How a Scalable Blockchain Will Win

Why the Crypto Consensus is Wrong

Jackson Laskey
Dave Mullen-Muhr

UNBOUNDED CAPITAL

How a Scalable Blockchain Will Win

Why the Crypto Consensus is Wrong

Jackson Laskey and Dave Mullen-Muhr

Originally published in 2020.
Updated 2022.

REVIEWS

"When I first started the e-book, I thought, oh boy, here we go, this is going to trigger so many people. I felt myself being defensive too when I read the chapter about Scale being more important than Trustlessness and Censorship Resistance. But since I know that Unbounded Capital puts a lot of thought into their writings, I continued reading. And as I did, I slowly got more and more onboard with their vision for Bitcoin. I had already been exposed to it, but the way it is articulated in this book is much more compelling, well structured and filled with solid examples. A vision of Bitcoin I would actually want to see happen."

—Aymard Dudok De Wit of **Ausum Ventures**

"There are a lot of exaggerated and inaccurate claims in the cryptocurrency industry. A lot of this misinformation revolves around a standard narrative about what cryptocurrency is and why it has value. Jackson Laskey and Dave Mullen-Muhr demonstrate in this cogent article that this misinformation fundamentally rests on a set of interlinked faulty assumptions. They take down every single one. In its place they build a vision of a scaled version of Bitcoin, where blocks are very large and the size is not capped by the protocol, which is far more realistic and compelling than anything pitched in the standard narrative. This alternative vision for Bitcoin is actually the original idea. This article is a must-read for any open-minded person involved in the cryptocurrency industry to better understand the problem Bitcoin solved, how it works, and why the original vision with uncapped block sizes is the only version of Bitcoin likely to work over the long term."

—Ryan X Charles, Founder and CEO of **Money Button**

"The book presents a well thought out investment thesis for the compelling road ahead for Bitcoin SV. It presents how Bitcoin as initially designed is an elegant, balanced, & scalable protocol. The book is essentially a shout out - 'The King has no clothes!'"

—Daniel Lipshitz of **Gap600**

REVIEWS

"The clearest, most complete case for Bitcoin I have come across. This book goes beyond surface level assumptions, reveals revolutionary new use-cases, and provides an excellent understanding of the economic incentives that make Bitcoin more than 'digital gold'. Both pro and anti Bitcoin mainstream narratives miss the mark, and this book explains why."

—Isaac Morehouse, CEO of **Crash**

"I've been in the cryptocurrency space for over seven years and have learned the space is rife with cargo cults, perverse incentives, cults of personality, and incoherent investment theses with no basis in empirical reality. *Why Multicoin Capital and the Crypto Consensus are Wrong,* in contrast, is boldly contrarian, logically sound, thoroughly researched, and thoughtfully written. It's an Overton Window shifting piece that moves away from focusing on Craig Wright's mannerisms to shine light on the first principles that underpin the Bitcoin SV investment thesis.

"This is a required read for any serious investor willing to do the critical thinking and due diligence required to get exposure to the Bitcoin companies rebuilding the foundation of finance and the internet."

—Kevin Pham: Blockchain Investor, Advisor, and Communicator

DISCLAIMERS

This ebook does not constitute an offer to sell, a solicitation of an offer to buy, or a recommendation of any security or any other product or service by Ezra New Economy Fund LP, Unbounded Capital SPV I LLC, Ezra Capital LLC or any other third party regardless of whether such security, product or service is referenced in this ebook. Furthermore, nothing in this ebook is intended to provide tax, legal, or investment advice and nothing in this herein should be construed as a recommendation to buy, sell, or hold any investment or security or to engage in any investment strategy or transaction. The information contained in this email has been compiled with considerable care to ensure its accuracy at the date of publication. However, no representation or warranty, express or implied, is made to its accuracy or completeness. You are solely responsible for determining whether any investment, investment strategy, security or related transaction is appropriate for you based on your personal investment objectives, financial circumstances and risk tolerance. You should consult your business advisor, attorney, or tax and accounting advisor regarding your specific business, legal or tax situation.

This commentary in this book reflects the personal opinions, viewpoints and analyses of Jackson Laskey and Dave Mullen-Muhr, and should not be regarded as a description of advisory services provided by Ezra New Economy Fund LP, Unbounded Capital SPV I LLC, Ezra Capital LLC or performance returns of any Ezra New Economy Fund LP or Unbounded Capital SPV I LLC client. The views reflected in the commentary are subject to change at any time without notice. Nothing in this book constitutes investment advice, performance data or any recommendation that any particular security, portfolio of securities, transaction or investment strategy is suitable for any specific person. Ezra New Economy Fund LP and Unbounded Capital SPV I LLC manages its clients' accounts using a variety of investment techniques and strategies, which are not necessarily discussed in the commentary. All investors are advised to conduct their own independent research into individual cryptoassets before making a purchase decision. Investments in cryptoassets and securities involve the risk of total loss.

I shall not be responsible for any consequential effect, nor be liable for any direct, consequential, incidental, indirect loss or damage, howsoever caused, arising from the use of, inability to use or reliance upon any information or materials provided on this podcast, whether or not such loss or damage is caused by us. Links to third party sites are provided for your information only. The content and software of these sites have been issued by third parties. As such, we cannot be responsible for the accuracy of information contained in these sites, nor be held liable for any loss or damage arising from or related to their use. Investors should be cautious about any and all cryptoasset and investment recommendations and should consider the source of any advice on cryptoasset selection. Various factors, including personal or corporate ownership, may influence or factor into an expert's analysis or opinion. All investors are advised to conduct their own independent research into individual cryptoassets before making a purchase decision. In addition, investors are advised that past cryptoasset performance is no guarantee of future price appreciation. Do not invest money you cannot afford to lose. All investments come with a degree of risk.

DISCLOSURES

New Economy Fund LP and Unbounded Capital SPV I LLC have net short BTC exposure and long BSV exposure. Authors Jackson Laskey and Dave Mullen-Muhr have long BSV exposure.

Who is this book for?

This book is written primarily for investors actively investing in the blockchain space or who have invested in crypto/blockchain funds. However, it is written to be accessible to anyone with an interest in learning more about Bitcoin and blockchain. We invite you to consult the resources section on our website for more information and to make use of the glossary at the back of this book for definitions and links to more information.

Table of Contents

INTRODUCTION

There's an old bit of Silicon Valley wisdom that the best technology doesn't always win. With that in mind, our strategy at Unbounded Capital may not look very pragmatic. We are investing exclusively in scalable blockchains like BSV. We only hold scalable blockchain tokens and we only invest in businesses building on top of scalable blockchains. The only blockchain we think has a chance of meeting global demand for using blockchain, BSV, is one of hundreds of blockchains and thousands of cryptocurrencies. It isn't even the main version of Bitcoin by market cap or visibility. That mantle is held by BTC.

Our blockchain/crypto fund peers are taking a very different approach, diversifying across a range of cryptocurrencies and blockchains under broad investing theses. This includes funds like a16z, Pantera Capital, Bitbull Capital, Blockchain Capital, Digital Currency Group, and Multicoin Capital. Virtually none of these funds have any exposure to BSV or BSV businesses in their otherwise diversified portfolios. To most others in the blockchain space, BSV is thought to be thoroughly uninteresting, extremely unlikely to work, or even an outright scam.

So why have we opted to forgo diversification in favor of investing solely in the one thing that all our peers seem to think is not valuable? It only makes sense when one realizes that BSV is something wholly different from BTC, Ethereum, EOS, Tezos, Chainlink, and virtually all other blockchains and cryptocurrencies. It isn't in the same category. It's

not that BSV is a different technology. In fact, BSV is attempting to restore the original Bitcoin design, the technology from which all other blockchains are based. Accordingly, BSV's differentiating factor lies not in its technology but in its market philosophy: it is informed by a completely different view on the value of Bitcoin and blockchain.

If BSV exists in its own category, what specifically is different about it? It all stems from assumptions shared by the rest of the blockchain community, or what we would call the **crypto consensus**. These shared assumptions inform views on why blockchain technology is valuable, what limitations exist in the technology, and what sorts of applications should be built. Even though variations on this general worldview manifest differently in distinct blockchains, applications, and investment strategies, these shared assumptions still unify nearly all non-scalable blockchains and cryptocurrencies in their own category since they are being built to pursue goals dictated by those assumptions.

What are these assumptions, and how are those of Unbounded Capital and BSV different?

CRYPTO CONSENSUS ASSUMPTION	UNBOUNDED CAPITAL VIEW
Bitcoin **can't scale** and is inefficient	Bitcoin **can scale** and is highly efficient
Decentralization is necessary to make Bitcoin valuable because it provides Bitcoin censorship resistance, trustlessness and security.	**Decentralization**, trustlessness, and censorship resistance are **not necessary** or desirable for Bitcoin. Bitcoin is valuable because it is efficient. Bitcoin is secure because it is public.
Bitcoin exists **outside of the scope of law** and code can be a pragmatic or preferable substitute for law.	Bitcoin exists **within the scope of law**. Bitcoin is more valuable and useful when it operates within the context of law.

Within the context of these shared assumptions, what may appear to be a diversified investment strategy in many blockchains with different strengths, weaknesses, and use cases is actually a concentrated investment in these shared assumptions. That strategy is making two big bets:

1. The qualities of decentralization, trustlessness, and censorship resistance have market value such that users are willing to sacrifice efficiency to attain them.
2. The benefits that come from these types of blockchains can't be replicated and exceeded on some other type of network.

In our view, both of these are losing bets. We don't believe that decentralization, trustlessness, or censorship resistance – as they are commonly understood by the crypto consensus – have value, and we think that scalable blockchains will be able to offer all of the valuable use cases these other networks are seeking to fulfill and more on one dominant network. This ebook will thoroughly explain how and why, but first we will explain how we came to this conclusion and why we decided to write an ebook explaining it.

A TALE OF TWO FUNDS

One of our grandfathers recently sent us a Forbes exposé on the cryptocurrency fund Multicoin Capital titled **Secrets of A Successful Crypto Trader: Question Absolutely Everything**. There was irony in the act of sending an article on cryptocurrency by cutting it out of a magazine and mailing it, but also in the idea that Multicoin Capital, a fund that we see as a standard bearer for the crypto consensus, is a fund that questions absolutely everything. In our view, this mismatch in how Multicoin Capital sees themselves and how we perceive them is rooted in the crypto consensus seeing their shared assumptions as facts, rather than assumptions needing to be questioned.

Despite our current divergence, Multicoin Capital and Unbounded Capital have similar origins. The Forbes piece describes how Multicoin Capital co-founders Kyle Samani and Tushar Jain viewed cryptocurrency as a sector with enormous potential but witnessed inexperienced investors in the sector making fundamental errors. Unbounded Capital launched for the very same reasons. In fact, once operating, we began emulating Multicoin Capital as an example on several fronts. Their approach of establishing themselves through high quality content was an inspiration for our blogs, research, podcasts, and

videos. Likely due in part to our consumption of their content, our initial thesis had similarities as well. We originated with a thesis that was also multi-coin, and we inherited the same assumptions that define the crypto consensus, as do almost all newcomers to the space. We imagined a future of various blockchains operating together as modular and complementary protocols. We imagined these protocols including a variety of cryptocurrencies which would accrue value as essential, incentive-aligning tools of their networks.

OUR JOURNEY

Our divergence from this thesis, and thus from Multicoin Capital which maintains it, was largely inspired by timing. We launched during the troughs of the bear market of 2018. Conversely, Multicoin Capital launched in spring 2017, in time to capitalize off the explosive bull market that followed that summer through winter. This generated impressive early returns and seemingly confirmed and reinforced their initial investment thesis. It also attracted new investors (up to 2020's $100M+ AUM) who were aligned with that thesis. Our comparatively uncertain origins in 2018 lacked this strong positive feedback and made determining how to proceed more of an open question. We had strong feelings about what certainly wouldn't work, much of it informed by the immediate failures and course corrections following the bull market. While we maintained a general optimism that there was value in the technology, we were having a difficult time finding opportunities strong enough to invest LP money.

Our course changed suddenly when a question was posed in an honest and introspective discussion in early 2019 between Unbounded Capital's core team of Zach Resnick, Jackson Laskey, and Dave Mullen-Muhr. "What if we don't even understand Bitcoin?" At first, it seemed like an absurd question. With all the complex, new "next-gen" blockchain technologies emerging, rethinking Bitcoin, one thing we thought we had a real handle on, felt like an unproductive use of time. Fortunately, we ultimately arrived at the view that our understanding of Bitcoin was unsatisfactory. We needed to form our own views on how Bitcoin worked, what made it valuable, its limitations, and ultimately in what form and for what purposes it would be successful, if at all.

At this time, there were three significant versions of Bitcoin: market dominant Bitcoin Core (BTC), Bitcoin Cash (BCH), and Bitcoin Satoshi Vision (BSV). All three originated

from the same place, as one unified Bitcoin. However, they later split into different versions in a process called forking due to disputes in the rules and the direction of Bitcoin. BTC and BCH split in 2017. BCH and BSV existed as one chain that traded as BCH for a time, but just two months before our 2019 conversation about rethinking Bitcoin, BCH and BSV split. At that time and even up to now, BSV was known primarily by its association with Dr. Craig Wright. Dr. Wright claimed to be Satoshi Nakamoto, the creator of Bitcoin, and almost no one, it seemed, believed him. For that reason, we wrote off BSV along with virtually everyone else as something that was extremely unlikely to be successful because of its association with the man many dubbed "Faketoshi." (The purpose of this ebook is not to explore this controversy, but readers interested in the topic can refer to our previously published piece, "**Why We Think Craig Wright is Satoshi, and Why That Matters**").

Soon after we dedicated ourselves to better understanding Bitcoin, we became BCH supporters. We felt that the BCH view – that Bitcoin could scale through the original plan of allowing the rate at which new transactions were added to Bitcoin to increase over time – was correct. BTC had placed a limitation on the rate at which transactions could be added to preserve decentralization. BCH wanted to remove this limitation. BTC was pivoting to a different solution called the lightning network. We didn't think lightning would work, which made BCH's plan of removing limitations the best course of action in our minds. Accordingly, we shifted some of our BTC position to BCH.

Riding off the momentum of this first change in strategy, we decided that we were uncomfortable with the fact that we couldn't "steel man" BSV. By "steel man," we meant to make the argument for BSV that BSV supporters would make themselves in order to properly argue against it. Instead, like so many others, we were against a "straw man," an argument that doesn't properly represent the views of the opponent. To help us steel man BSV, Dave was tapped to head to the local San Francisco BSV meetup.

Dave expected to encounter a group of Craig Wright acolytes, but instead he happened upon a conversation about Bitcoin unlike anything we had heard before that point. BSV's competition wasn't BTC or BCH, it was alleged, but rather companies like Amazon Web Services (AWS) and Google Cloud. Bitcoin wasn't just digital gold or a peer-to-peer cash system, but a public database. This database had efficiencies not found elsewhere on the internet. These efficiencies were the result of the same breakthrough technology that had made Bitcoin the first successful cryptocurrency. Bitcoin would be valuable because it would be native currency for a new internet built on Bitcoin.

Naturally, we found this view of Bitcoin to be farfetched. How could a technology maxing out at around a measly seven transactions per second in the form of BTC be used to compete with giants like AWS? But we were also intrigued. The people at this meetup – entrepreneurs like Money Button's Ryan X Charles and enterprise resource planning professionals like Joshua Henslee – certainly appeared to know what they were talking about. They were holding their own in, and perhaps winning, arguments with knowledgeable BTC developers who had also come to the meeting to investigate this seemingly strange BSV philosophy. They had a knowledge that seemed deeper and more robust, and they had a vision for Bitcoin that was far more expansive and potentially lucrative. We had to learn more, and the place to do it was obvious.

As we began reading Dr. Wright's writing and watching his talks, it was clear how one could label his speech as "technobabble," a term for Dr. Wright's arguments sometimes used by crypto consensus experts. His arguments were complex, veering from one topic to another, making one statement that made perfect sense followed by another that seemed outlandish. While we found certain claims implausible at first – like his claim that Bitcoin could be mined in terabyte-sized blocks, a far step beyond the one megabyte block size limit that BTC and BCH had been quibbling about – there wasn't anything that struck us as clearly wrong. Much of what he was saying made far more sense than anything else we were hearing about Bitcoin.

Our experience from the BSV meet-up propelled us to investigate the things we didn't understand about what he was saying. Ultimately, as we continued to learn more and more about Bitcoin and the world around it, the more we began to realize that BSV wasn't just a better version of Bitcoin: it was something else entirely. In time, we formed our own views about what Bitcoin was, how it could be used in the future, and what the presence of a version of Bitcoin with these capabilities meant to the rest of the blockchain ecosystem. It was this process that led us to focus on scalable blockchains.

We have ultimately come to see many of the crypto consensus's assumptions as both incorrect and as the primary reason that there is so little usage of today's cryptocurrencies and blockchains beyond speculation. In the long run, we think those who invest in and build blockchains and applications while operating based on the crypto consensus assumptions are destined for failure.

UNBOUNDED CAPITAL TODAY

Today, we have an understanding of Bitcoin and cryptocurrency so contrarian as to be bordering on the heretical. This updated understanding informs our present investment thesis, which can be thought of as two high-level theses: one negative and one positive. The negative thesis is contrary to the "cryptocurrency" landscape at large as we anticipate virtually every cryptocurrency other than BSV or other blockchains that adopt a scalable protocol to become worthless in the long term. This is our cryptocurrency "big short." However, this doesn't mean that we are bearish on the technology fundamental to the cryptocurrency ecosystem. On the contrary, our second and positive thesis that directly informs all of our investments is on the future of implementations of scalable blockchains and Bitcoin in the form of BSV. **We expect this version of Bitcoin to be so successful that it eclipses the internet as it exists today in scale, efficiency, and value generation.**

Both of these bets are vehemently rejected by the cryptocurrency consensus. Multicoin Capital is a fund that we see as a standard-bearer of this consensus, and often leads the charge on articulating the vision of cryptocurrency we once shared but now think is fundamentally flawed. In **Secrets of A Successful Crypto Trader: Question Absolutely Everything**, Multicoin Capital founders Kyle Samani and Tushar Jain are described as "pound-the-table Bitcoin bulls". We would say the same about ourselves, but we are pounding the table for a fundamentally different view of what Bitcoin is and how it will be successful.

Despite our differences, we sincerely respect Multicoin Capital. They were a major influence to our team members as we individually began our journey into cryptocurrency and they served as a role model when we launched our fund. The following critiques of the cryptocurrency consensus, at times by way of Multicoin Capital, are intended to be revelatory, not disparaging. We hope that by thoroughly explaining our understanding of Bitcoin, we can begin a discussion about the validity of these often unexamined, inherited assumptions. Once the legitimacy of the assumptions is open to debate and thoughtfully considered from our point of view, we think that many will find merit to our theses. Our desire is for Multicoin Capital's founders and disciples to be among the readers who use this ebook to reconsider these assumptions. Thank you, Multicoin Capital, for your thought-provoking public writing over the years. We hope you find this writing as helpful as we have found yours.

