's Web 3 infrastructure."

The end of the first World War set a precedent for trust and security standards of the 20th

century. The Treaty of Versailles established which governments and militaries could or could not be trusted with global security.[6] In the early post-war years, events like the implementation of the Federal Deposit Insurance Corporation (FDIC) in the US banking system formalized banks as custodians of trust and security – an authority that remains unchecked to this day.[7]

Institutional overreach can be seen in the management of identity on behalf of individuals. Local, regional, and national governments assign IDs, passports, and other social identification. Banks assign account numbers, balances, and authorized users. Tech companies assign email addresses, login credentials, and personal profiles. All forms of social identity are controlled by institutions, not their associated individuals.

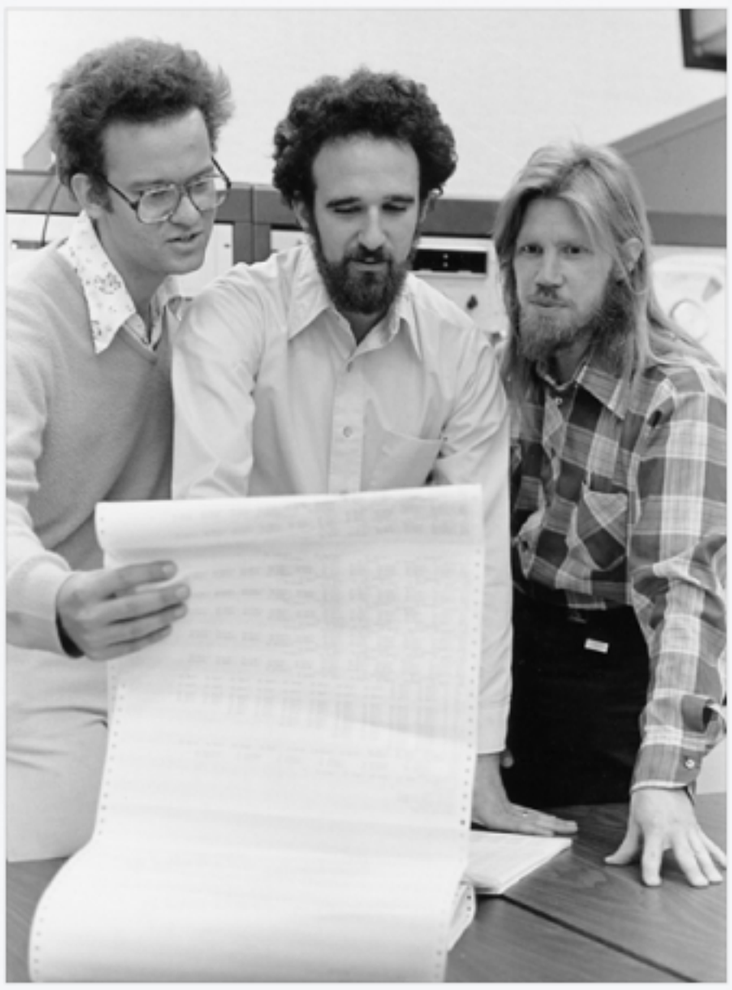
Through the latter half of the twentieth century, nations across the world continued to determine and define which governments were trustworthy and which were not. **This broad approach left no room for self-sovereign individuals to take responsibility for their own economic trust and security, and delegated personal decisions of identity, security, and wealth preservation to institutions.**

Trustless Security and Self-sovereignty

In wake of these world events, several passionate, innovative engineers started to build trustless security systems that were separate from the predefined global standards.

In the 1970s, computer scientists Martin Hellman and Whitfield Diffie developed a system for secure communication using a technique called **public-key cryptography**.[8] Hellman and Diffie's innovation allowed for the exchange of secure messages. **The security of public-key cryptography gave the public access to cryptographic security for the first time, and eventually led to the development of its most prolific use cases: the internet and cryptocurrency**. Hellman and Diffie's insight to use objective math instead of subjective institutional judgment to determine truth, planted the seeds for the cascade of innovations in cryptography that followed. Additionally, they removed identity from institutional authority to personal authority, as public keys could now replace many old systems.

With identity management removed from institutional authority, the next technical challenge was to ensure that communication between individuals preserved this trustless precedent. Individuals needed a way to send exchange messages directly, without relying on institutions or intermediaries to verify the accuracy of communication. **Public-key cryptography gave individuals autonomy over their personal data and identity which empowered them to become self-sovereign digital citizens of the world**.



RALPH MERKLE, MARTIN HELLMAN AND WHITFIELD DIFFIE

A few years later, Stanford PhD student Ralph Merkle created a system for individuals to manage digital data transfer online. Merkle's technique called the **'Merkle tree,'** allows secure communication systems to operate at scale.[9] A Merkle tree or hash tree, is a data structure that enables efficient and secure verification of large data sets by providing a short, condensed version of the data, called a hash, that can be easily compared to a previously calculated hash of the same data. Unlike private key cryptography, Merkle trees don't determine who is trustworthy and who is not, but instead provide

a mechanism for individuals to encrypt and transmit thei data in an independently verifiable way.

Merkle trees allowed cryptographically secure communication to scale by making it possible to efficiently verify large amounts of data. **Low latency is essential when coordinating between tens, hundreds, or thousands of individuals in a network**. When independently verifying a large dataset, it is not feasible to try to compare an entire dataset to a reference copy. The Merkle tree allows for the efficient verification of the integrity of a dataset by only requiring the comparison of a small number of hashes. Merkle trees also enhance security by making it easy for individuals to detect data modification or tampering.

Merkle's solution for secure, trustless data transmission was an elegant, yet highly sophisticated accomplishment. Thanks to the innovations of public-key cryptography and Merkle trees, **individuals now had the tools to control their identity and information and to reclaim the sovereignty and power that governments, militaries, and banks annexed in the twentieth century.**

Grounded in the fundamental truth of mathematics, Merkle, Hellman, and Diffie followed their curiosity and built the technology that would spread trustless cryptography across the world. Their desire to share this knowledge was innate in their identity as academics in pursuit of knowledge for the greater good. They quickly realized the potential this had for empowering individuals and worked tirelessly to spread these ideas to the world.

Censorship Resistance and Permissionless Action

During the 1980s, technology and software development outpaced lawmakers' understanding of how the technology worked. The rapid innovation led to a 'Wild West' environment on the internet and with it, a surge of sophisticated criminal hackers. **A small number of cyber attacks triggered a wave of vexatious litigation against honest internet users**. Dubbed Operation Sundevil, US law enforcement raided many companies and confiscated their equipment motivated by a fundamental ignorance on the hacker issue.

SJ Games, a small game development company is one example of the collateral damage. In the 1990's SJ Games skirted financial ruin over an unjust U.S. Secret Service raid. One employee's philosophical blogging about hacker culture was used to justify a raid and mass confiscation of the company's computer hardware. After four months without business equipment, the company narrowly avoided bankruptcy by laying off most of their workforce and sustaining near-catastrophic emotional and financial damages.[10] The company went on to counter-sue the agency and won two of three lawsuits. **The complete lack of hard evidence in their legal battle with SJ Games highlighted the government's utter misapprehension of the technology they were trying to protect.**

> "This broad approach left no room for self-sovereign individuals to take responsibility for their own economic trust and security, and delegated personal decisions of identity, security, and wealth preservation to institutions."

Cypherpunks developing cryptography were hindered by outdated legislation that lingered from cryptography's origins as a military technology. These outdated laws were formed in an era where information was exchanged on paper, and did not account for the digital revolution of the internet. Cryptography was governed under the Arms Export Control Act of 1976 which gave vague parameters about who was able to access such technology and share it.[11] Under some interpretations, sharing Cryptographic technology was legally equal with arms dealing.

Cypherpunks Go To Court

Cypherpunk values developed over time with their spirit attributable to real world events. Trustless security and self-sovereignty developed out of the public research on private key cryptography. Censorship resistance and permissionlessness out of years of legal battles. Decentralization and privacy out of technical innovation and public experimentation.

In April 1990, the FBI interrogated John Perry Barlow and Mitch Kapor, both members of online communities, regarding their alleged involvement in the hacker group NuPrometheus. During these interrogations, it became clear that the FBI did not understand the group's technology, raising concerns about the government's ability to respect the rights and freedoms of its users.

Barlow and Kapor went on to co-found the Electronic Frontier Foundation (EFF), an organization dedicated to protecting civil liberties in the digital world. The EFF was established in response to the growing number of threats to freedom and privacy posed by technology and the internet, and has since been working to defend free expression, innovation, and consumer rights online. It played a key role in shaping internet policy and law, and worked to educate the public about the importance of digital civil liberties.

There were several other key court cases in the nineties that challenged the legal classification of cryptography:

- In the 1996 case Bernstein v. The United States, Daniel J. Bernstein challenged the export controls on cryptographic software under the Export Administration Regulations. The court ruled that source code is protected speech under the First Amendment as free speech.[12]
- In the 1997 case Karn vs. The United States, programmer Phillip R. Karn argued that a physical print book containing cryptographic source code was not subject to the Munitions Act and should be protected under free speech.[13]
- And in 1998 Junger vs. In The United States, a law professor challenged the munitions regulation on the grounds that it violated the First Amendment and was eventually successful in 2000.[14] [15]

As a result of these court cases and Executive Order 13026 signed by President Bill Clinton in 1996, cryptography was removed from the munitions list, placed on a lightly controlled schedule, and the export of cryptography was no longer prohibited.

Philip Karns' public rebellion against this orthodoxy is permissonlessness in action. Printing cryptography in a physical book is the perfect analogy representing how physical rights should mirror digital rights. Written words are free speech as protected by the US constitution which anyone should be able to read and learn from. Books have been used for decades to signify freedom of information in the face of oppression and Karn's implementation of this symbolism illustrated that cryptography should be held in the same regard.

After a lengthy series of legal battles, the US justice system correctly identified the human rights inherent to cryptography. **Thanks to their tireless and vigorous litigation, the early cypherpunks' passion for censorship resistance, in that no central party should have the right to dictate harmless human behavior, brought cryptography to the general public.** Thanks to these unyielding cypherpunk developers, lawmakers learned to recognize the differences between applied cryptography's legitimate innovations and criminal behavior.

The demonstration of permissionless action and legal recognition of its merit allowed modern computer systems based on cryptography to be regulated as speech and set the precedent that participating in cryptography is also speech. With this designation, the cypherpunks made it clear that infringements and censorship of free speech will be met with intellectual and legal warfare.

" Thanks to their tireless and vigorous litigation, the early cypherpunks' passion for censorship resistance, in that no central party should have the right to dictate harmless human behavior, brought cryptography to the general public."