THE LOGIC OF THE CRYPTO CONSENSUS

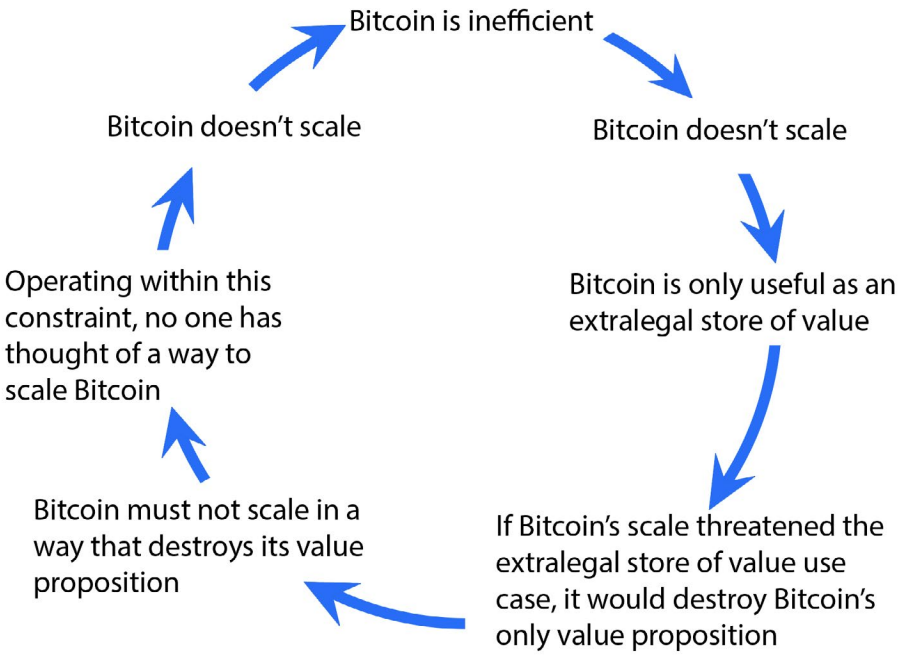
As we stated above, the foundational assumptions of the crypto consensus are as follows:

- Bitcoin can't scale/is inefficient
- Decentralization is necessary to make Bitcoin valuable because it provides Bitcoin's censorship resistance, trustlessness and security
- Bitcoin exists outside of the scope of law and code can be a pragmatic or preferable substitute for law.

Operating on these assumptions, the cryptocurrency consensus maintains a consistent internal logic. This logic appears strong so long as these assumptions are not scrutinized. Most people who discover the world of Bitcoin and cryptocurrency encounter this logic early and often. Those who buy into that worldview can quickly become immersed in this logic. Those for whom this logic does not resonate often write off blockchain entirely as a bubble likely to fail.

This internal logic is a circular chain of reasoning that interacts with several key assumptions. In some ways, the chain of reasoning is built off of these assumptions, and in other ways it informs these assumptions:

- Bitcoin is inefficient, THUS
- Bitcoin doesn't scale, THUS
- Bitcoin is only useful as an extralegal store of value, THUS
- If Bitcoin's scale threatened the extralegal store of value use case, it would destroy Bitcoin's only value proposition, THUS
- Bitcoin must not scale in a way that destroys its value proposition, THUS
- Operating within this constraint, no one has thought of a way to scale Bitcoin, THUS
- Bitcoin doesn't scale, BECAUSE



The assumption that Bitcoin doesn't scale is key, as people enter the chain of logic at different points. For some, the assumption is that Bitcoin literally does not scale. For others, the assumption is that Bitcoin must not scale. Regardless of how these conclusions are reached, the result is two-fold. The most must be made out of an unscalable Bitcoin, and non-Bitcoin alternatives are needed for any applications seeking greater scale. The implication is that these alternatives must make trade offs relative to Bitcoin or "recreate Bitcoin's wheel" with their own superior innovation in order to achieve greater scale.

TRUSTLESSNESS AND CENSORSHIP RESISTANCE

The crypto consensus view is that Bitcoin is inefficient and that Bitcoin's innovation and value are rooted in two important qualities: trustlessness and censorship resistance. Understanding these terms is essential. To begin, we want to provide a "steel man" and allow the crypto consensus to describe the terms in their own words. Binance is the largest cryptocurrency exchange and one of Multicoin Capital and the crypto consensus' primary investments. In their own learning resource, Binance Academy, they give the following definitions of what it means to be trustless and censorship resistant.

Trustless

"A trustless system means that the participants involved do not need to know or trust each other or a third party for the system to function. In a trustless environment, there is no single entity that has authority over the system, and consensus is achieved without participants having to know or trust anything but the system itself.

"The property of trustlessness in a peer-to-peer (P2P) network was introduced by Bitcoin, as it allowed all transactional data to be verified and immutably stored on a public blockchain...

"Centralized systems aren't trustless since participants delegate power to a central point in the system and authorize it to make and enforce decisions.

"In a centralized system, as long as the trusted third party can be trusted, the system will function as intended. However, serious issues can emerge if the trusted entity isn't to be trusted. Centralized systems are subject to system failures, attacks, or hacks. Data can also be altered or manipulated by the central authority without any public authorization."

Censorship Resistance

"Censorship-resistance may refer to a specific property of a cryptocurrency network. This property implies that any party wishing to transact on the network can do so as long as they follow the rules of the network protocol.

"It might also refer to the property of a network that prevents any party from altering transactions on it. When a transaction is added to the blockchain, it's propagated across thousands of nodes and added to the distributed ledger. Once the transaction has been added, it's virtually impossible to remove or alter it, making it (and the network) immutable.

"Censorship-resistance is considered to be one of the main value propositions of Bitcoin. The idea is that no nation-state, corporation, or third party has the power to control who can transact or store their wealth on the network. Censorship-resistance ensures that the laws that govern the network are set in advance and can't be retroactively altered to fit a specific agenda.

"While traditional financial institutions are in the hands of intermediaries, the Bitcoin network isn't owned by any single entity. As such, it's virtually impossible to censor transactions on it – in contrast, this isn't the case when it comes to traditional finance. For example, if a person is deemed an enemy of an authoritarian state, the ruling government might freeze their account and prevent them from moving their funds. While Bitcoin is mostly used as an instrument for speculation, this use case is probably the most fundamental reason why it's a substantial innovation.

> *"It's worth noting that censoring transactions on the Bitcoin network isn't completely impossible, but rather extremely resource-intensive. The security model of Bitcoin heavily relies on majority rule. This means that a single entity could, in theory, garner enough hash rate to gain control of the network in a scenario called a 51% attack. The chances of this happening are rather slim, but it's possible nonetheless."*

It is widely believed that these qualities are not only essential to Bitcoin but to the value of all cryptocurrencies and blockchains. These are considered to be the fruits of Satoshi's innovation. Ultimately, the crypto consensus is projecting a future where these trustless, censorship resistant platforms play an increasingly important role within the economy. Look no further than the first sentence of Multicoin Capital's **Mega Crypto Theses** where they claim that, "Open, distributed ledgers and permissionless, censorship-resistant, trust-minimized computation are going to reshape massive sectors of the global economy."

These qualities are thought to stem from decentralization, which makes preserving decentralization and preventing "centralization" paramount. It is thought that centralization destroys the value of these networks because it removes trustlessness and censorship resistance, and that centralization poses extreme security risks through attack vectors like a 51% attack. For this reason, severe limits to scale have been imposed on BTC and most other blockchain projects in order to minimize the risk of centralization.

SCALE > TRUSTLESSNESS AND CENSORSHIP RESISTANCE

At Unbounded Capital, we think Bitcoin's value is not derived from trustlessness or censorship resistance. Rather, Bitcoin's value comes from its efficiency, and that efficiency is maximized through scale. We have come to these alternate conclusions because we have fundamentally different views on the value of trustlessness and censorship resistance and on why Bitcoin works. We don't believe that Bitcoin or other blockchains are actually trustless. Instead, we contend they shift trust from traditional counterparties onto autonomous code – a counterparty that has not always proven to be trustworthy. We see the censorship resistance described by the crypto consensus more accurately described as extralegality, or existence outside of law. We believe that access to law is a huge net benefit to Bitcoin and that this security layer should not be so casually abandoned.

Decentralization is thought to be a necessary part of Bitcoin and other blockchains because it is necessary for security and for achieving some level of trustlessness and censorship resistance. We believe that Bitcoin's security comes from it being public, not from being decentralized. This, combined with our pessimism on the value of trustlessness and censorship resistance, leads us to the conclusion that no limitations should be placed on Bitcoin for the goal of preserving decentralization.

Throughout its history, severe limitations have been imposed on Bitcoin by the developers who maintain it for the goal of preserving decentralization. The key limitation is BTC's arbitrary 1 mb block size cap, which limits the total amount of data that the network can process to this small amount of 1 mb every ten minutes. These limitations persist in BTC but have been removed from BSV. These limitations severely stunted the development and adoption of Bitcoin. Further, they have created space for a myth to emerge that Bitcoin simply cannot scale. However, with BSV now able to scale to meet an ever-increasing demand, the theory that Bitcoin cannot scale has begun to be put to the test. Thus far, the theory hasn't held up as BSV continues to exceed what was thought to be possible.

In the coming pages, we hope to make abundantly clear why we disagree with the assumptions of the crypto consensus. We will also expand on our views of why BSV works, what Bitcoin can be, and why BSV's scale is unbounded. We will contrast the crypto consensus pursuit of limited goals such as Web3 and DeFi (decentralize finance) with how we envision the vast potential of BSV applications that leverage a scaled version of Bitcoin. Ultimately, we want to be clear that the crypto consensus may be diversified, but that diversification is hitched to bet on a single horse. For anyone invested in consensus funds, the question becomes: is this a horse you think can win?

PART ONE
Two Perspectives on Blockchain's Present and Future

CHAPTER ONE

The Goal of Bitcoin and Blockchain

CRYPTO CONSENSUS VIEW

Bitcoin is extremely inefficient but enables trustless, censorship resistant, and state-free money. Bitcoin's blockchain technology creates an opportunity to create other trustless, censorship resistant applications.

UNBOUNDED CAPITAL VIEW

Bitcoin is extremely efficient and will grow to become the foundation of an improved internet.

To understand how Unbounded Capital differs from the crypto consensus, it is necessary to understand how differently we see Bitcoin, the foundational technology for modern blockchains and cryptocurrencies. Today, we are focused on BSV and scalable blockchains while the crypto consensus is focused on BTC and non-scalable blockchains. However, these are more alike than different as they share the same direct origin: original Bitcoin. The differences in our views and that of the crypto consensus are more a manifestation of divergent understanding of what is possible and what is desirable for Bitcoin rather than a reflection of strictly technical incompatibilities, although these technical differences do exist and are growing. We think that Bitcoin – in the form of BSV or another blockchain similar to BSV in scalability – will be the dominant blockchain network that ultimately grows to subsume the internet. While the crypto consensus thinks Bitcoin is extremely limited,

they still view it as a success story, but as an extralegal store of value dubbed "digital gold."

This difference in how we perceive Bitcoin informs how we differ from the crypto consensus in the goals and structure of a blockchain future. In our view, Bitcoin as BSV offers efficiencies that will lead to the internet broadly shifting onto BSV or an alternative scalable blockchain yet to emerge. Those efficiencies are rooted in the ability to centralize data. Data becomes more valuable as it centralizes, and Bitcoin's innovation, which is best expressed on BSV, is rooted in becoming a database where that centralization can occur. As data is incentivized to centralize in one place – BSV's blockchain – we expect that BSV or a competing scalable blockchain will be the dominant, if not sole, winner from the blockchain space.

The crypto consensus views the ability to generate trustlessness and censorship resistance as the main value of Bitcoin, but this comes at the expense of efficiency. Because Bitcoin as BTC is too inefficient for many use cases, other blockchains have to be developed which make tradeoffs to improve efficiency and can enable other more resource-intensive use cases. Working together as a series of distinct blockchains, the consensus view aims to form a network of decentralized protocols to supplement the internet. Because it isn't clear which sets of tradeoffs or improvements for each individual blockchain will ultimately be necessary or successful, the diversified approach may seem prudent.

THE CRYPTO CONSENSUS GOALS

When it comes to Bitcoin, the crypto consensus is typically only interested in BTC, and it is BTC which informs their understanding of Bitcoin generally. The crypto consensus understands Bitcoin to be an extremely inefficient – but extremely valuable – system. This is because Bitcoin's value is not the result of its efficiency, but instead the result of its revolutionary ability to send scarce digital value anywhere in the world without needing to rely on any third party financial institutions. The culmination of these properties makes Bitcoin a "digital gold" which can serve the same functions of gold's historic use as a store of value, in addition to the added benefits that come from being digital. **The Bitcoin (BTC) wiki describes Bitcoin as**:

- ***Permissionless*** *and* ***borderless****. The software can be installed by anybody worldwide.*
- ***Do not require any ID*** *to use. Making it suitable for the unbanked, the*

privacy-conscious, computers or people in areas with underdeveloped financial infrastructure.

- *Are **censorship-resistant**. Nobody is able to block or freeze a transaction of any amount.*
- ***Irreversible** once settled, like cash. (but consumer protection is still possible.)*
- ***Fast**. Transactions are broadcasted in seconds and can become irreversible within an hour.*
- *Online and available **24 hours a day, 365 days per year**.*

The consensus claims that these additional properties of Bitcoin make it an exceptional store of value because (**also from the Bitcoin wiki**) stored Bitcoins:

- *Cannot be printed or debased. **Only 21 million Bitcoins will ever exist**.*
- *Have **no storage costs**. They take up no physical space regardless of amount.*
- *Are **easy to protect and hide**. Can be stored encrypted on a hard disk or paper backup.*
- *Are in your **direct possession** with no counterparty risk. If you keep the private key of a Bitcoin secret and the transaction has enough confirmations, then nobody can take them from you no matter for what reason, no matter how good the excuse, no matter what.*

The crypto consensus understanding of Bitcoin – as a censorship resistant digital gold that cannot be inflated or seized – is best expressed today by BTC. BTC is currently not scalable, maxing out at about 7 transactions per second. While the crypto consensus would welcome improvements in scale through initiatives like the lightning network, these aren't thought to be necessary for BTC's success. Instead, much of the development is actually going toward features which advance the ability to use the system anonymously such as coin mixers, schnorr signatures, the liquid network, and the lightning network, which would add anonymity in addition to scale. These are thought to improve censorship resistance and are characteristic of the crypto consensus' disregard for building tools which are legally compliant and thus useful for existing businesses.

This digital gold store of value use case is part of broader crypto consensus goals for blockchain technology which also include what can be described as Web3 and DeFi. Web3 is

the application of blockchain technology to create a more decentralized, trustless, and censorship resistant internet. DeFi is the same approach for financial services combined with potential efficiencies that come from creating a stack of financial protocols the way a stack of internet protocols exist today. These goals are described by Multicoin Capital in their **Mega Crypto Theses**, where they outline three broad goals for blockchain: Web3, Open Finance, and Global State-Free Money. **In a recent blog post**, a16z outlined a similar set of goals for their new $515M fund which will invest in next-generation payments, modern store of value, decentralized finance, new ways for creators to monetize, and web3. We will examine these goals throughout this book, and in much greater detail in Part III.

UNBOUNDED CAPITAL'S GOAL FOR BLOCKCHAIN AND SCALABILITY

Unbounded Capital's vision of Bitcoin is not confined to its recent history as an abstract digital money that lives on the internet. Our broader value proposition for *Bitcoin and blockchain* is rooted in efficiency, not trustlessness and censorship resistance. If our vision – the vision being pursued most closely by BSV – is realized, Bitcoin will be used seamlessly by internet users many times per day, possibly hundreds or even thousands of times. It will not be a part of the internet; it will be the internet. To understand why Bitcoin will be foundational to the internet of the future, it's important to understand the shortcomings of the internet without Bitcoin. What about the internet needs to be fixed?

REBOOTING THE INTERNET

Imagine you were tasked with building a new internet from scratch. What features presently unavailable on the internet would you include? What negative aspects of the existing internet would you avoid? These are difficult questions. A typical internet user could probably think of some complaints, but imagining what features the internet lacks is much more challenging. Against what alternative would they compare? Because of the internet's under-the-hood technical complexity, it's reasonable for users to accept its current configuration as an inevitability. As an analogy, one could imagine a pre-iPhone cellular phone user suggesting he be charged less for weekend minutes as a desired improvement to his user experience. But, could he imagine the ability to visualize how a Williams Sonoma kitchen table would look in his dining room through the use of augmented reality? For the latter idea to be born, the platform of "cell phone" first needed

to be expanded to include cameras, video screens, powerful computer chips, internet access, and other features.

So what could the internet be once the platform is expanded by a degree similar to the transition from cell phone to smartphone? Through understanding the technologically revolutionary features of Bitcoin, Unbounded Capital has been given a glimpse into new features that, once incorporated, will expand what the internet can do. Like an inspired soon-to-be mobile app developer who was just given their first explanation and hands-on demonstration of the iPhone, Unbounded Capital's understanding of Bitcoin has given us a vision for where the internet should go and, importantly, how it will get there.

THE PROGRESSION OF THE INTERNET

We can radically improve the efficiency of the internet with scalable blockchains. Despite appearing in the browser as a single source of information, the internet is a complex series of distinct communications of data stored across many disparate networks and databases; hence the name "inter-net". This decentralization of information presents many inefficiencies. When users and applications wish to access some information stored online, they need to locate the data and then route it to its destination. Services like Google have done an exceptional job of indexing the internet to make the data location process more user friendly, but because of the internet's decentralized and nonuniform network design they are aiming at a moving target. Users are familiar with the 404 error or "dead links" which occur when a piece of requested online information is not found. This occurs because a relevant piece of data was moved, deleted, or stored on servers that happen to be temporarily down at the time of a request. While a 404 error is typically nothing more than a minor inconvenience for the average internet user, it's indicative of a more meaningful problem. The inefficiency of locating and accessing data online has downstream consequences that render would-be verticals implausible.

In recent years the success of cloud storage has reduced the inefficiency and unreliability of online data. Cloud networks have done this by providing expertise and economies of scale in provisioning servers. Giant companies like Google and AWS house data in large data centers which offer redundancy and improved availability. These services have been able to significantly lower the cost of storing information online. For end users, this manifests as the ability to use online services to upload large files containing images and

videos on the internet "for free." This shift has increased the usefulness of the internet and dramatically reduced the price of its essential tools.

This transition has caused many to become sentimental for the days before our reliance on giant tech companies. What this perspective often downplays is how the benefits from economies of scale have not only improved the internet, but also made it usable for the first time for many people. What is ironic about this centralization of servers is that the data is still highly decentralized. More data moves to the cloud every year, but that data is kept fully segregated from the data of other cloud customers. This is where a scalable blockchain comes in. In the same way that centralization of server provision improved the internet, the centralization of data on a scalable blockchain will catalyze an even greater leap in the value provided by internet applications. Because blockchain is public, it accomplishes this centralization without reliance on specific massive tech companies like Facebook, Apple, Microsoft, Google, and Amazon. The internet on a scalable blockchain will be able to offer improved versions of the best aspects of today's internet, eliminate inefficiencies, and enable brand new features. With scalable blockchains, internet users can have an even better cake and eat it, too.

THE INTERNET WITH BITCOIN

The smartphone's platform-expanding features included affordable access to powerful computer chips, HD cameras, HD video screens, high speed internet connections, ubiquitous biometrics, and more. A scalable blockchain's data-centralizing capabilities will lead to internet platform-expanding features that include micropayment functionality, user-centric data ownership, digital scarcity, digital permanence, and a distributed trusted timestamping authority. All of these features are properties of the world's first successful **scalable, public, and immutable database called Bitcoin.**

A **public** database is one that is not owned and operated by any single third party like Google or AWS. A key feature of a public database is the ability for any user to read and write data to and from the database. This combination of having no central operator and having open access to reading/writing data often elicits blockchain's description as "decentralized," but the database's decentralization is better described as being public (we will explore this more deeply in future chapters).

An **immutable** database is one which ensures that, once written, data on the database is permanent. This means no more dead links, but also extends to many more significant benefits. Consider the massive, and growing, problem of hackers illegally accessing sensitive data online. These criminals are often difficult to track down because of their ability to delete essential evidence like server access logs. Server logs stored on an immutable database would go a long way towards making covering a criminal's tracks more difficult. A **scalable** database is one that theoretically has no upper bound on size and is able to grow as demand for its use increases. *The existing internet is also scalable, but what a scalable blockchain scales is far more valuable. The internet scales with disparate, ephemeral data. A scalable blockchain scales with centralized, immutable data.* This kind of blockchain solves a variety of problems that, prior to Bitcoin's invention in 2008, made achieving such a database impossible. Today, the only version of Bitcoin and the only blockchain that is trying to achieve Unbounded Capital's vision of Bitcoin is Bitcoin Satoshi Vision, which trades as BSV. Hence, in the same way that we describe a stack of computer communication protocols and databases as "the internet," from here on out we will refer to this scalable, public, and immutable database simply as "Bitcoin."