The fight against censorship took years of brutal court appearances, legal appeals, and effort. Luckily, a small group of individuals realized the importance of these fights and emanated the correct values. No future generations should have to fight the same battles again. The brave cypherpunks were highly motivated to install systems resistant to censorship and permissionless by default.

Decentralization and Privacy

As liberating technological and legislative victories continued to mount, the cypherpunks began building bottom-up systems of collaboration rather than top-down systems of authority.

As the nineties progressed, experiments with decentralized systems like the internet and SMTP email broke new ground, but institutional forces soon began infiltrating these efforts. SMTP email started as a decentralized network, but was reduced to a network of 4-5 providers with complete knowledge of their customers' information.[16] Tech conglomerates began to revert decentralized internet systems back to trusted and permissioned 'walled-garden' systems. Protecting internet infrastructure from tech company overreach would require innovations in decentralization, privacy and system architecture.

Despite these challenges, cryptography innovation proved unstoppable. In 1981, Berkley computer science PhD and cryptographer David Chaum developed "untraceable electronic mail," a system that allowed both a message and its metadata (ie. who sent it) to be encrypted, making email anonymous and untraceable.[17] Together, the ability to send anonymous, untraceable messages across secure, trustless decentralized networks sparked a new wave of creativity and ingenuity.

Chaum's idea worked for some time but more importantly, it inspired others to help build the decentralized future they wanted to see. **Email and the internet's devolution into centralization acted as cautionary tales for developers and entrepreneurs: without proper direction, the internet is vulnerable to the same centralizing forces that co-opted the global economy in the twentieth century**. This presented a difficult problem: Who would lead a rebellion against centralization without succumbing to the same forces?

Flash forward: Web 3 Builders Interview

How much do the cypherpunk values contribute to your decision or conviction in an investment?

It matters quite a lot. If Bitcoin didn't uphold the core crypto values I don't think we'd be where we are today. This contributes a lot in our decision making for investments because we want to see a better financial system and layer for everyone in the world. While a world that embodies these crypto values is ideal, it's not easy. That's why we at Magnus strive to find projects that create and scale these opportunities.

MAGNUS CAPITAL+

Fortunately, the solution to this problem may have formed organically. The cypherpunks represented a new paradigm of technologist, they aggressively protected their right to privacy. They believed that passivity in the face of breaches of privacy would result in the loss of personal privacy – a fundamental American value enshrined in the US constitution. Although the cypherpunks were a loosely affiliated group, they were fierce individualists at their core. **The cypherpunk community itself resembled the perfect architecture for a next-gen 'un-centralizable' internet infrastructure. In many ways, decentralization is the cypherpunks principle value, encompassing and supplanting all other core values.**

Most importantly, cypherpunks are builders and doers. Their actions bring their values to life, and encode them – literally – into protocols that others can freely use, share, break and improve. Some of the most successful early leaders include advocates like Julian Assange, technologists like the founders of TOR and Bittorrent, and the ephemeral author of the Bitcoin whitepaper.

A series of key decentralized projects grew out of the cypherpunk movement to defend free speech, enable secure private communication, enable direct peer-to-peer interaction and provide the world with its first natively digital asset:

- TOR (mid-1990s): An alternative secure, anonymous digital communication network
- BitTorrent (2001): A peer-to-peer file sharing system
- WikiLeaks (2006): A platform for anonymous whistleblowing
- Bitcoin (2009): Decentralized digital currency that ignited the Web 3 era

A loose collective of like-minded people decided they needed to organize for the betterment of the world. They worked together, without coercion in a decentralized fashion, to create technologies that respected and preserved individual privacy and autonomy. After much trial and error, their ideas were honed into products that did not reach mass adoption, but inspired the first decentralized distributed technology that would change the world economy.

In Pursuit of the Killer dApp

Although early cypherpunks created many innovative products, nearly all failed to penetrate to mainstream audiences. For example, despite being developed in the 1990's, the alternative internet routing protocol TOR remains relegated to niche communities and only represents 0.036% of today's internet usage.[18] Although TOR is a strong representation of cypherpunk values, the network failed to have worldwide impact.[19]

A prerequisite for any system designed for global use, is a global need or demand for its existence. The internet is a successful example. By the late nineties, people across the world needed an accessible way to instantly exchange information. The massive Web 2 tech giants that were built in the late nineties, ultimately met that need by providing a fast, cheap, and reliable system to serve people all over the world, at the expense of decentralization, trustless security, privacy, permissionlessness, censorship resistance, and self-soverignty.

> "The cypherpunk community itself resembled the perfect architecture for a next-gen 'un-centralizable' internet infrastructure. In many ways, decentralization is the cypherpunks principle value, encompassing and supplanting all other core values."

Built alongside the meteoric growth of Web 2, the cypherpunks kept building.
Asking themselves: What is the biggest unmet need of internet-connected individuals?

Cypherpunk legend Hal Finney's 1992 email proposed that what the world needed was a system to communicate economic value – the worth of a person's ideas and effort – to anyone, anywhere, instantly.[20] In other words: digital money.