The public nature of Bitcoin's feature-rich database allows the internet to vastly exceed its current data centrality, further capitalize off economies of scale, and create unparalleled data interoperability and coordination. We believe the transition from the current internet to an internet on Bitcoin will culminate in several major shifts:

- **Bitcoin will dramatically improve upon the network centrality of our current internet by being the single public database**

With Bitcoin as the internet's database, data uploaded to the internet will become much more valuable since it can be easily accessed by any party its uploader desires. Rather than uploading data for its usefulness on one particular application, users will upload data which can be used by an unbounded number of applications. Because Bitcoin is public, over time the competition to process this data will drive prices lower, over time, than they are today. This will result in users being able to put more data online and have more services interact with it in interesting and useful ways.

> **EXAMPLE:** Instead of your preferred streaming service competing for your favorite shows (Netflix winning the exclusive rights to show *Seinfeld* at the expense of Hulu), you have access to every show you like in one online application and you pay the show's creators directly. The owners of this online content will benefit as more people are able to access it through any number of applications which host and share it.

Bitcoin will introduce native privacy to the internet

Despite Bitcoin's public nature, data written to Bitcoin can be as private as the user desires. While it's true that content uploaded to Bitcoin *can be accessed* by anyone, the information *is not automatically viewable* to the public. The improvement that Bitcoin makes over the existing internet is in allowing owners of data to grant access to any party they choose that is stored on the database every party is already using. Data stored on Bitcoin can be optionally encrypted or stored behind built-in paywalls such that users retain full privacy rights while benefiting from the opportunity for interoperability.

The ability for internet users to upload data and manage the data's access options independent of the applications they are using and the cloud services those applications likely use significantly improves user privacy online.

> **EXAMPLE:** On today's internet, sensitive private information like electronic health records (EHR) are tightly regulated. The goal of this regulation is to minimize the inherent risks to individuals' privacy that come from making the information accessible online. The introduction of regulatory red-tape has had the negative impact of restricting EHR access to parties whose access could improve patient experience and outcomes. Because the benefits of digitizing medical records are so great, many patients and healthcare companies are willing to accept regulatory restrictions on EHR's utility as well as the remaining risks. By using Bitcoin, patients and healthcare companies can virtually eliminate the privacy risks of online health records without needing as strict regulatory controls. The ability for users to own and control access to their personal information could improve the usefulness of health records without sacrificing privacy.

Bitcoin will offer unrivaled digital permanence

Data written to Bitcoin will persist regardless of the success or failure of individual companies. Data stored on Bitcoin will always exist in the location that it was added. As the churn of dominant tech companies sees competitive upstarts replace former leaders, the valuable user data stored by these businesses will persist. This level of dependability is unique to Bitcoin and cannot be rivaled by any single operator offering a private database. This is a necessary complement to the existing web which excels at creating data which can be cheaply edited or deleted, but struggles to guarantee any type of permanence.

> **EXAMPLE:** Bitcoin would make the recent trend of "digital book burning" obsolete. Benign but politically unpopular information currently able to be censored by an existing tech giant would remain accessible despite one powerful company's protest. Companies like YouTube, which censor information uploaded to their servers, would no longer be able to effectively remove the information from the internet. Instead, they would

simply choose not to display it on their website. Other websites that wished to keep this information accessible and searchable would likely fill any demand for the information by doing so.

NOTE: *With Bitcoin's properties of improved privacy and digital permanence, one can imagine that it might enable the proliferation of undesired illegal content. Since all data uploaded to Bitcoin is tied to a specific private key, uploading anything illegal becomes very risky. Bitcoin ironically enables more privacy by making it economically feasible for users to retain control over their data, but also impedes criminal activity by leaving a trail of evidence that sufficiently motivated law enforcement could track and use to identify the culprit. There are also methods to prevent specific data from being served to end users without altering the blockchain's immutability or removing the evidence trail of that data having been uploaded.*

- **Bitcoin will remove dangerous security risks associated with big data tech companies**

When data is stored on private databases, there is an implicit categorization. If a hacker breaks into Apple servers, they know that they are getting Apple data. On Bitcoin all types of information are stored on the same database and can be individually encrypted. This leads to safety in numbers. Hackers can't easily distinguish what data is associated with what applications. Breaking into a honeypot of data on a private server can be worth the cost. Trying to uncover the same information transaction by transaction on Bitcoin is not feasible and would not be cost effective even if it were.

EXAMPLE: Infamous hacks of large companies like Equifax, which had sensitive personal information of nearly 150 million people compromised, have demonstrated how single points of vulnerability on private databases pose an opportunity to malevolent actors. If a hacker identifies that a database is controlled by Equifax and contains valuable personal information, they can attempt to access it and weigh the costs of doing so against the potential benefits of the theft. For the equivalent hack to occur on Equifax built on Bitcoin, the hackers would have needed to first identify the valuable Equifax data amongst all data on Bitcoin, and then do roughly 150 million times the work to access it since each file is uniquely encrypted. This increased cost would render hacks similar to the Equifax breach economically nonviable.

- **Bitcoin will provide alternative business models to companies currently dependent on indirect and inefficient internet business models**

The predominant business model on the internet requires many companies to sell ad

space to advertisers or user data to data brokers. Businesses that would prefer to directly charge users are often unable to because the value of their microservices fall below online payment minimums. Bitcoin's data centrality makes micropayments a reality. This means businesses can charge as low as fractions of a penny per service with Bitcoin.

> **EXAMPLE:** Spotify offers its users a choice between a "free" option that requires that they listen to and view ads and a "premium" option that removes ads for a monthly subscription fee. Would users unwilling or unable to pay the subscription fee be willing to pay directly per song to opt out of ads? Would Spotify and the artists they work with prefer this model?

- **Bitcoin will unbundle services that are currently, but unnecessarily, packaged**

Bitcoin's low transaction fees and micropayment capabilities enable the selling of products that are otherwise unfeasible to sell. As a result, many services that were bundled together can now be unbundled. Because many online companies depend on the internet's ad-based and data-based business models, once they accrue a large user base they are encouraged to keep them locked into an ecosystem. This presents scenarios where users are forced to accept subpar or unnecessary service on feature A because they are interested in retaining access to feature B. Because Bitcoin is public and all information is stored on the same database, new types of coordination between distinct services become possible. Businesses leveraging Bitcoin may ultimately be forced to compete for users on each unique product or service. This makes an a-la-carte configuration of features A through Z possible.

> **EXAMPLE:** Imagine an app user (Alice) who loves Instagram's discovery algorithm but prefers TikTok's video editing functionality. On the current application landscape, Instagram and TikTok have their own private databases which accumulate Alice's information to generate the companies' value. Because these services aren't willing to communicate, Alice will have to alternate between each application and enjoy her favorite features separately. On Bitcoin, both Instagram and TikTok could interact with the same data, which Alice owns and controls. This data could include images and videos that Alice uploads, as well as her follower lists and private messages. By charging micropayments per microservice, Alice's preferred features of Instagram and TikTok can be leveraged on the same super-application and both Instagram and TikTok can generate revenue by focusing on the features they create that users value most and charging directly for them.

- **Bitcoin will enable exclusive core functionality for businesses and applications to leverage**

Features unique to Bitcoin like micropayments, data ownership, tracing, scarcity, permanence, and time stamping will be utilized by creative entrepreneurs in unexpected ways. Just as internet entrepreneurs unexpectedly used near-instant communication to invent new categories like Social Media and products like Twitter, Bitcoin's novel properties will create new categories and essential products of the future.

> **EXAMPLE:** Games leveraging Bitcoin today are creating unique tradable items that can exist outside of and between games. Imagine a sword used in League of Legends functioning in Minecraft as well. The interoperable virtual world of Ready Player One is possible once data can be made scarce, owned, and easily integrated across applications.

CASE STUDY: ONLINE MUSIC MARKETPLACES

Examining the individual features unique to the scalable blockchain-enabled internet offers a glimpse into how current internet businesses could improve, but when a business is conceived and built natively on this improved internet, entirely new experiences are possible. While it's true that the internet improved the distribution of newspapers by putting their contents online, internet-native businesses like Twitter have arguably had a bigger impact on illustrating what the internet is capable of achieving. What is an example of a scalable blockchain-native business we might expect to emerge?

The music industry, from production through consumption, has been one such industry fundamentally transformed by the internet. We expect the blockchain-enabled internet to continue this trend. The development of the first online music store in the 1990s foreshadowed the potential of the internet as a tool for easily distributing and consuming music. Eventually, the downsides of digitizing music were realized as creators and owners of music experienced the difficulty of maintaining effective ownership when songs could be easily copied and illegally shared on platforms like Napster. In 2003, Apple alleviated some of this problem by releasing iTunes, the most successful online music marketplace to date, which aimed to make legally buying content so easy that it was not worth the effort or legal risk to pirate it.

Since then, legally accessing on-demand online music without first buying it was made possible through the rise of popular streaming platforms like Spotify. Spotify and its

streaming competitors have proliferated a "third-way" for online music which gives artists an additional monetization method through inclusion in a massive online music catalog which users can access through a freemium model. The freemium business model collects revenue from ad sales (generated through the "free" option) and monthly user subscriptions (the "premium" option) and distributes it to Spotify and owners of the music that is streamed. With Bitcoin, a fourth mode of music distribution can be enabled – one that will improve the experience for both artists and music consumers as well as simplify the business model of platforms like Spotify.

THE PROBLEMS WITH STREAMING

Although streaming services like Spotify have proven to be the preferred online music option today, the model is far from perfect. Each major participant in the model has problems that a Bitcoin-native alternative can remedy.

Artists

The ability for music streamers to listen to unlimited online music for free or relatively low monthly payments has presented some downsides for artists. **The average payout per stream** to an artist on Spotify is between 0.6 and 0.84 cents ($0.006 - $0.0084). This has inspired protest from high-profile artists like Taylor Swift, who temporarily stopped licensing her music to Spotify and **credited streaming with** "(shrinking) the number of paid album sales drastically" and leading to a loss in control for artists and labels, who she predicted "will someday decide what an album's price point is."

Listeners

Taylor Swift's rift with Spotify also identified a shortcoming for users. **A Business Insider article** contemporaneous to the Swift/Spotify feud articulated this problem as "In a word: permanence." Accessing inexpensive online music is great for listeners in the moment, but what about the future? For fans of Taylor Swift's music, its removal from their Spotify libraries highlighted their position as music renters rather than music owners. The convenience of renting access to music libraries like Spotify doesn't come with the guarantee of long term access. The article's author notes the fragility of a business like Spotify going under or how "at any moment, the whim of an artist, or a licensing negotiation gone sour, or a quirk of copyright law, could quietly erase vast swathes of

treasured music collections." This lack of control over access to a music listener's favorite artists is amplified by the competitive nature of streaming platforms, which vie for exclusive rights to certain artists and albums.

Spotify

As one of the most successful recent companies in music and technology, Spotify may seem like exclusively a benefactor of the streaming model. However, the additional complexities undertaken to achieve this success have required that they deviate heavily from their core mission of connecting musicians with fans. In the process of delivering this music service, Spotify became a participant in the advertising industry and needed to innovate and maintain new backend cloud infrastructure. In an interview about their backend design and transition to a Google Cloud infrastructure, **Ramon van Alteren, Director of Engineering at Spotify, was quoted saying** "If I'm really honest, what we really want to do at Spotify is be the best music service in the world, none of that work on data centers actually contributes directly to that."

If there was a way for Spotify to provide a better service without having to maintain this infrastructure, would they prefer it?

The Business Insider article about the streaming model's lack of permanence concluded by weighing the pros and cons of the existing options: ownership and streaming,

> *"Owning music has its own problems, of course. It's expensive, and takes up significant storage space. You can lose physical hard drives storing music libraries, too. In contrast, music streaming offers powerful convenience — tens of millions of songs in your pocket, anytime and anywhere…(however), custodianship of (my music library) is not a responsibility I'm willing to grant to Spotify, or Apple, or anyone else."*

A FOURTH WAY FOR ONLINE MUSIC: NETWORK CENTRALITY, DATA OWNERSHIP, AND MICROPAYMENTS

The next iteration of online music through a uniquely Bitcoin-enabled service could provide a solution that improves on the shortcomings of streaming experienced by all three parties. Imagine an online music alternative where content could be owned, maintained, and sold by artists and record labels through platforms with the identical functionality of Spotify, where users could pay directly for access to virtually any song without needing to listen to ads, become locked into recurring subscriptions, or fear ever losing access to their music.

Because Bitcoin enables data ownership on the world's single public database, artists and labels would be able to include their music in a collection larger than Spotify's without negotiating a contract directly with any single company. Once uploaded to the Bitcoin-enabled internet, the song would be accessible by any party under the terms set by its owner, realizing Swift's vision of the ability to set her music's price point. Once uploaded, online piracy would be disincentivized because of the native timestamping of the files. Illegitimate copies of the original would be provably inauthentic since they postdate the original and would be linked to the uploading music pirate through a digital paper trail, all of which could be used by motivated record labels as evidence in court.

Platforms like Spotify would add value through services they currently excel at, like indexing and curating music, to deliver it from the artist to the listener. Rather than focusing resources on licensing music, maintaining backend infrastructure, and selling advertisements, Spotify could refocus all of its resources on providing the best music specific features and charging micropayments of a fraction of a penny per microservice. Users who are interested in inexpensive on-demand music could then pay per stream. **Estimates of Spotify user activity** suggest the average user listens to 25 hours of content per month. If we assume this streaming is entirely composed of songs that average three minutes per song, this suggests that users listen to around 500 songs per month. At that rate of consumption, the average user could afford to pay artists more than double their current average rate, at almost 2 cents per stream ($0.01998), without paying more than Spotify premium's $9.99/month subscription fee.

This would have a few major impacts. First, it would enable light users of Spotify to forgo the free version's interruptions of ads without locking into a monthly fee and overpaying for their consumption. It would also incentivize artists to create more content as they are directly rewarded by its consumption. Without knowing the ultimate market price of

a stream in this type of environment, it's also possible that the per stream price would be such that particularly heavy current users of Spotify premium would be able to listen to their current quantity of music while still paying less than their monthly fee. In this paradigm, concerns expressed by "music renters" over their libraries' permanence would be all but eliminated as the disappearance of an artist's music from the internet, while possible, would be highly disincentivized. Once uploaded, an artist's content requires no additional payment or negotiation to remain accessible and its purchase through pay-per-stream services would be all upside for the artist. Access to music through Bitcoin would marry the data permanence benefits of music storage desired by listeners preferring ownership with the convenience of centralizing the world's music collection into a single and easily searchable repository.

Additional benefits for artists and record labels would include the cost reduction and removal of time delays that result from existing digital rights management and payment options. Artists who might currently be compensated by checks or direct deposits for their share of the content's revenue on a per month basis would be able to get paid instantly as music is streamed. Further, despite the low price point per stream, a payment as low as 2 cents could be automatically divided up and sent to each individual party who owns a right. Taylor Swift imagined a future where artists and record labels could simply control the price of their music. For artists like Swift, features like real time fractional payment would likely increase the appeal of such a system.

Another possible arrangement on Bitcoin would be an affiliate model of music distribution. Once Spotify no longer needs to provide the service of maintaining the complicated backend infrastructure of their platform, they are effectively music sellers who connect musicians with their fans. It's likely that artists would be interested in paying Spotify and others to provide this service. Artists like Swift could pay Spotify on a per stream basis for increasing the reach of their music. If Spotify remains particularly good at curating bespoke playlists for its users, artists would be incentivized to seek inclusion on those playlists. Because the data would be easily accessible on Bitcoin to any entrepreneur interested in competing with Spotify, the barriers to entry to getting into that industry would be dramatically reduced. By opening this arrangement up to other music curators providing this service, artists could reach more music listeners through a variety of competing recommendation platforms and user interfaces. **BlareSV** is a Bitcoin-native Spotify competitor building on BSV. In the future, companies such as BlareSV could potentially port over to a yet-to-emerge scalable blockchain.

CHAPTER TWO
The Current State of the Industry

CRYPTO CONSENSUS VIEW	UNBOUNDED CAPITAL VIEW
Crypto is early. Scale and mass adoption are right around the corner.	Crypto's lack of usage demonstrates a lack of product market fit and inherent technological problems.

The first thirteen years of Bitcoin and blockchain (up to the point of this book's latest edit in May 2022) have been dominated by crypto consensus goals and development. The state of the industry is a reflection of what is thought to be valuable by this consensus view. The crypto consensus believes that the industry is on the right track, but that it is still early. The lack of adoption is a temporary state, one which provides a huge opportunity to investors. This view is made clear in the investments that funds continue to make in technologies promoting decentralization, trustlessness, and censorship resistance.

In our view, the current state of the industry demonstrates the failure of this thesis. Inefficient technologies offering trustlessness and censorship resistance have been widely rejected by the public. Bitcoin in the form of BTC has become crippled. We see the digital gold use case as a last resort, a fallback from grander visions that still seems plausible given the consensus views on Bitcoin's technical limitations. Ultimately, we think this vision will run its course and be eclipsed by a version of Bitcoin in BSV which no longer

limits itself by seeking decentralization and focuses instead on expanding the efficiencies of Bitcoin through scale to create a better, more efficient internet.

THE REGRESSION OF BITCOIN

The widespread belief that Bitcoin is unscalable becomes more understandable when you realize that BTC, the most popular version of Bitcoin with a market valuation of $750 billion, is unscalable by design. Despite originating with the potential described in the previous chapter, twelve years of developer tinkering has yielded a broken Bitcoin in BTC. The developers who have assumed control of the main Bitcoin code value decentralization so highly that they intentionally prevented Bitcoin from achieving scale. By imposing technical constraints on the amount of data that could be written to the Bitcoin database and removing the native programming language which enabled much of Bitcoin's functionality, the initial developers of Bitcoin transformed BTC into what they consider to be state-free money or "digital gold". **One of Multicoin Capital's three "crypto mega theses" is that global state-free money**, like BTC, will be able to capture a market they value at $100 trillion.

Destroying Bitcoin's scalability resulted in a network that is slow and expensive, even at a level of usage that is miniscule relative to the valuation of the currency. As of 2022, BTC's transaction fees hover around $1.20 but have reached as high as $50 in times of peak traffic. BTC's lack of scale has eliminated the possibility for most of Bitcoin's revolutionary features and use cases. Since BTC's only remaining value proposition is trustless, censorship resistant "digital gold," which necessitates that the network doesn't scale, BTC indeed does not scale. With scale topping out at around seven transactions per second, we don't see how mainstream adoption is feasible.

Some may respond to this critique by suggesting that Bitcoin will scale via layer-two solutions like lightning network. Thoroughly explaining Unbounded Capital's critique of the lightning network here is not the best use of this ebook. Suffice it to say that even if the lightning network is able to alleviate BTC's transaction fees, its success would not enable Unbounded Capital's vision of Bitcoin. The lightning network creates an entirely separate network that does not share the features of Bitcoin as a scalable, public, and immutable database. From the perspective of the cryptocurrency consensus, a functional lightning network would be valuable because it scales the digital gold use case, but even the most

optimistic lighting network proponent would not suggest that it could enable the Bitcoin described in the previous chapter. As mentioned earlier, the only version of Bitcoin and the only blockchain that is trying to achieve Unbounded Capital's vision of Bitcoin is Bitcoin Satoshi Vision, otherwise known as BSV.

Ultimately, the success of the digital gold use case for BTC depends on what alternatives can emerge. We think that many investors who are interested in digital gold are interested in it primarily for its ability to serve as an inflation hedge that can be transferred over a communication channel. If given a choice between a version of Bitcoin with massive scale and utility that is seizable and recoverable or a version that is non-seizable and censorship resistant but is unable to scale, we think most will opt for scale and utility.

BITCOIN COMPETITORS

Although aspects of Unbounded Capital's vision for Bitcoin (like user-centric data ownership, improved interoperability, and improved privacy) have excited some operating within the cryptocurrency consensus, they assume that achieving it on Bitcoin is not possible. This assumption is rooted both in Bitcoin's perceived lack of scale, and also in the view that Bitcoin lacks key functionality that networks like Ethereum have. This has prompted the development of new, supposedly more scalable, functional protocols to accomplish what is ostensibly beyond Bitcoin's capabilities.