Money requires security and usability rather than speed and ease of use. It needs to be trusted by the market without giving away individual sovereignty. It's been centuries since the idea of money entered the human lexicon and it has remained relatively unchanged since the days of the Greek drachma. **The cypherpunks saw digital money as the revolutionary decentralized technology next in line for global adoption.**

Chaum saw the opportunity in offering the world its first killer dApp, and went on to found DigiCash in 1989 launching 'ecash,' the world's first digital cash system a year later. The company attracted the attention of distinguished cryptographers, hiring Hal Finney, Nick Szabo, and Eric Hughes. Although DigiCash experienced some success, the company rejected a $180 million acquisition offer from Microsoft, and declared bankruptcy in 1991.

As it turns out, the problem of launching a decentralized currency was so great that no single public company or individual would be able to do it. The innovation came from the thoughts and words of an anonymous individual or collective (it's unclear which), known online by the moniker Satoshi Nakomoto, in a whitepaper titled: Bitcoin: A Peer-to-Peer Electronic Cash System.

The Discovery Of Decentralized Money

TLDR

Bitcoin arrived at the perfect time after the 2008 financial crisis. It represented a new invention, the invention of an independent monetary system. A few key technologies and innovations made this network possible. The decentralized network began to take root and with no vectors of attack from opponents, even at the nation state level.

The cypherpunks identified the opportunity to create a digital currency by harnessing the power of modern cryptography and the internet. Cryptographic money had been tried before Bitcoin, but all attempts had failed.

Bitcoin's ongoing success is the result of many factors, but is underpinned by its alignment with the core cypherpunk values engineered in code and mechanism design theory.[21] The ultimate challenge facing Bitcoin is: will it survive as the de facto globally distributed, decentralized monetary network?

Bitcoin was created by a person or group identified online by the pseudonym 'Satoshi Nakamoto'. Whoever Nakomoto is or was, they understood the power of practicing what you preach. Nakamoto is credited with creating version 0.1 of the Bitcoin software and is thought to be responsible for mining the first block on the Bitcoin network. To this day, the identity of the creator(s) of Bitcoin remains unknown, posts and emails are the only remaining evidence that Nakamoto ever existed.


THE TIMES

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

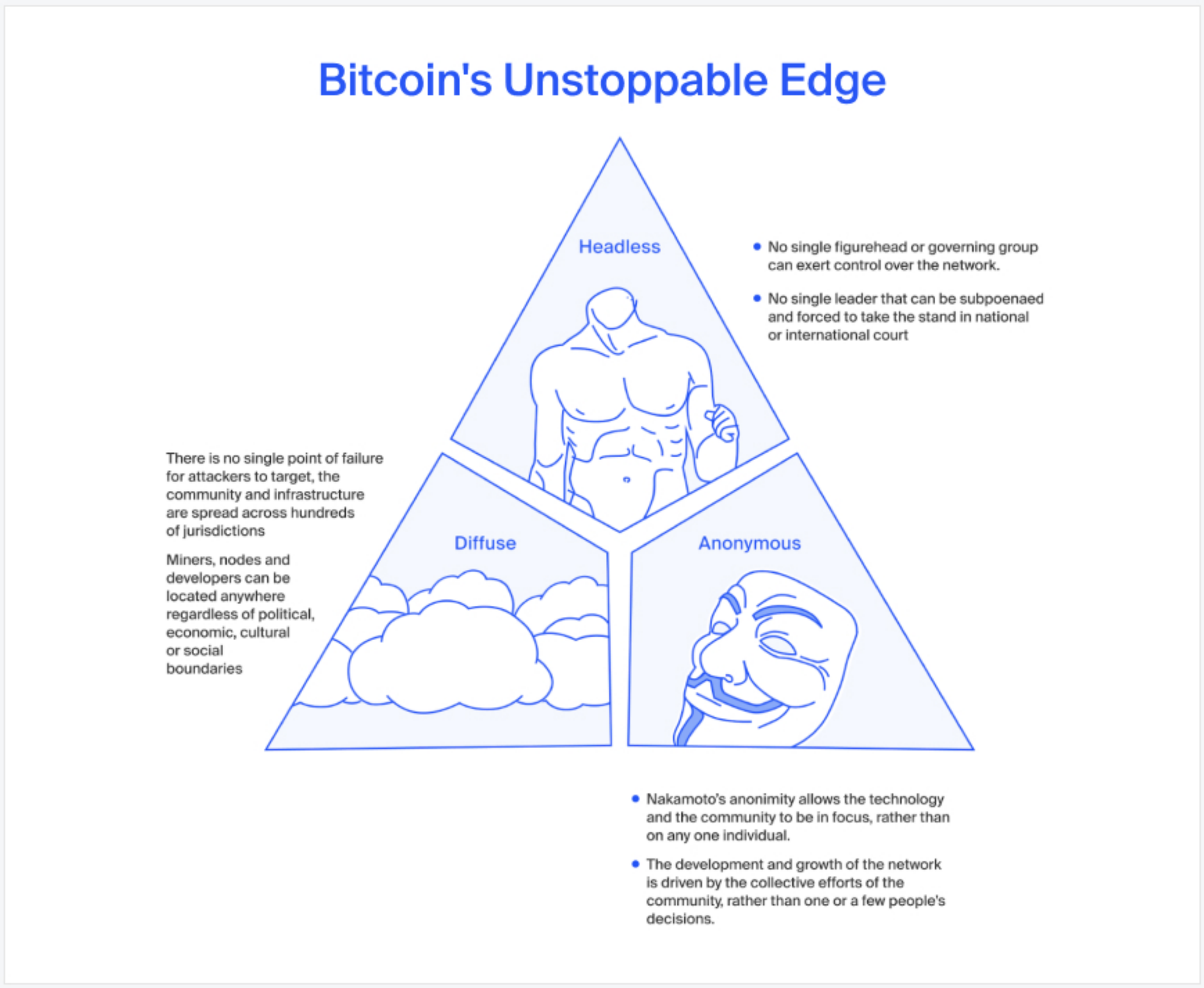
Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Bitcoin was first presented in a whitepaper published by Nakamoto in 2008.[22] The whitepaper describes Bitcoin's decentralized nature, **the proof-of-work** (**PoW**) **consensus mechanism**, and the function of a public blockchain to record transactions. The first version of the Bitcoin software was released in 2009, and the first block (the 'genesis block' or 'Block 0') was mined on January 3, 2009. A 'block' is a collection of transactions generated by the process of mining. Mining is the process of adding new blocks and new bitcoins to the Bitcoin blockchain carried out by computers solving complex mathematical problems in exchange for bitcoin rewards.

The genesis block that initiated the Bitcoin blockchain included a message that distills the ethos and values that the technological innovation represents: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks'"* [23]

The message is a sign of the frustration and disillusionment and can be seen as a critique of the centralized, government-controlled financial system, and a call for a new, decentralized monetary system that is free from government interference and is based on the core cypherpunk values. More broadly, it is a statement of the values that the Bitcoin community holds, and it represents a commitment to creating a more equitable and transparent financial system for all.



Bitcoin is a headless collective of anonymous individuals spread all across the globe, which has made it an incredibly resilient project to date.

The collective responsibility for building and maintaining the Bitcoin network is only part of the reason for its success. The technology built to distribute the system is where the force multiplying innovation lies.

Distributed Systems: Autonomous Computation At Scale

The Bitcoin blockchain is more than just a database with a series of linear entries keeping track of user balances – it is a protocol, a distributed system, and an asset.

A more familiar protocol is the 'rules of the road' that govern drivers and pedestrians in transportation systems around the world. As a driver, how do you get from one place to another in a vehicle? As a pedestrian, how do you safely walk from point A to point B? How fast should vehicles drive? What is the correct path to take? What surfaces should be used for travel? And how are other vehicles and pedestrians dealt with in the process of trying to get from one place to another?

> "As it turns out, the problem of launching a decentralized currency was so great that no single public company or individual would be able to do it."

The answers to these simple questions form a protocol that standardizes how actors – drivers and pedestrians – interact in transportation systems across the world (with some regional tweaks).

For example: drivers must stay on a specific path called a road which offers multiple routes to any destination. The rules also provide instructions on how to interact with other actors. An actor must stay on their designated path – sidewalk or lane, obey street signage, and observe traffic lights. When encountering others, actors must also abide by parameters that determine right-of-way, and who should move first. **Most importantly, there are supporting systems – like licensing offices, traffic enforcement and courts – that uphold these rules, and punish those who break protocol.**

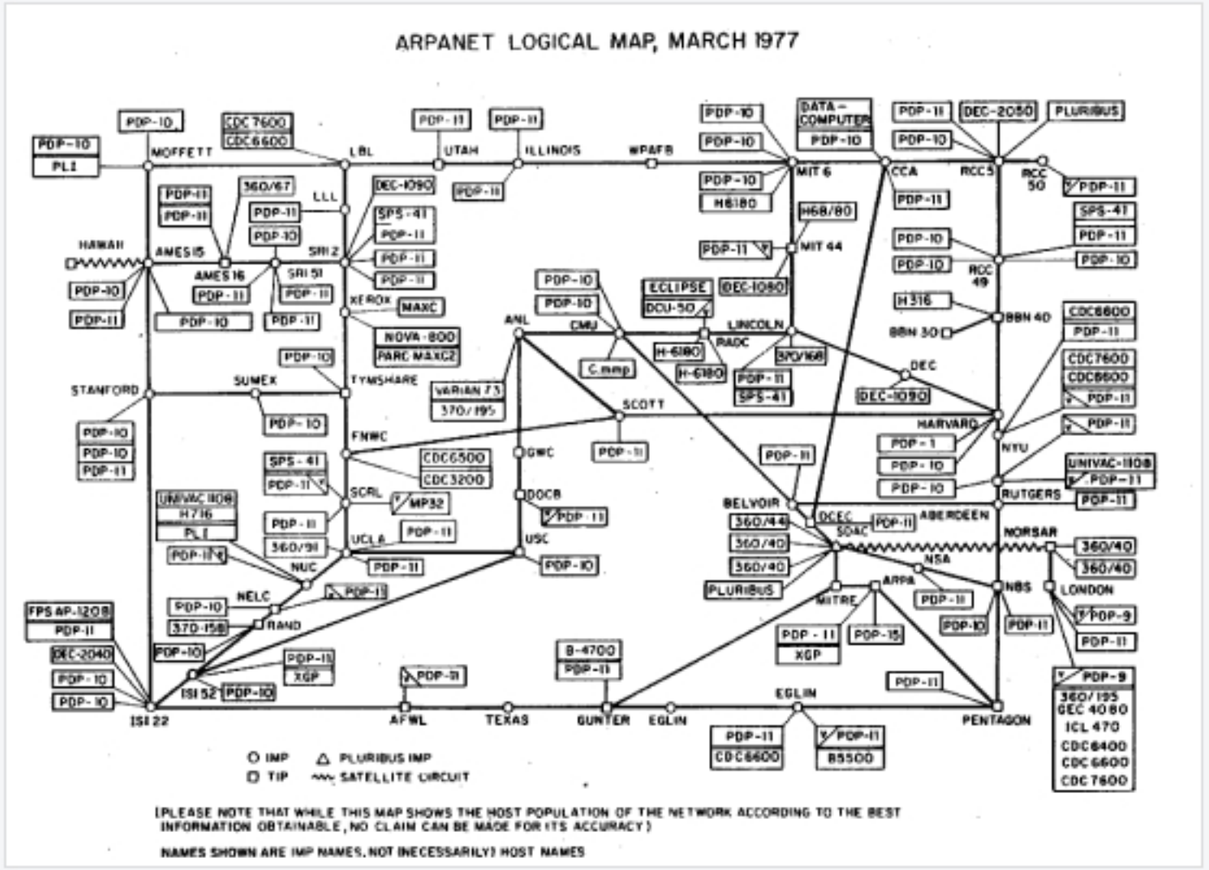
A distributed computing system is a network of individual computer 'nodes' that operate as one to achieve a common goal. In a distributed system, each node's software and hardware share resources with each other such as memory, storage, and computation, and coordinate processing in real time. Nodes can be located in a single room or in different parts of the world.