Blockchains like Ethereum were marketed in part as "turing-complete" Bitcoin. This insinuates that Bitcoin is not capable of the same types of computations that platforms like Ethereum are. This assumption is widely held, but is false. Multicoin Capital acknowledges that Bitcoin is "**technically programmable**," but Bitcoin is widely thought not to be turing-complete. To be turing-complete is to be able to compute anything that a turing machine can compute, or as it is commonly understood, to have the computing ability of a modern computer. Bitcoin script, a function largely disabled by BTC, but re-enabled on BSV, is computed through a 2-PDA, a structure well known for being turing-complete. While the view that Bitcoin is incapable of what other smart-contracting platforms can do is erroneous, BTC's lack of scale at the time these competing platforms were developed made the interrogation of this false assumption pointless. In practice, BTC lacks turing-completeness, and the BTC developers' stubbornness about maintaining this limitation incentivized the creation of alternative platforms. Had BSV been around then, it is unclear whether or not these platforms would have proliferated.

Turing-complete, programmable Bitcoin alternatives like Ethereum have promised a vision of a decentralized web3. Today, the cryptocurrency consensus contends that their vision of web3, perhaps best articulated by Multicoin Capital, is still in the early days. At Unbounded Capital, we disagree. We believe the assumptions guiding the development of these protocols are in their late days. The theses built on these assumptions are being disproven in real time by a stunning lack of adoption and scalability.

What has twelve years of non-Bitcoin cryptocurrency development yielded? As of our latest edit in 2022, we have a landscape of thousands of non-Bitcoin cryptocurrency and blockchain projects which cumulatively are valued at over $1 trillion. What do these projects do? Unfortunately, outside of enabling speculation on their future value, the networks do very little. The most highly valued layer-one Bitcoin alternatives like Ethereum, Cardano, and Solana have enabled few if any popular decentralized applications (DApps) and appear to have already hit scaling limitations. For instance, the most common use-bases of these layer-one blockchains in terms of DeFi and NFTs have also been most successfully used as vehicles for speculation.

With its launch in 2015, Ethereum was the first Bitcoin alternative to enable the development of DApps. Five years in, what is the current state of DApps? The website **State of The DApps** monitors DApps' and their platforms' publicly available metrics over time. The metrics (as of the book's original publication in 2020) reveal DApps to be a virtually unused technology.

Platform	Total DApps	Daily Active Users	Transaction Volume (24 hours)	Number of Contracts
Ethereum	2,823	31,910	79,260	4,420
EOS	323	13,210	855,010	509
Steem	84	8,510	352,440	172
Klaytn	50	30,020	153,770	118
Hive	25	2,650	9,320	46
Blockstack	23	-	-	0
Neo	21	175	2,730	31
POA	19	65	1,030	48
TRON	19	2,730	23,270	87
Loom	15	-	-	54
xDai	12	5	25	39
ICON	9	1,300	62,230	8
GoChain	7	-	-	17
OST	2	35	373	2
Total	**3,432**	**90,610**	**1,539,458**	**5,551**

THE FAILURE OF DApps

Compare these cumulative ~ 3,500 DApps across 14 platforms five years after Ethereum's launch to the Apple App Store's **900,000+ iOS apps** and Android Google Play's **1,000,000+ apps** available in 2013, five and four years after their respective launches. Five years in, these DApps cumulatively generate less than 100,000 daily active users (DAU). Contrast this to the big winner of Apple's five year anniversary, **Candy Crush Saga, which generated over 128 million DAU playing 1.2 billion unique games per day by itself in Q4 of 2013**. Worse still, *State of the DApps* lists about 35% of these DApps as abandoned projects, suggesting diminished possibility for future growth for over a third of existing DApp projects.

Beyond the woeful metrics, what are the apps that do exist currently used for? As we've seen with Apple and Google's app platforms, a popular use case is gaming, which makes up the plurality of DApp's DAUs with roughly 30%. Online card games like **Splinterlands** (built on Steem) or retro-aesthetic role playing games like **My Crypto Heroes** (built on Ethereum) have 4,200 and 2,500 DAU's respectively, topping the State of the DApp charts. However, these decentralized games pay a heavy price on user experience due to exceptionally high barriers to entry for user onboarding. To simply play DApp games like Splinterlands and My Crypto Heroes, users need to link crypto wallets, which requires making accounts on third party services like Metamask or Steemconnect. Once made, these accounts need to be funded with the relevant cryptocurrencies, which often require users to make yet another account on one or multiple third party exchanges. Contrast this to typical iOS or Google Play games that either don't require sign-in, or, if they do, leverage authentication services like Facebook or Google where users already have accounts. iOS and Google Play games that come with a cost or include in-game purchases typically incorporate one-touch payments with everything denominated in, or automatically converted to, currencies the users already own.

Even if one is able to make a successful DApp given these user experience challenges, limitations on scale can kill momentum. The most famous example was CryptoKitties, **a digital pet breeding game which caused a massive amount of congestion on Ethereum** leading protocol developers to criticize the game for taking up space for frivolous reasons. Ethereum has made plans to address this lack of scalability, but doing so has added complexity to the developer experience. In fact, the CryptoKitties team found Ethereum proposed scalability solutions such as sharding to be so damaging that they **launched their own blockchain** instead of continuing to use Ethereum. Since the

original publication of this book, NFTs have seen a meteoric rise in popularity but have not managed to transcend the limitations of unscalable blockchains that Crypto Kitties demonstrated. More on this in Chapter Ten.

DApp OPTIMISM

Considering these shortcomings in user experience relative to the competition, it's no wonder DApp games have such abysmal traction. Despite attempting to buy additional scalability relative to BTC by sacrificing some decentralization, these platforms are still unable to offer a gaming experience that can compete with existing apps. So what else can DApps offer? The State of the DApps' data indicates that the majority (roughly 55%) of DApps' DAUs fall under the categories of Exchanges, Finance, Gambling, and Wallets, which together facilitate the buying, selling, trading, and saving of cryptocurrencies.

It's somewhat ironic that despite the DApp platforms' *raisons d'etre* of expanding blockchain's utility beyond BTC's digital gold use case, the same inability to scale while maintaining decentralization encouraged platforms like Ethereum to gravitate towards a vision similar to digital gold dubbed decentralized finance (DeFi) and another speculative vehicle for collector's art called non-fungible tokens (NFTs). Despite the irony, the shift to this focus makes logical sense for a few reasons. First, from a developer's perspective all of these are computationally cheap and thus technically feasible despite the platforms' lack of scale. Second, the DeFi and NFT visions and applications fall in line with the BTC inspired consensus understanding of cryptocurrency that suggests the technology's value is primarily financial in nature.

Operating in this DeFi context, these products are offering ostensibly novel services like taking out a USD-backed loan without interacting with any established financial institutions, and thus have no direct competition so long as "[not] interacting with any established financial institution" is the primary selling point. The last reason is perhaps the most subconscious, and most important, factor in attracting resources and attention to DeFi. Because it is currently technically possible to build tools on an unscaled protocol to facilitate speculation, which is fundamentally about *future utility*, the cryptocurrency ecosystem's lack of *current utility* due to unscalability can be forgiven. That is to say, by shifting the burden of scaling and utility creation to the theoretical-future, the failures of the practical-present can be ignored while still claiming cryptocurrency as a revolutionary technology.

WHY HAVEN'T DApps SUCCEEDED?

The consensus' explanation for DApps abysmal traction and lack of user friendliness is that the technology is still in the early stages of its development. The infrastructure that DApps need to succeed is still being built and scaled. Once their scale is increased, they will be more user friendly and able to compete with the likes of Candy Crush. Multicoin Capital says as much in a blog post titled "**The Web3 Stack**",

> *"Considering how much of the Web3 stack is still under development, it's no wonder that dapp usage is abysmal: it's practically impossible to build usable dapps given the state of the Web3 stack today! Like many other technologies, the Web3 stack will progress slowly, and then quickly after surpassing some tipping point.*
>
> *"The dapp revolution will happen shortly after the Web3 stack achieves some level of usability, stability, and feature-completeness. I suspect this is 2-3 years out."*

In 2022, almost four years after this blog's publication in July of 2018, DApp and decentralized protocol scale have shown no real improvement. The idea that it is still early would make more sense if not for the array of new Bitcoin-alternative blockchains that have been developed since and claim to enable greater scale. A fund like Multicoin Capital, which has invested in several allegedly scalable layer-one protocols, needs to explain why these protocols currently lack DApps. After investing in DApp platform **Solana**, Multicoin Capital published **a blog post that claimed** "Solana offers all the properties that developers of trust-minimized apps need," noting its ability to enable throughput that "today supports 50,000 transactions per second on a global network of 200 consensus nodes." Platforms like Solana have failed to get significant traction with DApp creators and users because they are either unable to actually achieve the scale they claim, or perhaps their product – a DApp platform offering trustlessness and censorship resistance – is not wanted. In Solana's case, although it has significant technological problems, it has largely been used for minting and trading NFTs. Even with this lack of demonstrated product market fit, **funds like a16z are still investing in a DApp future**, having recently led a $21M token sale for NEAR protocol, a platform for building DApps.

Unbounded Capital's explanation for the failures of DApps and the allegedly-scalable platforms they are built on is that the people who are funding and building these technologies fundamentally misunderstand the value of Bitcoin, cryptocurrency, and decentralization. These DApps are built to provide a trust-minimized, censorship-resistant user experience. This is not valued by the market for reasons we will explain in Chapters 3 and 4.

FUNDRAISING AND UTILITY

In our view, the ICO (initial coin offering) craze of 2017-2018 goes a long way in explaining the continued investment into DApp platforms and protocols without any demonstrated product market fit. According to an **article in CoinTelegraph**, ICOs were used to raise $6.9B dollars in Q1 of 2018. Most of this was for platforms or protocols that could be used to build DApps or for specific DApps themselves. This ICO craze launched the careers of many crypto investors and made it appear that there was genuine interest in the goal of decentralizing the internet. The early success of DApp oriented theses and early retail investor enthusiasm has fueled years of continued development without continued interest from users or retail investors.

Just a year after **Dentacoin**, a blockchain concept for the global dental industry, individually set out to raise $28M, only $118 million in total was raised through ICOs in Q1 of 2019. This was in part because the fundraising mechanism of an ICO had gone out of style, primarily for legal reasons. It still points to a declining interest from the broader public and suggests that the current theses are unsustainable. It will take time for these projects to run out of money, as VCs are still providing a lifeline to the DApp industry, but ultimately these platforms need to get some traction or interest will die out completely.

The following focus on other token offerings such as Equity Token Offerings (ETOs) and Security Token Offerings (STOs) after the year of 2018, as well as the craze surrounding non-fungible tokens (NFTs) in 2021 were similar in that they initiated with great optimism only to lose traction for one reason or another.

WORTH THE COST?

The decision to intentionally cripple Bitcoin's inherent scalability in the name of decentralization has been an incredibly costly error for the cryptocurrency consensus. What was gained in a theoretical concept like decentralization came at the expense of providing a network that could generate enormous utility. This trade-off has rendered BTC and the cryptocurrency consensus' favorite Bitcoin-alternative projects unable to deliver more than a casino of virtual assets and hobbyist level games and applications that fail to generate interest. At Unbounded Capital, we think it's clear that the demand for inefficient DApps simply isn't there. Attempting to convince people that they should want a decentralized network for ideological reasons appears to be a failed strategy.

PART TWO
Faulty Assumptions of the Crypto Consensus

CHAPTER THREE

Trustlessness

CRYPTO CONSENSUS VIEW

Traditional businesses are trust-based while blockchain applications can be trust-minimized.

UNBOUNDED CAPITAL VIEW

Current applications of blockchain technology don't minimize trust but instead shift trust from traditional counterparties onto code and developers.

In the absence of efficiency, trustlessness is one of the major qualities of Bitcoin and other blockchains that inform the crypto consensus view of what makes these technologies valuable. The crypto consensus imagines that reliance on trust is something that blockchain can be used to minimize or eliminate. This ability to remove trust is thought to be a major source of blockchain's value relative to traditional options. **The Bitcoin wiki** states that "Bitcoin is only useful if it is decentralized because centralization requires trust. Bitcoin's value proposition is trustlessness."

Blockchain applications are often referred to as trustless or trust-minimized. While the crypto consensus acknowledges that trust has served an important and useful function in the world to this point, its necessity poses a threat that many would like to avoid. The theory follows that as trust-minimized applications become more and more efficient,

users will increasingly opt to eliminate the need for trust rather than continue to rely on it and risk occasionally experiencing severe consequences from doing so.

In our view, trustlessness is a misnomer. Rather than being trustless, these applications place an extreme level of trust in code and the developers who create that code. The results of this effort are less trustworthy applications. We believe that applications and blockchains seeking to promote trustlessness at the expense of efficiency are highly unlikely to be successful since they are pursuing a goal with little to no value over a goal with immense value.

WHERE DOES TRUST-MINIMIZATION COME FROM?

It isn't surprising that a narrative formed about how blockchains can be used to minimize or eliminate trust when one considers that the introduction of the **Bitcoin whitepaper** is a description of the issues that stem from needing trusted third parties in internet commerce, an issue Bitcoin was designed to solve. However, reading precisely what Satoshi wrote in the whitepaper is extremely revealing and informative about the nature of the problem Bitcoin solved.

> *Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.*
>
> *What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could*

easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Our interpretation of this section is that Bitcoin seeks to be able to remove trusted third parties from internet commerce for a very specific goal: micro-payments. Imagine a version of Google that doesn't know who you are. You make a search, you attach a micro-payment, and you get results. Nothing is tracked. This is impossible without non-reversible micro-payments. The need for micro-payments is obvious, but these also need to be non-reversible or else users could just revoke the money even though Google can't revoke the search. By eliminating the need for transaction processors with a legal obligation to mediate disputes, these casual, non-reversible micropayments become possible.

We do not see this section as evidence that Bitcoin or its blockchain technology can remove the general need to trust third parties. We also don't see anything here that suggests that third parties aren't trustworthy or even generally helpful. It simply points out a specific application that is prohibited by a specific inefficiency of internet payment intermediaries and provides a solution. If anything, the whitepaper makes it seem that the customers are the ones who are untrustworthy. It doesn't put any weight behind a general idea that financial institutions are not trustworthy from the standpoint of providing services.

THE CRYPTO CONSENSUS CONFUSES TRUST WITH ECONOMIC INCENTIVES

The crypto consensus, going far beyond the contentions of the whitepaper, makes a much larger claim about the role blockchains can play in eliminating or minimizing trust. Consider this passage from Multicoin Capital's **Crypto Mega Theses**. In describing what unites their three crypto mega theses, Open Finance, Web3, and Globalized State-Free Money, they note:

The common theme underlying these theses is reducing trust between transacting parties. The modern economy is built on compounding layers of trust. We trust tech giants, banks, insurance companies, the government, and more every minute of every day.

We trust so many institutions that we take for granted just how many layers of trust the economy is built on. When we're born and raised with certain trust assumptions, we don't even recognize them as assumptions anymore. Given global complexity, detecting abuses of trust is more difficult than ever before (e.g. Facebook + Cambridge Analytica, Marriott/Target hacks, Equifax hack, etc.).

For the first time in human history, using open networks bound by cryptography and free-market economics, we can incentivize specific human behaviors without creating new trust assumptions. This is a subtle but profound shift.

This is not to say that trust is intrinsically a bad thing. However, all risk is built on trust. By creating a world with fewer trust assumptions, we can reduce systemic risk, and create ultimately healthier and more productive economies and societies.

They go on to note that "Trust is the foundation on which all financial services are built."

In our view, they have misidentified trust as the foundation on which so much of society is built. At Unbounded Capital, we see economic incentives as the foundation of trust, and thus the foundation of whatever trust is built upon. In starting at the trust layer and not the deeper economic incentives, the crypto consensus creates, perhaps unintentionally, a deceptive narrative. In many contexts, the ability to trust someone is rare, special, and sacred. You may trust your bank, but probably not in the same way you trust your best friend. By using the word trust, which carries this emotional context, it is easy to make the goal of eliminating the need to trust so liberally seem worthwhile.

Ultimately, the crypto consensus succumbs to its own narrative and fails to see that the blockchains and applications they promote do not actually eliminate or minimize trust. Instead, these technologies shift the burden of trust from individuals and businesses to code and developers. In advocating for their specific form of trust minimization, they are advocating for a shift from trusting the economic incentives of traditional counterparties to trusting code and the economic incentives of the developers writing that code. This may seem like an appealing shift, even if trust isn't really minimized, but we will show why in practice one should expect this shift to actually make applications less trustworthy.

TRUST STEMS FROM ECONOMIC INCENTIVES

Oxford defines trust as the "firm belief in the reliability, truth, ability, or strength of someone or something." In the world of economic transactions, reliability and truth take

outsized importance. When choosing a bank, one typically would want the services the bank claims to offer to be delivered reliably and for the information the bank serves them to be true. The same applies to blockchain and blockchain apps. These need to function reliably and the information on these blockchains needs to be true. In this case, truth means that information on the blockchain is what it should be based on the inputs and the rules of the system.

Without considering the economic incentives in the world, the source of so much trust would be utterly inexplicable. Why do all of the things we trust tend to work so wonderfully and consistently? The bank functions how it is supposed to because it wants your business. Computers reliably output the right number because if they didn't, they would be worthless. An entire system of law has been developed over centuries to create economic incentives which promote more cooperative, civil behavior. Individuals' actions are thoroughly dominated by their desire to gain economic benefit while avoiding economic loss. These incentives are not always expressed in dollars or some other currency, but they still exist.

As Multicoin Capital points out, performing calculations about the incentives of one's counterparties to evaluate trustworthiness have become second nature for many. Consider that most would be happy to buy a sandwich from a cafe but would not accept a free sandwich from someone standing out on the street giving them away. The cafe has an incentive to provide good service to get repeat customers. Further, if they did something like serve spoiled or poisoned food, they are easy to track down and hold accountable. The person on the street doesn't have the incentive to give a good product and is much harder to hold accountable. The risk that this is a deranged person handing out poisoned sandwiches is too high for most people to accept the offer, especially since other motives to give away sandwiches are less clear.

TRUST-MINIMIZED APPS MAXIMIZE TRUST IN DEVELOPERS AND CODE

Even if economic incentives are sufficient to generate trust, these blockchains would be extremely valuable if they could provide a genuinely trustless solution. Unfortunately, these solutions are not actually trustless, but instead shift the burden of trust from traditional entities to autonomous code. Even if this shift sounds good on the surface, such a distinction between traditional entities and autonomous code cannot actually be drawn.

Instead, the shift is from one set of individuals and businesses onto another, one that often has far less trustworthy economic incentives than the traditional counterparties.

Computers are very trustworthy. They are used to compute numbers and they are exceptionally fast and reliable at doing so. They can also store a vast amount of information reliably in small physical spaces. The strength of computers at generating true, reliable computation and storing information has changed the world in a dramatic way. Many tasks once delegated to people are now delegated to computers, which are much more trustworthy when it comes to computation and storing information.

The trust we extend to businesses promising to deliver services has become almost universally intertwined with the trustworthiness of computers. Hire a bank, and you are hiring the bank's computers. Companies have an incentive to use computers wherever those computers provide a cost-effective advantage. They also have an incentive to refrain from using computers if computers are not cost effective or if computers threaten the trustworthiness of a product. Choosing to trust a bank versus a trust-minimized open finance protocol is not a choice between trusting people and trusting computers. In both cases, it is a combination.

In the crypto consensus, computers' superiority in computation is extended to mean greater universal trustworthiness of computers relative to humans, even if it isn't always articulated in this manner. Consider this excerpt from Multicoin Capital's **Crypto Mega Theses**.