> "The ultimate challenge facing Bitcoin is: will it survive as the de facto globally distributed, decentralized monetary network?"

The internet is a prime illustration of a distributed system of servers and computers connected as one. It utilizes protocols to communicate information such as the Internet Protocol Suite (TCP/IP). Protocols serve as rulesets that nodes use to exchange data in a consistent and reliable way between diverse devices and systems.

The earliest version of the internet was launched in the late 1960s as a way for university labs across the United States to instantly exchange information.[24] As the network expanded from universities, to households and businesses, service providers emerged as specialized hosts for the nodes that facilitated a world wide web. As public demand for internet access exploded, internet service providers (ISPs) emerged as centralized private companies offering internet access to individuals and businesses through dial-up and broadband connections.

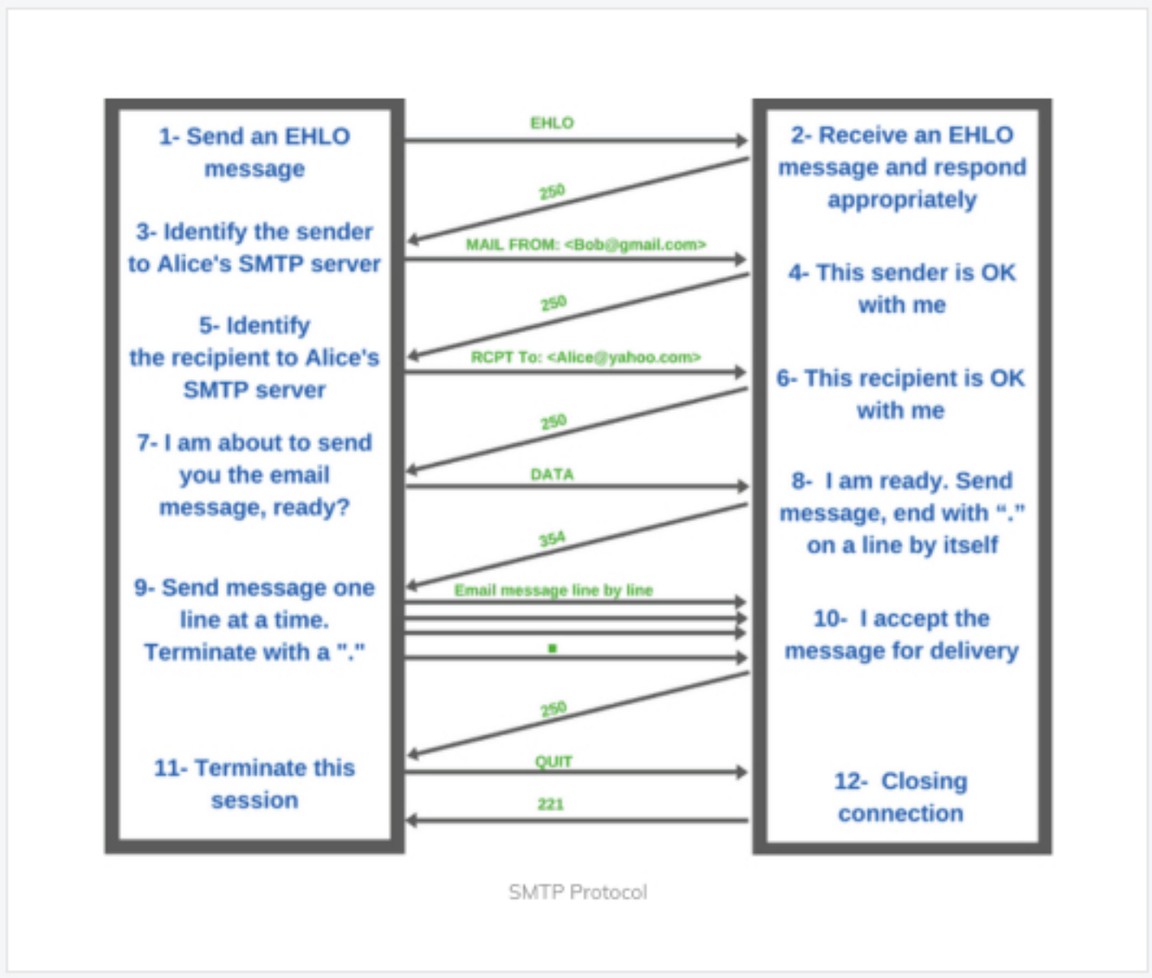
ISPs choose to sacrifice network resiliency to accelerate mass adoption and improve usability since they couldn't meet the booming public demand, **but the centralization of server owners by private companies came with a cost.**[25] What used to be a network of decentralized individual nodes freely sharing information, open to all, became a group of intermediaries with control over content, distribution, and system access.



A MAP OF EARLY INTERNET SERVERS – A HIGHLY COMPLEX EARLY DISTRIBUTED SYSTEM

Email is another example of a protocol that began as a decentralized distributed system, but became centralized over time. Email's simple mail transfer protocol (SMTP) was developed to define how email servers should send and receive email messages.

Unfortunately, due to heavy network spam, in the late 1980s the distributed decentralized network of email servers began to converge into a few giant email providers, like Hotmail, Yahoo! Mail, and eventually Gmail, that were better equipped to defend against spam.[26] Adam Back attempted to solve this problem with PoW for email but the SMTP network incentives were not optimal and his solution ultimately failed. Decentralized systems have always tended towards centralization or failed to reach global relevance due to some centralizing force.
This left truly decentralized systems confined to small niche communities, all save one: Bitcoin.



EMAIL'S HIGHLY COMPLEX 'SIMPLE MAIL TRANSFER PROTOCOL' (SMTP)

Like TCP/IP and SMTP, Bitcoin is also a protocol – a set of rules or guidelines that dictate how different entities should interact with each other. But instead of exchanging data or messages, the Bitcoin protocol exists for one purpose: to exchange value. Specifically, bitcoin tokens or BTC, money created within the decentralized system to incentivize PoW, to be exchanged in a decentralized fashion by the protocol.

Nodes are actors in the Bitcoin network that actively participate in a protocol to ensure the ongoing operation and security of the distributed system via the PoW **consensus mechanism**. In the Bitcoin protocol, the 'rules of the road' are parameters such as: the maximum size of a block is 2MB, the **SHA256** cryptographic function secures the blockchain, and the maximum supply of bitcoins is 21 million.

The genesis block that initiated the Bitcoin blockchain included a message that distills the ethos and values that the technological innovation represents: ***"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"***.[23]

Bitcoin managed to escape the centralization spiral of distributed protocols through a series of technological innovations and game theory design principles making trustless cooperative collective action possible.

While previous distributed protocols like the internet and SMTP achieved global scalability, their prioritization of convenience and cost-effectiveness over decentralization resulted in their takeover by centralized intermediaries. After more than a decade, Bitcoin remains decentralized.

Closing Thoughts: Build From First Principles

A group of renegade but principled computer scientists, mathematicians, and political libertarians spent years fighting for a freer, fairer and more equitable world.

The cypherpunks challenged institutions gatekeeping knowledge with mathematics and cryptography to uphold their principles of trustless security and self-sovereignty. Then they prevented government overreach from stifling innovation by fighting in defence of censorship resistance and permissionless action in court. And ultimately, though the cypherpunk community disbanded, a loose collective of private individuals unified behind the goal of sharing their ideas with the world, and ensured the principles of decentralization and privacy remain alive and relevant to this day.

The quest to create new solutions underpinned by cypherpunk values to benefit humankind led to the development of bitcoin, the world's first decentralized money. Bitcoin's major innovation is threefold: a decentralized network of nodes, the rules to permissionlessly transact value, and the world's first decentralized money. The Bitcoin Network, the Bitcoin Protocol, and bitcoin (BTC) started what has become the Web 3 movement.

The legacy of the cypherpunk movement continues to inspire builders today, particularly those who feel frustrated or helpless in parts of the world where power, money or data has become overly centralized. Web 3 is an attempt to use blockchain technology to further the values of decentralization, trustless security, privacy, permissionlessness, censorship resistance and self-soverignty. Any enterprise that builds from that foundation will be ahead of the competition.

The next installments of the Blockchain Fundamentals report series will expand on why understanding these values is critical for success in Web 3. Each report will focus on a key component of foundational decentralized infrastructure. Part II will identify the engineering and game theory design solutions Bitcoin used to ensure a permanent decentralized money system. Part III will explore how smart contracts are transforming legacy systems with secure, efficient and decentralized distributed systems.

References

1. "Before Bitcoin Pt.1 — 70s “Public Key Saga” | by Peter 'pet3rpan'." https://pet3rpan.medium.com/history-of-things-before-bitcoin-cryptocurrency-part-one-e199f02ca380. Accessed 2 Jan. 2023.

2. "Before Bitcoin Pt.2 — 80s “The Origins of Decentralization”." https://pet3rpan.medium.com/history-of-things-before-bitcoin-cryptocurrency-part-two-94c4576005. Accessed 2 Jan. 2023.

3. "Before Bitcoin Pt.3 — 90s “Cryptowars” | by Peter 'pet3rpan'." 13 Apr. 2018, https://pet3rpan.medium.com/before-bitcoin-pt-3-90s-cryptowars-e857915fab82. Accessed 2 Jan. 2023.