> *The key innovation enabling open finance is the modularization of financial primitives. By modularizing financial primitives, the open finance stack commoditizes trust such that no application has a unique trust advantage over any other.*
>
> *Modularizing financial primitives is an abstract concept. What exactly does it mean to modularize financial primitives?*
>
> *Over the last 24 months, a number of open finance protocols have launched. All of these protocols are modular, and are being used by higher-level applications (and often combined). None of these protocols market to end-customers, provide customer service, or deal with local laws. These protocols are just pieces of code that live on blockchains. This is comparable to how email is built on a suite of open protocols like SMTP, TCP/IP, and HTML/JS to render email in the browser.*
>
> *For example, let's consider BlitzPredict (BP). BP is an exchange focused on sports betting built on top of the Augur, 0x, and (in the near future) Maker protocols. BP relies*

on the Augur protocol as a means to create different kinds of markets, create shares in those outcomes, and ultimately resolve markets. BP relies on the 0x protocol to trade shares between users. And BP will soon rely on the Maker protocol for its collateralized stablecoin, DAI, to denominate trades. Each of these protocols function independently. Because they are modular, a higher-level application like BP can combine the underlying financial primitives to produce a trust-minimized user experience that was never before possible.

It isn't clear how the conclusion, "No application has a unique trust advantage over any other," is drawn. Perhaps one could conclude that each of the applications had no trust advantage if these applications are combinations of various on-chain code that themselves are all equally trustworthy. Since these applications are trust-minimized, presumably the code is trust-minimized, or fully trustworthy. If they were not, then applications combining them would have variance in their trustworthiness.

Computers are very trustworthy, but code is unfortunately far less trustworthy. That is because code comes from humans, and instructing computers is a complicated task for humans. The complicated nature of this task is what has made the ability to write code such a lucrative skill. Further, actually predicting how code will function has a cost. Intentions are one thing, but any developer knows that code doesn't always work as it is supposed to. If code was extremely easy to predict there would be far fewer hacks and errors. Unfortunately, understanding what exactly code will do in all scenarios is effectively impossible. An entire industry exists to audit code. Another industry exists to provide technical security in case things go wrong. Finally, yet another industry exists which assumes something will inevitably go wrong and require an enforceable resolution. This industry is composed of lawyers, courts, judges, and arbitrators. It occasionally uses police officers, detectives, and correctional officers as well.

Just because code isn't necessarily trustworthy doesn't make any particular blockchain code untrustworthy. As established earlier, trust is a function of economic incentives. Which parties have economic incentives relevant to the trustworthiness of autonomous blockchain code and DApps? Typically, the answer is some combination of the developers of the code, auditors of the code, potential hackers, base protocol maintainers (Ethereum miners in many cases), and possibly token holders since many of these applications have a native token used within the system. Hackers clearly aren't incentivized to help users, but their presence is important since they are the ones who exploit security vulnerabilities. For the others, there isn't a one-size-fits-all evaluation for how these

different entities impact the trustworthiness of various trust-minimized applications. They are almost certainly not equally trustworthy. However, there are some important things to consider which are generally applicable.

The incentives of the developers are very important. How directly do the developers benefit financially from successful usage of the protocol? Are the developers legally or financially accountable if something goes wrong? In today's blockchain apps, the answers are often unsatisfactory in both of these cases. Typically, rather than charge directly for services rendered, developers profit from releasing a token which is used in conjunction with the service. They own an outsized share of that token and benefit from its appreciation. However, token appreciation and successful usage have been shown to have only a loose relationship. Further, the developers are often not considered to be liable if things go wrong. There is no "throat to choke." Law enforcement can be called in to track down hackers, but it is widely accepted that nothing can actually be done to reassign stolen funds. There have been occasional breaches of this assumption, such as when Ethereum rewound the DAO hack, but this is considered against the ethos of crypto, or simply not possible in some cases.

The other parties have very limited, if any, ability to influence the trustworthiness of applications' on-chain code. When things go wrong, it is often widely reported and sometimes usage diminishes. However, this doesn't protect the users who were adversely affected by the first issue. Paid auditors with a reputation to protect is a good sign, although it is far from a guarantee that issues won't pop up. Base protocol operators have very little incentive or ability to ensure reliable service of a specific application using the base protocol. Token holders do have this incentive, but they are plagued by a tragedy of the commons and often have little ability to act if things go wrong.

At this point in time, Unbounded Capital would argue that traditional entities are much more trustworthy than on-chain code because of the economic incentives faced by the relevant businesses and individuals. This will likely only change if and when providers of on-chain code benefit more directly from the successful usage of their code and are more consistently held accountable for failures.

CHAPTER FOUR
Censorship Resistance

CRYPTO CONSENSUS VIEW	UNBOUNDED CAPITAL VIEW
Censorship resistance is an essential property of Bitcoin and other blockchains.	Censorship resistance as it is commonly understood is a liability that makes Bitcoin less useful.

Like trustlessness, censorship resistance is thought to be an essential quality of Bitcoin and other blockchains by the crypto consensus. While the degree to which censorship resistance is necessary or attainable differs within the crypto consensus, it is seen as a positive quality worth maximizing within the constraints posed by other goals in a platform. In our view, censorship resistance as it is commonly understood equates to extralegal status for blockchain based activity. We do not see this as a valuable quality.

Although we agree that there are benefits to users from censorship resistance outside of extralegal status, we think these are more likely to be achieved by a version of Bitcoin that scales, BSV, rather than blockchains that sacrifice efficiency to try and achieve censorship resistance or extralegal status through code. To us, that goal is the inheritance of some of Bitcoin's early adopters who sought to use it as a replacement for E-Gold, a failed cryptocurrency that was widely used for illicit purposes.

WHAT IS CENSORSHIP RESISTANCE?

In the same way trustlessness uses the word trust, the narrative around censorship resistance derives a lot of momentum through use of the word censorship. Censorship is widely considered to be bad, and resisting it is therefore good. But in the context of Bitcoin, what does censorship actually look like? What is it specifically that the crypto consensus wants to resist?

Censorship resistance – the ability for anyone to use Bitcoin without being denied service – can really be divided into two categories: censorship by miners and censorship from governments. This censorship can come in two forms: rejecting transactions and changing the contents of the database. Rejecting transactions is equivalent to a denial of service. For example, if a government issued a freezing order on certain funds, the miners would reject transactions attempting to spend these funds. If a single miner included a transaction containing these in a block, the other miners would reject that block.

The second form of censorship, changing the database, is more potent. Changing the database in a way that follows the rules of Bitcoin is extremely difficult and expensive. We will discuss this more in the next chapter. However, changes can be made that don't follow the rules to meet the goals of a miner or government. For example, if a government wanted to reassign stolen funds, they could add an invalid transaction to the database that miners could then treat as valid. In a sense, this would be extending the rules to accommodate law.

These forms of censorship could be used to make Bitcoin far less valuable. If miners routinely denied service or appended invalid transactions that stole people's balances, Bitcoin would quickly become useless. What is relevant, however, is not what can be done but what would be done, and that is a function of economic incentives. If these mechanisms are available to miners and governments, how would they be used? Would they be used in manners that help or hurt Bitcoin? In our view, this is the important question, and our belief is that, in practice, these forms of censorship would be used to Bitcoin's benefit.

CENSORSHIP IN PRACTICE

It is our view that miners have very little ability or incentive to censor specific individuals or entities. We will expand on this in Chapter 6. However, it is worth highlighting a form

of censorship being practiced by miners which is non-specific to any particular individual but instead censors harmful transactions that hurt the value of Bitcoin as a network.

In BSV, valid transactions are currently being censored through the "first seen rule." Consider that a signed transaction has two states: already included in the Bitcoin ledger and not yet included in the Bitcoin ledger. Before a signed transaction is included in Bitcoin, another signed transaction could be generated spending the same coins. The original Bitcoin protocol used inclusion in the ledger as a way to make sure coins weren't spent twice, but there was no clear way of distinguishing which transaction not yet included in the ledger would ultimately be included. This posed an issue to users who wanted to spend money as soon as they received it, or at least be sure that a signed transaction sent to miners was as good as cash in the bank.

Miners created a solution through transaction censorship. They only accept the first transaction they see which spent those coins. If I pay you BSV and then try to send it back to myself, the miners reject that second transaction assuming it is received second. If a block is mined which includes that second transaction, the block will be rejected, meaning that miners do not include the second transaction. This is a form of censorship which enables a key feature: zero-confirmation transactions. In BTC, this rule is not present. This means that waiting for ledger confirmations, preferably more than one, is best practice. This results in confirmation in seconds on BSV and industry best-practice confirmation times of 60 minutes or more on BTC. Because this form of censorship improves the performance of the system by denying what is likely either an accident or a crime, it is hard to make the case that censorship resistance is always good.

One may argue that this isn't censorship but is instead a new rule. That is a reasonable way of describing it, but it's a distinction without a difference. Bitcoin comes with a certain ruleset, but nothing about those rules prohibits miners from rejecting transactions they feel are not in their best interest to mine into blocks. In creating the first-seen rule, miners are in a way 51% attacking the network. They form a majority coalition to enforce rules not native to Bitcoin. This works because the miners are incentivized to make Bitcoin valuable. Censoring these transactions makes Bitcoin more valuable, so the miners do it.

It is interesting to note why this feature is not present on BTC. Because block sizes are limited on BTC to increase decentralization, there is often a long line of transactions waiting to be included in a block. Paying higher fees lets a transaction move up in line. Now, what if someone sends a transaction at the going fee rate and then traffic spikes?

At this point, their transaction may not go through for hours or days. The workaround is that they can create a new transaction spending the same coins for a higher fee. This destroys the ability to trust that transactions not included in a block won't be spent twice, but what's waiting a few hours or days in the name of decentralization?

TO EMBRACE LAW OR NOT TO EMBRACE LAW

Censorship resistance can certainly have value. Most would argue, for example, that censorship resistance is good in the sense that free speech is good. If political dissidents were prevented from using Bitcoin the way they can be prevented from using a system like PayPal, this would be an undesirable quality of Bitcoin to many, Unbounded Capital included. What is meant by censorship resistance to many, however, is the ability to operate outside of all laws.

Bitcoin can be an extremely private system. Transactions are pseudonymous, and massive scale makes tracing extremely expensive. In BTC, expensive transactions lead users to adopt an account model where payments go from one address to another. With the cheap transactions common on BSV, payments can operate on a many to many basis. If I am sending $10, I can send that in 1000 cent sized transactions to 1000 individual addresses. At 2020's fees this added privacy would cost me around ten cents, about 18 times less than it would cost me to send a single BTC transaction. These techniques make tracing and censorship by profit-seeking miners extremely unlikely since identifying possible targets of censorship would be so costly. Governments, however, are more likely to bear a high cost when they are highly motivated to track criminals or other individuals and organizations. Further, governments can force users to hand over information through existing offline legal means. For these and a host of other reasons, censorship is most likely to come from governments. Because these government actions have significant costs, Bitcoin isn't likely to be used to track petty crimes. This tracking capability is likely to be reserved for large criminal organizations and make Bitcoin far less useful to them.

While there can be costs to users from government censorship, there can also be significant benefits. It is disturbing to think of peaceful dissidents having their funds frozen, but it is comforting knowing that stolen funds can also be frozen and ultimately reassigned. Non-seizable assets are also non-recoverable assets. It is possible to have funds reassigned on Bitcoin, although it would likely require a highly expensive international

court order. This requirement would prohibit virtually all countries from oppressing their own people through censorship of Bitcoin transactions. However, it would permit countries working together to stop major crimes and coordinate to reassign stolen or lost funds. Bitcoin at scale both creates privacy that prohibits mass surveillance and makes auditing systems and proving lawfulness far easier.

With law as a security layer, the incentive to steal Bitcoin is very low because it can be easily tracked if the starting point is known as it would be by the victim of theft. In particular, large honeypots like exchanges and custodians could rest assured with the knowledge that theft or human error could be corrected. Further, by embracing law at the protocol level, BSV businesses and businesses building upon scalable blockchains such as BSV adopt a mindset of compliance. This is far less common on other protocols. Many were funded through illegal security sales in the form of ICOs, and the feeling that decentralization places one outside of the domain of individual jurisdictions has created an attitude about compliance which makes adoption difficult for individuals and enterprises for whom compliance is a must.

STATE-FREE, NON-SEIZABLE, DIGITAL GOLD

Much of the popularity and market cap of BTC comes from its perception as a useful inflation hedge. It is argued that its digital scarcity makes BTC valuable as a store of value, a role which should be accompanied by a sizable market cap. However, it isn't typically made very clear why non-confiscability is necessary for Bitcoin to serve this function.

Multicoin Capital describes the opportunity for state-free money in their Mega Crypto Theses:

> *Because fiat money is bound by trust in human institutions rather than physics, we have to place immense trust in the human institutions that govern money.*
>
> *There is a massive opportunity for a trust-minimized money. A natively digital, bearer asset bound by physics, math, and free-market economics rather than human institutions. That money will be the global, state-free measure of value, i.e. money.*

Another way of saying this could be that it's good to have forms of money that governments can't inflate. It doesn't follow that censorship resistance as commonly understood is also necessary. However, it is clear from Multicoin Capital and the crypto consensus'

bodies of work that non-seizability is a priority for stores of value. Why can't digital gold be confiscatable and valuable? Which is better for storing value – a seizable, recoverable asset or a non-seizable, non-recoverable asset? The latter is a much better target for theft, and presents much greater risks if mistakes are made during transfers. At Unbounded Capital, we think Bitcoin could be used as a store of value, but that a censorship resistant, non-seizable version is much less likely to serve this function long term.

DECENTRALIZATION AND CENSORSHIP RESISTANCE

Many of the decisions made in Bitcoin and the broader cryptocurrency space to this point are hard to understand without realizing that the primary motivation behind them is to maximize the chance that these networks can operate outside of the scope of all laws. The importance of this framing becomes more clear when we understand the extralegal use cases imagined and designed by Bitcoin's early adopters. Once the importance of functioning in an extralegal context is established, we can better understand the cryptocurrency consensus' acceptance of inefficiency and their assumption that code is a necessary and desirable substitute for law.

BITCOIN EARLY ADOPTERS AND USE CASES

It's possible that many of Bitcoin's earliest adopters were users of failed predecessors like E-Gold. E-Gold was a gold-backed online cash that launched in the late 1990s and grew to over one million accounts by 2004. Anyone with an email could register an E-Gold account. The required personal information could be easily faked. Regardless of the intentions of E-Gold's founder, who claims to have earnestly started E-Gold as a legitimate operation, the anonymity provided by the service made it a popular online currency and make-shift bank for criminals. E-Gold was particularly attractive to operators of credit card scams, money launderers, and illegal pornographers whose black market operations needed a way to easily move money internationally without the risk of exposing their identities. E-Gold's popularity among criminals eventually attracted the attention of governments and ultimately led to its demise. In 2007 E-Gold's founders were indicted for money laundering, conspiracy, and operating an unlicensed money transmitting business. In July 2008, three months before the release of the Bitcoin whitepaper, they pled guilty, and E-Gold was no more.

Given the coincidental timing of E-Gold's failure and Bitcoin's launch, it's likely that many early Bitcoin users were introduced to the technology in the context of its potential to replace E-Gold as extralegal money. As early as 2010, Bitcoin enthusiasts were on forums **troubleshooting how to best use Bitcoin in the creation of an online heroin store**. The next year, the online black marketplace *Silk Road* was launched and became one of the first popular commercial applications to use Bitcoin. On *Silk Road*, users bought and sold illicit goods with Bitcoin, demonstrating their belief that it was useful as extralegal money.

INEFFICIENCY AS A FEATURE, NOT A BUG

How was E-Gold shut down? Because the network was operated by a group of identifiable individuals, the government was able to easily apply pressure and cease operations. A reasonable theory for how to avoid this fate could be to remove the central point of failure that a database operator creates. Because Bitcoin was designed to create a database without reliance on any central party, it's understandable why ideologically motivated early adopters understood it as an improved and more robust form of extralegal money relative to E-Gold.

However, Bitcoin's future success posed a dilemma. As users of the network, Bitcoin's early adopters wanted it to succeed and become a widely used online money, since its utility would grow with each new user. However, too much success would be accompanied by economies of scale leading to Bitcoin mining being done in large data centers. The scale of these data centers would make Bitcoin's operators as easily identifiable as E-Gold's, and thus offer no robustness in the event that Bitcoin was abetting the evasion of law. Thus, if Bitcoin was intended to be E-Gold 2.0 it needed to be successful, but not too successful. This required trade offs which were eventually made by BTC, like limiting the computational growth of the blockchain and removing its smart contracting functionality. In removing these features, BTC's developers forced network operators to keep Bitcoin computationally small, decentralized, and thus inefficient. Influential BTC thought leaders like Nick Szabo, who had spent the 1990s and early 2000s thinking publicly about how to remedy the weaknesses of centralization experienced by E-Gold, have gone as far as suggesting that inefficiency is a key feature of Bitcoin. In a **Multicoin Capital blog post** they support Szabo's suggestion, writing

> *"Nick Szabo frames trustlessness as an inverse function of technical efficiency. Basically, the less efficient the computer, the more difficult it is to manipulate. The more*

difficult it is to manipulate, the more you can trust it, therefore making it trustless. In other words, to paraphrase Szabo, blockchains trade technical efficiency for social scalability."

Because of this perspective, it was the goal of BTC developers who desired the creation of E-Gold 2.0 to make Bitcoin as inefficient as possible. In this they succeeded. The logic required to end up at this backwards conclusion only makes sense under the assumption that Bitcoin's utility as an extralegal tool is paramount.

CODE AS LAW

A necessary logical conclusion of assuming that BTC's value depends on its usefulness as an extralegal money is that law cannot be a part of any system that interacts with it. This sounds obvious and largely desirable for individuals who are exchanging illegal goods online, but without law present, the ability to enforce contracts is made more difficult. What's to stop someone from sending you subpar drugs after receiving payment in anonymous and non-reversible BTC as E-Gold 2.0? In physical black markets, contracts are often enforced through the threat of violence. In an anonymous online black market, physical violence isn't an option. To remedy this, the developers of online black markets like *Silk Road* concluded that code must replace law. If the drugs aren't delivered as described, sellers could be punished through reputational violence rather than physical violence. More technically complicated systems of escrow were theorized to guarantee the ability to exchange with BTC "trustlessly." While the assumption that code is law in the context of online blackmarket activity makes some sense, why are users extending this assumption to virtually all of today's legitimate cryptocurrency projects which operate in a context where legal recourse is available if someone defrauds you?

Unfortunately for many cryptocurrency investors' sensemaking, the framing of what one might desire for Bitcoin in a black market context stuck and has since extended to the legitimate cryptocurrency and blockchain ecosystem. As a result, inefficient solutions to solving trustlessness have become a necessity with the economic incentives from law removed. Law has become understood as something that is either undesirable or ineffective in regulating cryptocurrency. In the context of legitimate goods and services, the desire to remove law simply doesn't make sense. If one is acting within the law, there is no reason one would not be able to leverage legal remedies if one was robbed. Importantly,

if the assumption that one *cannot* and *should not* have access to legal recourse is baked into the majority of projects using blockchain technology, the resources dedicated to their development will be inefficiently allocated to try and solve an invented risk that logically would only apply to a black market context.

One such example of misallocated resources that presupposed code replacing law is the decentralized platform **Augur**. *Augur* is a decentralized prediction market and was an early success story of DApps. A key innovation of *Augur* was the ability to trustlessly serve as a decentralized oracle which could translate off-chain reality into on-chain outcomes. Imagine you want to place a sports bet in a trustless and decentralized context. How can you know if the Chicago Bulls won or lost last night's game in order to determine the outcome of the bet? If building a betting application in the context of law you would simply appoint a trusted oracle who would relay the information after it happens. An easy solution would be Google or a large institution without incentive to lie. If in reality the Bulls win but Google misreports the outcome claiming that the Bulls lost, defrauded gamblers would be able to hold Google accountable through law. In the code as law context of the cryptocurrency consensus which informed *Augur's* design, the use of law as a backstop is not possible. As a result, *Augur* has invested extensive time and capital resources into designing a network with perfectly calibrated incentives such that the platform can determine the factual conclusion without needing to rely on any one individual.