4. Kerckhoffs, Auguste. “La cryptographie militaire.” Journal des sciences militaires, vol. IX, no. Jan, 1883, pp. 5-38, https://www.petitcolas.net/kerckhoffs/.

5. Singh, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor, 2000.

6. "Jun 28, 1919 CE: Treaty of Versailles | National Geographic Society." 19 May. 2022, https://www.nationalgeographic.org/thisday/jun28/treaty-versailles-ends-wwi/. Accessed 3 Feb. 2023.

7. "73d CONGRESS. SESS. I. CHS. 87-89. JUNE 15, 16, 1933. made in ...." https://govtrackus.s3.amazonaws.com/legislink/pdf/stat/48/STATUTE-48-Pg162a.pdf. Accessed 3 Feb. 2023.

8. Diffie, Whitfield, and Martin E. Hellman. "New Directions in Cryptography." IEEE Transactions on Information Theory, vol. 22, no. 6, 1976, pp. 644-654.

9. Merkle, Ralph. "Secure Communications over Insecure Channels." PhD diss., Stanford University, 1979.

10. "SJ Games vs. the Secret Service." http://www.sjgames.com/SS/. Accessed 3 Feb. 2023.

11. "Arms Export Control Act (1976) | Wex - Law.Cornell.Edu." https://www.law.cornell.edu/wex/arms_export_control_act_(1976). Accessed 1 Feb. 2023.

12. Bernstein v. United States Department of Justice. 922 F. Supp. 1426 (N.D. Cal. 1996).

13. Philip R. Karn, Jr., Appellant, v. U.S. Department of State and Thomas E. Mcnamara, Appellees. 107 F.3d 923 (D.C. Cir. 1997).

14. "Junger v. Daley, 8 F. Supp. 2d 708 | Casetext Search + Citator." https://casetext.com/case/junger-v-daley-2. Accessed 30 Jan. 2023.

15. "Junger v. Daley, 209 F.3d 481 | Casetext Search + Citator." https://casetext.com/case/junger-v-daley. Accessed 30 Jan. 2023.

16. "The Death of Decentralized Email - Cypherpunk Cogitations." 4 Nov. 2022, https://blog.lopp.net/death-of-decentralized-email/. Accessed 3 Feb. 2023.

17. Chaum, David. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms." Communications of the ACM, vol. 24, no. 2, 1981, pp. 84-88.

18. "Welcome to Tor Metrics." https://metrics.torproject.org/. Accessed 30 Jan. 2023.

19. "Digital Around the World — DataReportal – Global Digital Insights." https://datareportal.com/global-digital-overview. Accessed 30 Jan. 2023.

20. "Electronic Banking - cpunks.org." https://lists.cpunks.org/pipermail/cypherpunks-legacy/1992-November/000876.html. Accessed 10 Feb. 2023.

21. Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." Journal of Economic Perspectives, 29 (2): 213-38.

22. "A Peer-to-Peer Electronic Cash System - Bitcoin.org." https://bitcoin.org/bitcoin.pdf. Accessed 22 Dec. 2022.

23. "Genesis block - Bitcoin Wiki." 14 Mar. 2021, https://en.bitcoin.it/wiki/Genesis_block. Accessed 22 Dec. 2022.

24. "ARPANET, Internet | LivingInternet." https://www.livinginternet.com/i/ii_arpanet.htm. Accessed 4 Jan. 2023.

25. "The Death of Decentralized Email - Cypherpunk Cogitations." 4 Nov. 2022, https://blog.lopp.net/death-of-decentralized-email/. Accessed 22 Dec. 2022.

26. Dumbill, Edd. "Email Evolution: The Rise of Centralized Email." O'Reilly, O'Reilly Media, Inc., 12 Jan. 2009, oreilly.com/radar/email-evolution-the-rise-of-centralized-email/

About Waves Labs: Waves Labs is the growth engine for the Waves Blockchain Ecosystem. With the primary objective of mass adoption of Waves technologies, Waves Labs seeks to grow awareness, support projects building on Waves with funding and mentorship, and integrate Waves with leading blockchain protocols.

General Disclosure: This material is prepared by Waves Labs and is not intended to be relied upon as a forecast or investment advice, and is not a recommendation, offer or solicitation to buy or sell any securities, cryptocurrencies or to adopt any investment strategy. The use of terminology and the views expressed are intended to promote understanding and the responsible development of the sector and should not be interpreted as definitive legal views or those of Waves Labs. The opinions expressed are as of the date shown above and are the opinions of the writer, they may change as subsequent conditions vary. The information and opinions contained in this material are derived from proprietary and non-proprietary sources deemed by Waves Labs to be reliable, are not necessarily all-inclusive and are not guaranteed as to accuracy.

As such, no warranty of accuracy or reliability is given and no responsibility arising in any other way for errors and omissions (including responsibility to any person by reason of negligence) is accepted by Waves Labs. This material may contain 'forward looking' information that is not purely historical in nature. Such information may include, among other things, projections and forecasts. There is no guarantee that any forecasts made will come to pass. Reliance upon information in this material is at the sole discretion of the reader. This material is intended for information purposes only and does not constitute investment advice or an offer or solicitation to purchase or sell in any securities, cryptocurrencies or any investment strategy nor shall any securities or cryptocurrency be offered or sold to any person in any jurisdiction in which an offer, solicitation, purchase or sale would be unlawful under the laws of such jurisdiction. Investment involves risks.