The problem with this, of course, is that balancing the incentives through code such that the system is perfectly free from error is virtually impossible. In 2019, *Augur* was experiencing significant problems with **scammers using the platform to create misleading and invalid markets as a means of stealing user funds**. The reality is that without consequences from law acting as a disincentive, scammers will inevitably find loopholes to exploit and rob users. Writing the perfect code is not a realistic expectation, and pouring resources into attempting it is a waste when extremely simple and effective solutions currently exist under the protection of law.

BTC AS E-GOLD 2.0

The parallels between E-Gold Founder Doug Jackson's vision for E-Gold and the current state-free money/digital gold vision for BTC are striking. **As described in a Wired exposé** written in 2009, one year after Jackson's guilty plea,

> *"Jackson envisioned (E-Gold as a) private, international currency that would circulate independent of government controls, and stand impervious to the (stock) market's highs and lows. Brimming with evangelical enthusiasm, Jackson proclaimed (E-Gold) a cure for the modern monetary system's ills and described it at one point as 'an epochal change in human destiny' and 'probably the greatest benefit to humanity that's ever been thought of.'"*

Compare this to **one of Multicoin Capital's three crypto mega theses** on "Global State-Free Money."

> *"There is a massive opportunity for a trust-minimized money. A natively digital, bearer asset bound by physics, math, and free-market economics rather than human institutions. That money will be the global, state-free measure of value, i.e. money. The simplest way to think about the opportunity for a global, state-free money is digital gold....The transition from a trust-based economy to one of self-sovereignty will be behind one of the largest wealth transfers in human history."*

Multicoin Capital goes on to claim that global state-free money like BTC is "seizure free," like "a Swiss bank account in your head," and imagines it addressing a market as large as $100 trillion.

> *The demise of E-Gold was preordained by its success and usefulness in evading the laws of powerful governments like the United States. If extralegal status is a key value proposition of BTC as the cryptocurrency consensus claims, how will powerful governments respond to its success? Because E-Gold was technically centralized on servers operated by its founders, it was relatively easily shut down once its illegality was identified. The ideologically motivated developers in charge of BTC appear to be betting that decentralization can save them from E-Gold's fate. Even if ideologically motivated protocol developers are able to avoid this outcome for the underlying BTC network, for most, it's unlikely that the costs paid in crippling BTC's efficiency and removing the safeguards of law will make the benefit worthwhile. Besides criminals using BTC as state-free digital gold, the cost/benefit analysis of limiting Bitcoin's usefulness doesn't make sense. For all legitimate use cases of Bitcoin, the removal of law in favor of decentralization and rule by code-as-law has dramatically reduced the network's utility rather than increased it.*

CHAPTER FIVE

Proof-of-Work is Much More Than a Consensus Protocol

CRYPTO CONSENSUS VIEW

Proof-of-Work is a resource-intensive consensus mechanism that can be substituted for other consensus mechanisms, namely Proof-of-Stake, to improve scalability without significant consequences.

UNBOUNDED CAPITAL VIEW

Proof-of-Work is much more than a consensus mechanism and performs other key functions in making Bitcoin trustworthy.

At Unbounded Capital, we think Multicoin Capital and the crypto consensus are mistaken for prioritizing Bitcoin's trustlessness and censorship resistance over its scale. At a more fundamental level, we don't think they truly understand why Bitcoin works. This is evident not only in their evaluation of Bitcoin's scaling potential, but also in their significant investments into systems that have abandoned an essential component of what made Bitcoin successful: its Proof-of-Work protocol (PoW). For anyone unfamiliar with PoW, we recommend reading **this description of PoW** on our website.

The crypto consensus typically describes PoW as a consensus protocol, or a method of reaching consensus on the contents of a blockchain. PoW does serve this function, but it accomplishes much more. By thinking of PoW simply as a consensus protocol, the crypto consensus misses key elements of PoW that make Bitcoin trustworthy. In particular,

their significant investments into Proof-of-Stake (PoS) networks – such as **a16z's recent investment in NEAR** – demonstrate this misunderstanding. By examining how PoW makes Bitcoin trustworthy, we can better understand Bitcoin itself and see where firms like Multicoin Capital have erred in their investment into PoS systems. For anyone unfamiliar with PoS, we recommend reading **this description of PoS** on our website.

WHAT IS BITCOIN?

Bitcoin is often thought of as a digital currency. While this is true, it is inseparable from the fact that Bitcoin is also a revolutionary database. Bitcoin's PoW protocol solves a complex coordination problem which, prior to Bitcoin's specific use of PoW, made creating a truly public and immutable database that people are willing to use impossible. The potential applications of this type of database are vast. In fact, when Bitcoin abandoned these other applications in favor of focusing on censorship-resistant digital gold, the widespread excitement around Bitcoin's potential morphed into the "blockchain, not Bitcoin" movement which found the ledger more exciting than the currency. However, in our view the two are not separable, and attempting to divide them has already proven to be as unproductive as limiting the potential of Bitcoin in favor of censorship resistance.

The Bitcoin database is structured as a blockchain. However, blockchains have existed since the 90s. The blockchain outside of the context of Bitcoin's PoW-based protocol has very little value. In fact, many of the modern "blockchains" – which are really attempts at creating an immutable, preferably public database – have abandoned the blockchain as a data structure. They are colloquially called blockchains, but they aren't actually blockchains. This is fine because a scalable, immutable, and public database is the goal, not blockchain. Unfortunately, these other attempts which fundamentally misunderstand Bitcoin are running into issues that Bitcoin has already solved.

For most, the question remains - how does Bitcoin incentivize the creation of this special database in a manner where users can trust it? The challenges of creating a public database that individuals and businesses trust enough to actually use, especially for extremely consequential purposes, are manyfold. The bar to get people looking to get rich quick to invest in these databases is not so high, but the lack of trust is evident in the failure to get significant adoption from enterprises or a large number of individuals. The beauty of Bitcoin's PoW protocol is that it solves these challenges through its own

design and by making it easy to interface with other institutions like the law, which help add necessary layers of trust.

WHAT DOES IT TAKE TO TRUST A DATABASE?

As we described in Chapter 3, a trustworthy database is one that functions reliably and has true information. In the case of Bitcoin, proper functioning means that the rules are followed and that the information on Bitcoin is what one would expect based on the inputs and rules of the database. Bitcoin data is also immutable. One can expect that once data is added to Bitcoin through the publication of a block, it will always be a part of Bitcoin and it will be in the same location on Bitcoin. Further, transactions in Bitcoin are ordered, so a location corresponds to an ordering. Finally, these blocks are published widely, so the ordering can serve as a timestamp. If data exists in a block published one year ago, that can serve as legal proof that the data existed in that form at that time.

For a database like the one described above to be trustworthy, one needs to be certain that the rules will be followed, the contents will be maintained, and that it will remain accessible. Further, one may want assurances that operating with this database will be an efficient, cost-effective process. It isn't much good if accessing the database or writing to the database is extremely expensive.

Part of the challenge of a public database is incentivizing the maintenance of it. If the database is valuable, incentivizing people to hold a copy of the database is easy. However, adding to the database is possibly a thankless job. There could be millions or billions of entries a second at scale. Making sure that these follow the rules of the database and adding them accordingly is a task that can scale to a huge magnitude. How can anyone be sure that this will be done, let alone done efficiently?

Consider that a private company cannot necessarily do this. When the rules and contents of a database are public and everyone can coordinate to work on the same version, there is no exclusivity to offering services around that database. For example, it's unlikely that selling access to contents that are public could justify the expense of maintaining a public database. If a private company could have exclusivity to the database then in what sense would it be public? If the database wasn't public then the failure of the company maintaining it would mean the failure of the database. It would be foolish to trust the permanent existence of a company as most individual businesses fail eventually.

The ideal circumstance would be if anyone could maintain the database, but without anyone having to worry about whether the maintainer would follow the rules or not. Further, if the most efficient set of maintainers were always doing the maintenance, that would make the database maximally cost effective. This would also accomplish the issue of maintainers failing. Individual businesses involved in maintaining the database can fail while the system continues.

This is what Bitcoin's PoW protocol accomplishes. It creates a system of incentives that allow anyone to participate in maintaining Bitcoin's database where it can be easily understood that these maintainers will follow the rules of the system and that the most efficient maintainers will ultimately take on that role. This makes Bitcoin's ongoing existence, trustworthiness, and efficiency assured.

HOW DOES PoW MAKE BITCOIN TRUSTWORTHY?

Maintaining Bitcoin has cost, primarily borne through adding data to the database. In Bitcoin, additions come in the form of transactions. Therefore, it makes most sense for individuals to pay a fee per transaction to have their valid transactions added to the database. If one has to pay through traditional means, it poses huge problems. Traditional payment methods have high minimum fees which would make it expensive to use the database. Further, if anyone can participate in database maintenance, it isn't clear to whom the fees will need to be sent. The best solution to these issues is to have a native currency that is kept track of within the database. That currency can be used in extremely small amounts and can be paid instantly to whatever entity ends up processing the transaction. This is why Bitcoin tokens are a necessary part of Bitcoin. Paying for maintenance of Bitcoin's database would not be possible without them. In the future it is possible that a tokenized version of something like USD could be substituted, but this poses extreme challenges in the early going and isn't necessarily competitive longterm with a native currency.

The other benefit to this native currency is that it provides a means for speculation by early maintainers. A database like Bitcoin's is unprecedented. People who see the value in it and understand why it will ultimately become useful and trustworthy can speculate on its native currency. This gives early maintainers an incentive to act. If they can receive native currency for their work, they can either speculate themselves or sell to speculators and get paid in a currently usable currency for providing maintenance.

With the understanding that the database maintenance will be paid for on a transaction-by-transaction basis using a native digital currency, two questions emerge: how is the currency initially allocated, and which maintainer gets paid any given transaction fee? Bitcoin's PoW protocol answers both of these questions. Maintainers, colloquially known as miners and referred to as nodes in the Bitcoin whitepaper, add transactions which follow the rules into the next block. To have a block accepted by the other miners, they must prove that they have solved a problem which can only be solved by brute-force randomness using a hashing algorithm. The first to find a proper hash can broadcast their block to the other miners. If the miners accept that the transactions in the block follow the rules and that the Proof-of-Work was done, the block is accepted and miners begin finding the next block. The longest valid chain is considered the correct chain, so miners are incentivized to add to the longest chain and not try to substitute old blocks for their own since these will be ignored by the public and the other miners.

The value in finding a block is that the miner is given the block reward. The block reward includes the transaction fees for the included transactions and what is called the coinbase, a predetermined number of newly minted Bitcoins. These new Bitcoins are released on a per block schedule. The difficulty of finding a block is variable such that a block is found every 10 minutes on average. The issuance of new Bitcoins decreases by a factor of two every four years in an event now called a halving. Ultimately, 21 million will exist where each of these Bitcoins can be further divided into X number of indivisible units, meaning there are 21 quadrillion individual Bitcoin tokens. These indivisible units are now called satoshis. Through this process, new Bitcoins and transaction fees are both allocated. The manner in which these are allocated has a few important consequences key to the success of the system.

PoW PERFORMS AN IMPORTANT SIGNALING FUNCTION

Proof-of-Work uses a lot of energy. Hashing blocks takes energy. This is a major source of marginal cost in Bitcoin maintenance or transaction processing. Many people in crypto consider this to be wasteful. However, what is considered waste by many in the crypto consensus is actually an extremely important signaling function. Hashing is equivalent to sending a signal of investment in the system. This is because hashes are not free, and the only way to recoup value from these hashes is through earning new Bitcoins and Bitcoin transaction fees. That means that the overall level of hash in Bitcoin corresponds to the

total investment in the system and that this investment can only be recouped through maintaining Bitcoin. The more that is invested, the more users can be assured that maintenance will continue.

This signal has another important consequence: exposing the identity of the miners. Setting up a large mining operation is not something that can be done secretly. Large miners need significant facilities to house their hashpower. The visibility of this process exposes miners to their local authorities. This is good, since if mining could be done secretly without any consequences for illegal behavior, the system would be far less trustworthy. The identifiability of miners gives users a "throat to choke" if they aren't served correctly, resulting in damages. Proof-of-Work is such that if one doesn't make a significant investment into mining, one will not be able to mine new blocks and get new Bitcoins or fees. If one does make a significant investment, they become exposed to law enforcement and gain accountability.

PoW LEADS TO EFFICIENCY

A final key quality of the allocation by Proof-of-Work is that it incentivizes efficient transaction processing. Database users care that their transactions are processed efficiently and accurately. Miners are incentivized to maximize their profit per hash. Because the coinbase is a fixed quantity, the way to get profit is to be able to hash more cheaply than competitors and/or to be able to add transactions to blocks more cheaply than competitors. Both of these will allow miners to expand their operation relative to competition and start finding a larger share of blocks. Ultimately, the inefficient miners will be driven out of business and economies of scale, specialization, and innovation will dictate what firms are able to engage in database maintenance at any time.

WHY DOES BITCOIN'S POW PROTOCOL RESULT IN SECURITY?

How can we trust miners to be honest and follow the rules of Bitcoin? The main reason is that Bitcoin is public. New blocks will be scrutinized by competing miners for errors. These miners have an incentive to disregard blocks with errors. They know that other miners will also disregard blocks with errors and that the block reward from that block is still available. Erroneous transactions will also be visible to the public and affected

parties will sound the alarm. If all the miners fail simultaneously, they will still ultimately be alerted of their error and will have to dismiss those blocks. If miners refuse to process transactions correctly, they could be subject to legal action. This would also harm their business and their investments in maintenance equipment.

Finally, the structure of Bitcoin's blockchain plays an important role. Each block in the chain has a block header. These headers are important because they can be used to prove the existence of a transaction in a block through something called a merkle proof. This merkle proof connects a transaction to the block header proving that the transaction is contained in that block. This becomes very useful as blocks grow to be extremely large. Importantly, there is no way to fake a merkle proof. This means that fake transactions can always be detected.

These block headers are chained together in the PoW process, hence the name blockchain. This means that a block header can't be altered in isolation or else it would no longer fit into the chain. These headers are published with each block and are easy for users to keep track of. Since knowing the headers gives one the ability to assess whether a transaction has been included into a block or not, it is very notable if the block headers suddenly change. The headers are public, so changing them in secret is impossible. Further, these headers are chained together through PoW, meaning that for changing one header one must change all subsequent headers. This is prohibitively expensive. The financial difficulty and lack of secrecy in altering the blockchain provides an ironclad incentive to focus on adding new blocks to the chain instead of rewriting history.

Law is another essential component in keeping miners honest. Since miners are visible due to their investment, they can be held accountable if they violate laws. This includes things like stealing Bitcoin or changing people's data. Miners also have very little incentive to act dishonestly since the value of their investment is tied indelibly to the overall economic value generated by the network. If the price of Bitcoin drops or the revenue available from fees drops, miners can recoup less of their investment in each block. Their incentive is the opposite - make Bitcoin as valuable and useful as possible.

WHY PoS MISSES THE MARK

A lack of understanding about what PoW accomplishes, combined with a suspicion that PoW is somehow unscalable, has led firms like Multicoin Capital to seek other solutions. The most popular alternatives by far are variations on Proof of Stake. Multicoin Capital has invested in four PoS blockchains – Algorand, Solana, Dfinity, and Near – and is investing in applications that leverage these chains. They have also written in support of EOS, which is a PoS network, and have invested in applications leveraging Ethereum, which is attempting to transition to PoS.

These PoS networks are purported to have scalability advantages over their PoW alternatives. In our view, this is incorrect. We don't see any theoretical limit on the scalability of either network. This is the focus of Chapter 7, where we explain why there is no limit to Bitcoin's scalability. In our view, scale is the ability for network maintainers to meet increases in demand. To us, the incentives for miners in a PoW system to rise to the challenge of increased demand is much clearer than in PoS. This forecasts a relative difficulty with scaling before considering other shortcomings with PoS.

The main issue with PoS in regards to meeting the challenge of increased demand is a well known phenomenon: the tragedy of the commons. The incentive for PoS miners to improve the speed at which they can process transactions is much less direct than for PoW miners. In a PoW system, more efficient transaction processing will lead directly to a larger share of the fees. This makes efficiency a long-term certainty. In PoS, miners typically have much less to gain from becoming more efficient unilaterally. PoS miners will want the system to be more efficient, but they have little incentive to invest in scale unless all miners invest in scale. Our expectation is that PoW systems will continue to be far more efficient for this reason. **We are observing that the efficiency of BSV today relative to PoS networks is continuing to grow: there is not a single PoS network or any other blockchain network today besides BSV that is gaining users and transactions without transaction costs skyrocketing. In contrast, on BSV, the increased adoption drives costs down.**

Oligopoly is another issue with PoS networks. Since token ownership correlates with access to block rewards, incumbent miners have an incentive to protect their revenue and not make changes that risk their access to that revenue. These sorts of issues have been made apparent on networks like EOS, which has seen people leave the network over concerns that votes to determine which entities would participate in the mining

process **were being traded or bought**. If increasing scale increases miners' costs, this oligopoly has an incentive to resist increased scale unless it is absolutely necessary. If the costs of scaling exceed the benefits to this oligopoly, scaling will not happen. Because all miners are guaranteed work in this system, especially if they can coordinate to stay in power, unilateral improvement is also disincentivized.

This lack of a scaling advantage is problematic for PoS proponents who themselves acknowledge certain PoS shortcomings. Multicoin Capital notes in their essay on **scaling trustless computation** that "PoS schemes are far less battle-tested than PoW schemes in real-world settings. For example, the first PoS implementation, Peercoin, faced nothing-at-stake attacks, among others. As such, PoS schemes should be considered fundamentally riskier." In our view, these security concerns are more of an issue in the early stages. Since all networks go through early stages, these issues are significant, but much of the security in all blockchains is derived from their public nature, which PoS networks share. There are, however, other reasons to be concerned with PoS which suggest to us that they are much less likely to be secure at scale than PoW networks.

Another issue with PoS is the lack of accountability. In PoW, mining requires significant investment in physical infrastructure. In PoS, this is not necessarily the case. PoW miners are necessarily exposed to the public. This brings accountability. Large amounts of cryptocurrency can be owned privately. This is a good feature for ownership, but a worse feature for mining. An attack is much more likely on PoS because miners can be anonymous. On PoW, an attacker will necessarily have an extremely large physical footprint.

Even though there is significant investment in these facilities for PoW miners, PoS can't offer any advantage in terms of economic cost to miners. The economic law that marginal cost equals marginal benefit applies to both protocols. However, PoS does change the nature of the costs in a way that is appealing to environmentalists who see increased use of energy as inherently negative. In our view, however, that energy is being used extremely well. It brings accountability to the miners who maintain the world's public database. We think this will have a positive impact that vastly outweighs any potential environmental cost. Bitcoin can and does work just as well with renewable energy sources. The incentive to save money has driven Bitcoin mining to rely heavily on underused renewable resources. Bitcoin's ability to use these sources ultimately **incentivizes the development** of ways to harness energy that **are typically viewed as waste**. In all likelihood, Bitcoin's environmental impact has been, and will continue to be, positive.

A final issue with the current generation of PoS networks is that they are designed with trustlessness and censorship resistance in mind. Bitcoin was designed with efficiency and trustworthiness in mind. In our view, Bitcoin is undoubtedly the gold standard design for creating a trustworthy public database today. Even if a better design could be created, we think that Bitcoin will have enormous staying power due to its network effects. The future is a future built on PoW.

PoS SUFFERS FROM A MINDSET PROBLEM

What is also particularly troublesome with PoS networks is the technocratic mindset that their proponents tend to espouse. Normally, the arrangement is that there exists some sort of governance structure. This structure can alter the rules. Improvements to efficiency are considered a top-down phenomenon and many of these networks have specific foundations or organizations whose explicit task is to improve the network for all.

Even if the incentives are well aligned in these contexts, we don't think this top-down, governance-oriented mindset will be competitive with a network like Bitcoin in the long run. Bitcoin's rules are its greatest asset, but they also represent its greatest failure to this point. That failure was not clearly stating the rules and establishing a culture of keeping those rules constant. Between the original Bitcoin whitepaper, website, codebase, and existing laws, the rules could be understood. However, the line between what is a rule and what is code that could be, and often needed to be, improved was not clear.

This lack of clarity allowed a culture of changing the rules to emerge. Few people would dispute the necessity to improve Bitcoin's code over time. Code, however, is an instantiation of the rules. In fact, multiple versions of code can exist simultaneously in Bitcoin as long as they follow the same rules. Ultimately, having multiple versions of the code is ideal in order to have more competition and innovation.

However, the need to improve the code was equated with a sense that the system should be improved in other ways. As we've already outlined, these "improvements" tended to prioritize censorship resistance at the expense of scale. Beyond the lack of utility in these improvements, the culture of changing the protocol rules created a great deal of instability. This may not be extremely disruptive if one's goal is digital gold which exists outside of existing financial regulations, but for applications trying to build on Bitcoin, the constant rule changing was a big problem. In fact, many other blockchains

have inherited this mindset of rule-changes dictated by some form of governance. In our view, this is a mistake for a public database where predictability and consistency across time are paramount.

Issues with this governance came to a head in a recent episode involving PoS network Tron and PoS network Steem. Tron acquired the company which founded Steem, receiving about 40% of the STEEM tokens in that transaction. In what was described as a hostile takeover, **they were accused of colluding with exchanges** who were custodying other users' tokens to limit the power of certain developer accounts. At Unbounded Capital, our view is that political struggles to control the rules of blockchains will hinder their progress. If the rules of the system work, it is better to keep them unchanged and let independent actors compete in provisioning them.

This instability can be removed from Bitcoin much more easily than from PoS systems. Innovation is necessary to compete over the long term, but in Bitcoin this can happen at the level of the miner. Each miner has an incentive to become more efficient. That incentive is much weaker in a PoS system, so some central structure tasked with increasing the efficiency over time is typically a feature. We are betting that the Bitcoin miners will innovate far faster than the governance structures on PoS networks.

In BSV, great lengths are being made to codify the precise nature of the rules and a culture is being set to maintain these rules. The result is that entrepreneurs who grew frustrated with the shifting landscapes of BTC, BCH, and Ethereum have been flocking to BSV for both the additional scale and the certainty that comes with well-defined, unchanging rules.

CHAPTER SIX
Why Decentralization Has No Value in Bitcoin

CRYPTO CONSENSUS VIEW	UNBOUNDED CAPITAL VIEW
Decentralization is necessary to achieve trustlessness and censorship resistance. Decentralization also is necessary for Bitcoin's security. This makes decentralization essential to Bitcoin's value.	Decentralization is not necessary for Bitcoin's security or proper functioning. Bitcoin's security is economic and not dependent on decentralization.

In the opening sentence of their essay "**New Models for Token Distribution**," Multicoin Capital states that "Crypto networks are supposed to be decentralized". At Unbounded Capital, we would argue that decentralization is not needed or even important for Bitcoin to be successful. In light of the magnitude of this statement, it is necessary to closely examine what value decentralization has to Bitcoin. We have already identified trustlessness and censorship resistance as unnecessary or even poor goals for Bitcoin, so promoting decentralization to achieve these qualities cannot be the justification. However, are there other ways in which centralization of mining would negatively impact Bitcoin's reliability, security, and general proper functioning?

To consider this question, we decided to pose a thought experiment. Since centralization is typically discussed within the context of mining and efforts to promote

decentralization impact the mining process, it is interesting to consider what Bitcoin would be like under a mining monopoly. We can consider the mining monopolist condition to be a situation where anyone can mine, but only one company engages in mining. What would the problem be with the monopolist miner? The answer to that question makes the value of decentralization very clear. How could a monopolist miner use its position to harm or destroy the value of Bitcoin, and would it?

WHAT CONSTRAINS THE MONOPOLIST MINER AT SCALE?

Before diving into what risks a monopolist miner poses, it is worth examining what forces constrain the monopolist miner. In the history of Bitcoin, technical restrictions on miner power have been given the most attention. In actuality, there is little to no technical restraint on the monopolist miner. A miner willing and able to ignore the protocol can do anything. While cryptography can prevent a miner from signing a valid transaction stealing coins, the miner can just accept an invalid transaction stealing coins instead. If the monopolist miner wants to mint 1,000 new Bitcoins per block, there is no technical limitation that prevents this. This malleability of code is what makes reassigning coins per court order a possibility. The restraints are not technical.

So what restrains the monopolist miner? Many things, but in general, self-interest. To be more specific, economic loss to competition, economic loss from a reduction in business, and economic loss due to legal action are the major constraints on the monopolist miner. The beauty of Bitcoin mining is that upfront investment is required proportional to the revenue available to miners. If Bitcoin mining revenue is $100 billion dollars annually, some amount on the order of $100 billion dollars will be invested annually by that miner. This means significant losses are possible if one loses business to competitors or reduces the overall revenue available.

WHAT RISKS DOES A MONOPOLIST MINER POSE?

With the economic constraints on the monopolist miner, what threat would it pose to the important qualities of Bitcoin – cheap transactions, fast transactions, secure transactions, reliability, scarcity, and service availability?

The classic argument against monopolies is that they raise prices and reduce supply. That is a justifiable fear when a monopoly is enforced by law, but a naturally occurring monopoly is a function of economies of scale. In other words, this mining monopoly occurred because it was able to produce output and process transactions at a cheaper unit price than any other competitor. This also assumes that the monopolist miner has an advantage in any possible specialization of transaction processing. It also isn't necessarily true that a monopolist is incentivized to limit supply and raise prices. Rather, the monopolist is incentivized to maximize profits, which could easily occur at a price below the level which any competitor could offer. Further, the monopolist has incentive to choose a price which doesn't bait possible competitors to invest in a competing entity. Due to these factors, it is highly unlikely that a mining monopolist would adversely affect the affordability of transactions given that the monopoly was formed naturally.

Why might a monopolist miner choose to adversely affect the security of Bitcoin? The typical threat cited is the double spend. A double spend would entail the monopolist miner replacing a transaction that sent money to someone else with another transaction that sends the money back to the monopolist miner. The monopolist miner could also coordinate with some other party to offer this double-spend service. This can pose serious issues if there is no legal recourse. However, in practice this attack would be highly unlikely for many reasons. For one, it would be illegal, and there is no way to accomplish this without leaving a trail of evidence which would make reclaiming the stolen funds through legal action exceptionally easy. This monopolist miner is likely among the most visible and sueable companies in the world with data centers across the globe. Additionally, even if the monopolist miner could get away with it, they would be destroying their own credit and driving business away from the system. Stealing $1000 worth of Bitcoin isn't likely to be worth it to the mining monopolist. Stealing $1 million isn't going to be possible from a legal standpoint. This is the 51% attack vector so many people are worried about in the crypto consensus. It simply isn't economically incentivized at scale.

The reason why the monopolist miner has trouble altering the security of Bitcoin is the public nature of the system. A monopolist miner is forced to make the blockchain public, or competitors will. Further, the system doesn't work without the blockchain being public, as one would have no way of knowing if they had been paid or not without being able to see. In BSV, many are using the blockchain as a database for all kinds of applications. These also depend on a publicly viewable blockchain. Because a miner can only steal or change what is already public, doing so alerts the world to that alteration.

How about the reliability of the system? The monopolist miner clearly has a strong incentive to guarantee uptime. Further, the monopolist miner will be incentivized to distribute data to avoid any data loss and remove central points of failure. Distribution is probably a better word to describe the value of decentralization, and it can be accomplished by a single operator in the same manner as a service like AWS would distribute data.

A far more salient threat to reliability would be changing the rules of the system. This may be the biggest threat from the monopolist, although a strong argument is currently being made that changing the rules would be illegal. In fairness, the allegedly decentralized BTC has undergone many rule changes which negatively affected the reliability of the system. Therefore, it isn't clear that the monopolist miner poses a greater threat than the status quo of achieving changes through "social consensus," perhaps more accurately described as the will of the BTC core developers. What can be assumed about changes made by a monopolist miner is that these changes would result in greater profits to the miner. This may actually be a benefit to the system if these changes increase revenues or lower costs. Profit to miners is certainly a much better signal for making changes to the system than the whims of protocol developers, the primary change agents to this point in Bitcoin's history, are. Further, if one's expectation is that reliability is economically beneficial, it is unlikely that changes will be made that disrupt this reliability. And, the law also exists as a final preventative measure and backstop.

The defined scarcity of Bitcoin is another element that would likely be protected by law but is irrelevant. Using Bitcoin for saving is a function which gives an outsized contribution to the price of Bitcoin. Since there are so many substitute goods for saving value, a miner would jeopardize their source of revenue by altering the planned issuance of new Bitcoin.

What about denial of service? Again, a strong legal argument can be made that a miner is not allowed to prohibit service, sort of like an internet service provider. It is unlikely this miner would be able to freeze users' funds at their own discretion from a legal standpoint. However, even if that case could not be made, there are still major barriers to a monopolist miner censoring his customers. First, the miner would not necessarily know what to censor. Transactions are pseudonymous and the data in those transactions can be encrypted. Among the thousands, millions, or billions of transactions processed every second, what effort can be afforded in an attempt to censor? Further, if one is successful at denying service, that may drive other customers away. If it is known that your Bitcoin can be trapped through arbitrary censorship by a service provider, it makes it much less valuable. This is in contrast to knowing that money can be frozen or reassigned by a

legal authority, since these types of denial of service have extreme benefits in addition to drawbacks.

With so many factors ensuring the monopolist preserves the valuable qualities of Bitcoin, censorship resistance becomes the obvious reason to preserve decentralization. When censorship resistance is defined as existing outside of law, the degree to which it can be achieved through the status quo is unclear, as is its desirability. Many have alleged that mining is already centralized to the point where a coordinated intervention by governments is possible on BTC. This would not be surprising due to economies of scale. Liberty Reserve, a pre-Bitcoin attempt at globally decentralized extralegal online money, was ultimately shut down through the cooperation of more than a dozen nations led by the United States Justice and State Departments. Their failure serves as precedent for such an intervention despite the effective decentralization of the operation. In fact, Multicoin Capital makes reference to the current centralization of networks like BTC and Ethereum in their essay **Why Decentralization Matters: A Response**, where it is noted that there are likely around 20 miners that comprise the vast majority of hashrate on BTC and Ethereum respectively. In that piece this is described as the natural result of cartelization, although we would have probably used the term economies of scale.

Bitcoin's potential has been severely stunted by efforts to preserve decentralization. The major quality that can be preserved through decentralization is what Multicoin Capital calls "sovereign-grade" censorship resistance – in other words, having extralegal status, although it isn't clear that networks like BTC have achieved this due to the inevitabilities of economies of scale. Further, the value of this censorship resistance is not clearly positive, as we outlined in Chapter 4. If you are a Bitcoin user, investor, or enthusiast today, an important question exists: what is the value of decentralization, and what will you give up for it? For the crypto consensus, the answer may be everything.

CHAPTER SEVEN

Why "Bitcoin Can't Scale" is Wrong

CRYPTO CONSENSUS VIEW	UNBOUNDED CAPITAL VIEW
Bitcoin can't scale at all or can't scale while remaining secure/valuable.	Bitcoin has no fundamental limits on its scale and can scale to meet any level of demand.

It is key to the crypto consensus that Bitcoin can't scale. So much has been invested in protocols developed to remedy Bitcoin's lack of scalability that a scalable Bitcoin is an enormous black swan to these portfolios. In one fell swoop, the assumptions girding these protocols would crumble just as a new competitor emerges that could potentially eclipse what these platforms can offer. In our view, this black swan is already here in the form of BSV, and other black swans could develop in the shape of a new blockchain focused on scale. To the crypto consensus, this is as distant a threat as one can imagine. To them, if there is one certainty in all of blockchain, it's that Bitcoin doesn't scale.

WHY IS IT THOUGHT THAT BITCOIN CAN'T SCALE?

It's easy to understand how the narrative that Bitcoin can't scale has survived for so long. That perception is rooted in the fact that BTC, the dominant version of Bitcoin by visibility and market cap, has been defined by its lack of scale. Further, because the majority of

people most involved in Bitcoin assume that decentralization is a requirement for Bitcoin, paths to scale which threaten that decentralization are dismissed. Bitcoin is also thought not to need scale in order to be valuable. It's believed that Bitcoin's scarcity combined with its decentralization is all that is necessary to take on the digital gold store of value function, the only application of Bitcoin that BTC seeks to fill. In BTC, these beliefs and priorities manifest in a version of Bitcoin that doesn't scale and has no concrete plan or strong desire to scale. The assumption that Bitcoin simply can't scale follows naturally.

This assumption is backed up by an intuition that something about Bitcoin is clearly inefficient. Because of the lack of scale, many miners are still small, home-based operations. PoW is thought to be wasteful. How could such a decentralized network of electricity burners be efficient? It is even thought that inefficiency is an essential part of Bitcoin. As we already noted in Chapter 4, Multicoin Capital paraphrases Nick Szabo's description of how lack of scalability leads to trustlessness in their "**Models for Scaling Trustless Computation**:"

> *But first, we need to establish context for the term "trustless." Nick Szabo frames trustlessness as an inverse function of technical efficiency. Basically, the less efficient the computer, the more difficult it is to manipulate. The more difficult it is to manipulate, the more you can trust it, therefore making it trustless.*

The idea that Bitcoin is severely inefficient – but that its limitations facilitate trustlessness and censorship resistance, which ultimately give Bitcoin value – makes sense on the surface. It helps that this goes unquestioned by the crypto consensus. The idea that Bitcoin has wasted a decade functioning far below its capabilities for lackluster reasons seems much less plausible. Experts who embrace the supposed limitations are considered pragmatic and believable. Those who say Bitcoin can replace the internet sound fanciful given the lack of scale to this point.

THERE IS NO BARRIER TO SCALE IN BITCOIN

Vitalik Buterin, a creator of Ethereum and a crypto consensus authority, is confident **that BSV can't scale**. But, how would one actually go about proving that Bitcoin cannot scale? There would have to be some fundamental barrier or an asymptotic expense which could not reasonably be assumed.

Maybe something about the algorithm described by the protocol does not scale. Perhaps there is a fundamental limitation to what can be transmitted between the miners. Maybe there is an economic incentive not to scale which can't be overcome.

Virtually no one actually goes through this process of trying to identify the barrier to scale. The barrier is assumed to be the risk of centralization. We have already established that centralization does not pose a risk to the network outside of bringing it into the scope of law. So, what other barriers to scale may exist, and what is the mechanism for scale if these barriers do not exist?

WHAT IS SCALE IN BITCOIN?

Increased scale is the ability for Bitcoin to include more data and more transactions overall and to accept the same transactions and data at lower fees. Layer two solutions like the lightning network are not actually scaling solutions because they are not solutions that provide the full feature set of Bitcoin, which includes having ownership tracked on the blockchain. These also don't work for technical, economic, and legal reasons that are well articulated **in these resources**.

More transactions and data leads to larger block sizes. In BTC, there is a block size limit. This is the barrier to scale imposed to increase decentralization. It is important to recognize that scaling isn't something that happens by removing a block size limit. Real scaling is a two-sided process. On the one side, users must demand greater scale by generating more transactions and paying the associated fees. On the other side, miners and other service providers must respond to increased demand by investing in greater capacity. Scale happens first and block size increases follow, not the other way around. There is no maximum block size on BSV today, but there is still a long way to go in terms of scaling.

BITCOIN IS HIGHLY FLEXIBLE

To understand Bitcoin's scalability, it is important to realize that the system has a lot of built in economic flexibility. There are two main variables that create this flexibility: the mining difficulties and variable fees.

Bitcoin blocks are supposed to be discovered every 10 minutes on average. The rate of block discovery is a function of hashrate and the mining difficulty. Hashrate, the total hashing volume of miners on the network, can increase or decrease over time depending on the efficiency of hashing and the available revenue to miners. Mining difficulty resets to keep the average block time consistent at 10 minutes. This difficulty resets approximately every two weeks. Since mining difficulty resets to keep average block-time constant, there is no hash-based limitation to scale. If increased scale makes hashing more difficult, the mining difficulty can adjust to facilitate that scale. Therefore, the hashing necessary from PoW cannot be the limiting factor in Bitcoin's scale.

Bitcoin transaction fees are also adjustable. There is no set fee rate in Bitcoin. Users are free to offer whatever fee they like, although there is no guarantee that transactions will be included if fees are too low. If a situation emerged where fees started to increase because current capacities were being reached, miners would be incentivized to invest to accommodate greater scale and earn these higher fees. This is the mechanism that leads to scale. If capacity is reached, fees increase, creating an incentive for miners to invest in greater scale. On BTC, fees regularly increase, but since scale is prohibited no investment occurs towards being able to process more transactions.

BITCOIN'S ALGORITHM IS EFFICIENT

An easy place to look for possible scaling bottlenecks is Bitcoin's algorithm. Bitcoin miners accept transactions, verify them, send them to other miners, include them in a block, solve the PoW puzzle, and then propagate their block to other miners. Which of these steps would be the scaling bottleneck? We know that finding a valid hash can't be the bottleneck, since mining difficulty is variable. An easy place to look for a theoretical bottleneck would be in transaction verification. As of 2020, miners can meet peak demand by verifying hundreds of transactions a second on BSV, but is there an algorithmic limit? Are millions or billions a second possible?

The key to understanding the scalability of transaction verification is realizing that Bitcoin is fully parallelizable. This means miners can validate new transactions independently. Other than in edge cases which can be handled easily, Bitcoin miners can validate multiple transactions simultaneously. This means that a miner can scale horizontally by adding additional computers that work in parallel rather than simply trying to invest in the fastest,

most powerful computer. This horizontal method is extremely common in large professional data centers. The BTC code has not taken advantage of Bitcoin's initial built-in parallelizability for obvious reasons. Since BTC and BSV have shared origins, BSV inherited mining software that was optimized for single-thread processing, not parallel processing. Fortunately, multiple parties are currently building parallelized implementations of Bitcoin mining software to accommodate the future needs of BSV, most notably **Teranode**.

Parallelizability exposes flaws with competing blockchain technology. Platforms like Ethereum have a state which changes on a per-transaction basis. Validators must all evaluate transactions in the same order to determine if a block is valid. This means that only one processor can be used. This limitation has been crippling to Ethereum's scalability and has played a role in their plan to switch to a PoS network that leverages sharding. This plan has been in the works for several years, showing the difficulty of such a task, and many application developers oppose sharding because of added complexity. Many other platforms have this same problem of not being parallelizable. These sorts of mistakes come from protocol developers who haven't properly thought through what it takes to achieve massive scale. This isn't surprising since massive scale is not the goal of most of these projects. Censorship resistance, trustlessness, and in some cases acquiring retail or private financing through ICOs or venture capital are more pressing concerns than building for long-term success.

Some developers in BSV have actually gone through the process of formally evaluating the efficiency of Bitcoin algorithms using Big O notation. Prominent examples are Attila Aros of MatterCloud and Nithin Mani of Xoken Labs. Nithin has **published several pieces** on the scalability of Bitcoin and surrounding algorithms.

MINER BEHAVIORS CAN CHANGE AT SCALE

Other possible bottlenecks on scale have to do with components of the protocol that directly relate to miner behavior. These components include accepting transactions, sharing transactions with other miners, including transactions in blocks, and sending those blocks to other miners. There are no fixed rules for any of these actions. Miners act according to their own interests, as they weigh costs and benefits.

As Bitcoin has worked in a certain way for so long, with most miners simply running the main Bitcoin Core software with default settings, people don't think about the flexibility with these processes. Miners are set up in a peer-to-peer network with other miners and

the default is typically to treat these other miners equally. Ultimately, miners can be more selective about their peers. They can be selective about who they accept transactions from, with whom they share transactions, what they include in blocks, and to whom they send blocks. Users navigate these considerations by having relationships with one or more miners and by adjusting fees to provide more incentive to have transactions included.

It is worth acknowledging that existing systems outside of blockchain have achieved massive scale. Companies like Amazon, Google, Facebook, and Netflix have helped drive innovations in sending massive amounts of data around the world. Internet speeds have increased 100-fold every ten years. Today, **fiber-optic cables are being researched** which can transmit over a Petabyte per second. That means around 1,073,741,824 BTC blocks will soon be able to be sent across a fiber-optic cable every second. There is very little reason to think that bandwidth will be the prohibiting factor for Bitcoin's success.

INVESTMENT LEADS TO SCALE

Ultimately, miners are incentivized to find blocks and include transactions. This is how they make money. Miners will always be incentivized to include transactions if it is profitable. Further, miners are incentivized to make investments that increase their profitability. This can be investing in hardware or software to verify transactions. It could be investing in greater bandwidth to send and receive data more easily. Coalitions of miners can invest in greater connectivity or invest in processes which make coordination easier. Ultimately, the miners who make the best investments will earn an outsized proportion of the available fees by offering a more efficient system. That efficiency leads to greater profits, allowing miners to invest in more hashpower. More hashpower raises the mining difficulty and squeezes less efficient competitors out of the network. The only thing necessary to facilitate this process is demand for using Bitcoin expressed by fee-paying transactions and the elimination of artificial barriers.

THE REAL BARRIER TO SCALE

In BTC the barrier to scale is self-imposed, but this has already been eliminated in BSV. In BSV today, the real barriers are much more mundane, including typical business challenges such as PR, marketing, and sales. The narrative and branding around Bitcoin

today is not conducive to adoption. It is hard to get individuals and businesses to adopt a system they believe is highly inefficient, unstable, and possibly illegal. Because of this perception, people don't think to use Bitcoin the way they think to use other blockchains like Ethereum. Unfortunately, the failures of chains like Ethereum have further poisoned the well of blockchains generally, including BSV, to the extent that a scalable blockchain is not considered by many to be possible without significant tradeoffs.

The lack of scale and usability on public blockchains have driven some companies to consider using private blockchains. However, to the astute reader, the notion of a private blockchain will seem very strange since the point of systems like Bitcoin is to be public. In our view, private blockchains have no advantage over existing database solutions. They are most likely being adopted by companies that are more preoccupied with being perceived as innovative than with actually engaging in real innovation. With the public options having dropped the ball to such an extreme degree in relation to the hype around blockchain, who can blame them?

Ultimately, the misunderstandings surrounding Bitcoin's scale and the value of decentralization will be resolved. Telling a better, more accurate story about Bitcoin and driving adoption is the next great business opportunity for the world. Entrepreneurs are flocking to BSV for this exact reason. Bitcoin is almost certainly too useful to fail. However, the faster that adoption can be driven, the more likely its success is. We chose the name Unbounded Capital because we believe that Bitcoin has unbounded scale and potential. We are working tirelessly to help accelerate that scale and the adoption which drives it. We hope that this ebook inspires others to join us on that mission.

PART THREE
Comparing Theses

CHAPTER EIGHT
Unbounded Bitcoin vs Web3

CRYPTO CONSENSUS VIEW	UNBOUNDED CAPITAL VIEW
Web3 will be composed of a modular stack of many inefficient but trustless protocols which derive their value from decentralization.	The future of the internet will depend on an extremely efficient and massively scaled Bitcoin which derives its security from economic incentives and competition.

At a high level, Multicoin Capital's vision of "web3" has similarities with Unbounded Capital's vision of the internet built on scalable blockchains. In their blog post "**Mega Crypto Theses**," Multicoin Capital describes their forecasted transition from web2 to web3 as being,

> *"about empowering consumers to control their own data, as opposed to the status quo in which tech giants (...) hoard consumer data. As this paradigm shifts, incumbents will lose their primary competitive advantage—their data monopolies and associated network effects—creating massive opportunities for new value creation."*

At Unbounded Capital we mostly agree with this statement and have written similarly about why we anticipate a shift towards a **user centric data ownership paradigm on BSV** and what that might mean for the **existing big data tech giants and their business**

models. The key differences between Multicoin Capital's vision and Unbounded Capital's vision are the specifics on where this data will move, how it will be organized, how it will interoperate, and why the relevant parties will be incentivized to undertake this transition.

HOW TO BUILD Web3

As we illustrated in Chapter 1, we envision Bitcoin becoming the world's single scalable public immutable database. The value of using this database compounds as more data is added and more applications and users leverage it. This is not a property of Multicoin's web3, which is a modular conglomeration of dozens of disparate decentralized protocols and networks. In fact, some of these networks' sole purpose is to allow the other networks to communicate with each other. In their blog post, **The Web3 Stack**, Multicoin provides a visual representation of how they imagine this landscape of networks will look. The diagram and blog post suggest a complex network of interconnected protocols with each serving one of more than a dozen specific purposes, as opposed to a scaled version of Bitcoin serving as a general purpose protocol.

The complexity of such a landscape would make it obviously inferior to a single network with equivalent functionality. The wisdom of Occam's razor, originally written as "Entities should not be multiplied without necessity," encapsulates why. The reason that Multicoin Capital sees value in this vision of web3 is because of the last two words of Occam's razor, "without necessity." Because Multicoin Capital is confused about Bitcoin's ability to scale and the value of decentralization, they think a disparate web3 is necessary in order to achieve our shared goals. If they understood Bitcoin could serve all the same functions on one network, we think they would likely prefer that approach. In their blog post **The World Computer Should be Logically Centralized**, Mulitcoin writes,

> *While there are many types of scaling solutions being worked on, each of them create idiosyncratic forms of complexity for application developers, users, and the ecosystem as a whole. The last of these forms of complexity - what I call "creating ecosystem baggage" - is particularly challenging to deal with. For example, wallets need to know where user assets are across many chains and state channels; users need watchtowers; liquidity providers need to provide liquidity; liquidity pools are broken; latency is introduced in all kinds of weird places; etc.*
>
> *Or said another way: all of these heterogeneous scaling solutions break the elegance and simplicity of a single logically centralized system (but architecturally and politically decentralized) that is bespoke, not uniform, and logically fragmented.*

This analysis is spot on until the parenthetical clause in the last sentence. Because these forms of decentralization are not essential parts of Bitcoin's security or value proposition, they can be disregarded. Combining this sentiment with the reality that Bitcoin is unbounded in scale when left unencumbered by tinkering developers, it appears as though Multicoin is poised to appreciate the full potential of Bitcoin.

HOW TO TRANSITION TO Web3: DATA STORAGE

For the sake of argument, let's assume that Multicoin's web3 vision has been realized. How and why would a business currently using the web2 data storage transition to web3? Recall our analysis of the lack of traction for today's DApps as outlined in Chapter 2. The demand for decentralized internet applications doesn't appear to be strong. If users are as happy with their web2 applications as their current rate of usage suggests, will they abandon them for web3 clones simply because they are decentralized? If not, can we assume that DApp proliferation will be the result of functionality they uniquely offer?

For Unbounded Capital, our answer for how the current internet transitions to an internet built upon scalable blockchains (e.g. a BSV enabled internet) is more clear: economic incentives. The efficiency improvements for both application developers and users will incentivize a transition to scalable blockchains such as BSV. This incentive only increases as information is added. Today this process is beginning with BSV enthusiasts and early adopters launching applications as proofs of concept. As the success of proofs of concept attracts larger organizations, more businesses will understand the efficiency gains that are possible and will leverage it out of necessity to remain competitive.

A prime example of the increasing economic incentives to build upon scalable blockchains is the offering of regulatory compliance enabled by the BSV startup Tokenized. Tokenized enables regulatory compliance to investment tokens such as non-security assets, securities such as publicly issued shares and investment products, and identity tokens such as citizenship and licenses. In fact, Unbounded Capital invested in Tokenized in the wake of the Financial Action Task Force's (FATF) updated guidelines for anti-money laundering and know your customers (AML/KYC) best practices for DeFi and NFTs. While Tokenized offers a Tokenized protocol that is in fact an on-chain presence of compliance-enabling smart contracts on the BSV blockchain, its CEO James Belding is not using the on-chain presence of the corporation to create a Decentralized Autonomous Organization (DAO)

to avoid the company's social and regulatory responsibilities.

In terms of stage of growth, Tokenized is as early to global businesses as ERP software was in the 1980s. Just as ERP moved resource relations to software and automated its management, Tokenized is tokenizing asset ownerships and enabling smart contracting of business relations. However, whereas ERP only reaches larger companies, Tokenized can reach the entire spectrum of business, from entrepreneurial projects led by one or more persons to the largest global enterprises.

At Unbounded Capital, we can imagine a day when the issuance of tokens of all sorts, such as identity tokens for persons, security tokens representing assets, and rights ownership tokens are stored on the Tokenized protocol. These tokens similar to, but more meaningful than, what NFTs offer today arepossibly managed by the Tokenized platform because the costs of creating a token in a web2 manner would cost more than developing a token on web3-enabled Tokenized platform. When such a day arrives, the least costly method for trade of assets or identity checks will be performed on-chain. However, while Tokenized automates the processing of these transactions and business operations through on-chain smart contracts, Tokenized will not attempt to be a DAO devoid of social responsibilities to governments, people and businesses alike. Instead, Tokenized will be a responsible organization that leverages the economic benefits of moving parts of its operations onto the BSV blockchain.

We believe that many more businesses will also be interested in Bitcoin's ability to provide alternatives to the existing online business models like we described in Chapter 1. Similarly, proofs of concept like Twetch, a social network that leverages direct micropayments for microservices, will pave the way and eventually catch the eye of legacy services as they prove this model's viability and benefits. Because of the vast landscape of competing protocols vying for prominence in Multicoin's vision of web3, there is no similar solution which is standardized across platforms to enable micropayments.

HOW TO TRANSITION TO Web3: SMART CONTRACTING

Beyond Bitcoin's scalability, Multicoin Capital also misunderstands the versatility of Bitcoin's scripting language. In their blog post **"Models for Scaling Trustless Computation**," Multicoin Capital describes Bitcoin as "just a trustless database." This requires elaboration and nuance. The initial release of Bitcoin version 0.1 included a robust scripting language

that enabled a full range of programmability. The Opcodes that comprised this language were removed by developers in control of the node software because of the aforementioned concerns over decentralization. Today, as a result of this neutering, only a handful of Opcodes still function in BTC and transaction customizability has been reduced to a limited set of "standard transactions." The removal of Bitcoin's scripting language in addition to the BTC developer imposition of a ~1 megabyte block size limit have resulted in partially validating Multicoin Capital's claim about BTC being "just a database."

While this is somewhat true of BTC, it is not true of BSV. BSV (which, in Samani's defense, did not exist as an independent blockchain at the time of the blog's writing) has restored Bitcoin's scripting language and removed all developer-imposed restrictions on block size. As a result, BSV entrepreneurs and developers are once again allowed to use Bitcoin as more than "just a database." In the same way Multicoin Capital observed **developers leaving BTC for the "greener pastures"** of Ethereum, today's developers are making the same journey from Ethereum to BSV. While there have been several large-scale projects that have fled Ethereum for BSV – like gaming/E-Sports platform **CryptoFights**, which as of April 2022 posted an average of greater than 2 million daily transactions on BSV network, with a daily data size greater than 1.5GB,BSV – it is noteworthy in that (as far as we know, please email us examples if we are wrong) not a single developer has left its ecosystem in favor of any of its blockchain competitors.

Successful investors like Warren Buffet, Charlie Munger, and Mark Cuban have referred to diversification as a "**hedge against ignorance**." At Unbounded Capital, we understand Multicoin's investment in an array of competing protocols at various layers of their envisioned web3 stack as a manifestation of exactly this sensibility. Once one understands that Bitcoin can scale to offer a superior version of web3 in one protocol, there is no need to be diversified amongst inferior candidate protocols which hope to be components of a less viable network. We imagine the difference between the bet on Bitcoin and the diversified bet on component protocols of web3 as being analogous to a dotcom investor focusing exclusively on businesses that leverage the public internet and ignoring any potentially exciting private intranets. In both instances, the incentive is for data to coalesce around one network. The only plausible candidate for this today is BSV. Until another credible candidate emerges, the BSV ecosystem will remain the sole focus of our investing.

CHAPTER NINE
DeFi

CRYPTO CONSENSUS VIEW

DeFi is an early success story for crypto with exciting long-term potential.

UNBOUNDED CAPITAL VIEW

DeFi has little long-term potential for success as currently conceived. Bitcoin's transparency and efficiency will improve financial services, not trustlessness.

As we described in Chapter 2, blockchain has seen very limited usage to this point. Even with hundreds of billions of dollars raised and over a trillion dollars worth of crypto in existence, actual usage of blockchain-based applications is miniscule. One mild exception is the area of DeFi, a shorthand for decentralized finance. In a February 2020 Coindesk article titled **Why DeFi's Billion Dollar Milestone Matters**, writer Brady Dale wrote that "It was only December when the entire decentralized finance (DeFi) market was worth less than $700 million. Early this morning, it hit $1 billion, a figure that even the most fervent blockchain skeptics would have a tough time dismissing as meaningless."

That number has increased to $140 billion at the time of this updated writing in April 2022, and this level of activity still dwarfs all other blockchain apps. What is the opportunity

seen in DeFi? In their **Mega Crypto Theses**, Multicoin Capital describes the opportunity for Open Finance, their preferred terminology for the sector.

> *By making units of value—stocks, bonds, real estate, currencies, etc.—interoperable, programmable, and composable on open ledgers, capital markets will become more accessible and efficient. Just as the proliferation of capital markets over the last 100 years enabled staggering levels of wealth creation, open finance will make capital markets more efficient and accessible to everyone on the planet.*

At Unbounded Capital, we fully agree with this thesis. However, we think that the current generation of DeFi protocols are doomed to fail for the same reasons as the protocols they are built on. The current generation of DeFi is happy to sacrifice efficiency to achieve greater trustlessness and censorship resistance. In our view, it is not these qualities, but rather transparency and efficiency that will improve the current array of financial services and create opportunities for new players who can effectively leverage scalable blockchains such as BSV.

Since our initial publication of this book, the size and scope of the DeFi markets have grown exponentially. Because underlying blockchains continue to support DeFi, the prioritization of decentralization and censorship resistance over scale and efficiency still resonate.

DeFi MAXIMIZES FOR TRUSTLESSNESS

Multicoin Capital makes it clear in their Mega Crypto Theses that they believe the success of open finance will be rooted in trust-minimization.

> *We cannot overstate the magnitude of this breakthrough. For the first time, financial markets can be global, permissionless, and for many kinds of derivative contracts, free of counterparty risk. This was impossible until recently.*
>
> *The world's financial market infrastructure will move to the Open Finance stack because the Open Finance stack enables millions of businesses—those that are local, national, and international in scale—to offer trust-minimized financial products to the people and businesses who need them most.*

As we established in Chapter 3, trust-minimization is not actually the removal of counterparties or trust. Rather, it is the substitution of traditional businesses for autonomous code as a counterparty. A brief look at the history of DeFi reveals these counterparties to be far from trustless.

Consider MakerDAO as an interesting example. MakerDAO is a multi-faceted platform. It allows crypto asset holders on Ethereum to lock collateral, typically ETH, to produce a stablecoin called Dai. That collateral is managed algorithmically to keep Dai pegged at one dollar. Governance of the system is done by holders of a separate token, MKR. MakerDAO is the leading DeFi protocol. More than half of all collateral locked in DeFi is locked into MakerDAO. As of May 2020, there was $457M of collateral creating $98M worth of Dai governed by $350M worth of MKR. Andreesen Horowitz, a VC firm which had recently raised a $515M crypto fund, was an investor in MKR.

MakerDAO is often compared to Tether, the leading stablecoin in the Crypto space with over $8B in supply with daily volume occasionally exceeding $100B. Tether is operated by Bitfinex, a major cryptocurrency exchange. Tether is often criticized for being centralized. Bitfinex has had legal issues with New York State. **According to Tether's own lawyer, at one point Tether was only 74% backed by cash or equivalents**, and again in October 2021, Tether's management companies were ordered to pay a penalty of $41M for making misleading statements and omissions of material fact regarding their backing of USDT with other valuable assets.

In their piece **An Overview of Stablecoins**, Multicoin Capital describes the functioning and potential issues of a centralized stablecoin like Tether.

> *The first [method of issuing stablecoins] is to issue IOUs. This is the model used by tokens like Tether and Digix. Here, a centralized company holds assets in a bank account or vault and issues tokens that represent a claim on the underlying assets. The digital token has value because it represents a claim on another asset with some defined value. The problem with this approach is that it is centralized. These tokens require trust in the issuing party – that they actually own the assets being represented and that they are willing to honor the IOUs. This model imposes serious counterparty risk on holders of the token. Tether is the canonical example given the serious concerns that the public has about their solvency and legitimacy.*

We agree that the solvency and legitimacy of Tether is a serious concern. What is interesting is that a community that values decentralization, trustlessness, and censorship resistance so regularly opts to use a centralized stablecoin. If the existing crypto community does not value decentralization in practice, it is strange that they tend to be so bullish on the ultimate success of decentralization. The reality is that traders greatly prefer using tether. Tether has held its peg much more effectively than has Dai. Even with as untrustworthy a counterparty as Bitfinex, Tether's founders incentive to keep Tether

backed is enough to assure Tether users. If a more reliable counterparty took on this role, it appears likely that they would dominate over decentralized models.

This concern that crypto traders have with MakerDAO may be well-founded. In fact, Coindesk reported on April 14th that MakerDAO is currently being sued by its users in a class action lawsuit.

> *The suit alleges the Maker Foundation and associated parties – including the Maker Ecosystem Growth Foundation, the Dai Foundation and the Maker Foundation – "intentionally misrepresented the risks associated with CDP ownership" resulting in the loss of $8.325 million in investors' money on Black Thursday.*

Recently, on March 30, 2022, a gaming exchange called Ronin Network was subjected to the biggest cryptocurrency theft of all time, involving assets worth $614M dollars. The attacker had stolen the private keys required to authenticate transactions and had transferred large amounts of Ethereum and a USD stablecoin to their own wallets. The company behind the Ronin network's operations is now working with law enforcement to recover the funds.

Another example of a famous attack was the theft of $611m from Poly Network in August 2021. Poly Network is a smart contract platform that allows users to exchange tokens between disparate blockchains such as Bitcoin and Ethereum. The attack was fundamental in that the attacker had found a way to buy tokens on the Poly Network protocol without selling the corresponding tokens on other blockchains. In a stroke of extreme fortune, the money was returned and disaster was avoided.

These two examples demonstrate how the code underlying the bridges that connect multiple blockchains could be vulnerable. It is no surprise that when attacks like this take place, the platforms responsible for recovering the losses due to the attacks rely on law enforcement to recover their assets. By now, it should be obvious to DeFi investors that code is not a risk-free counterparty. Further, the possibility that stolen or misplaced funds cannot be retrieved will be a non-starter for institutions.

Even more shockingly, in May 2022, TerraLabs' "algorithmic stable coin" gave us a great example of the high risk of allegedly risk-free assets in DeFi. A stablecoin pegged 1:1 with the US dollar is as risk-free an example as one might expect. Despite the best intentions of its algorithmic self-balancing mechanism, the UST stablecoin broke its peg and rapidly lost 90% of its value, wiping out nearly $19B worth of value in a matter of days. UST's

more speculative pair asset LUNA fared even worse, losing nearly $28B over the course of several days as confidence was completely lost in the 'stablecoin'.

DeFi SUCCESS IS A FALSE POSITIVE

DeFi is an extension of the true current crypto success story, trading. Speculators have had a field day in cryptocurrencies. The largest businesses by far are crypto exchanges. Unbounded Capital has no problem with speculation, but it is important to recognize that this speculation may be a temporary state. If one network emerges from the pack as the dominant blockchain, how much intra-crypto asset trading will be necessary? In our view, large exchanges have been complicit in propagating a narrative that crypto is unscalable and that tradeoffs are necessary. This is great for their business, since a world with hundreds of protocols and tokens is much better for these exchanges than a world built on Bitcoin.

DeFi today is an extension of this trading-dominated reality. Crypto asset holders have very little that they can do with their assets. While they hold these assets, platforms that allow them to earn interest or gain leverage are very useful. Many traders are happy to get better rates by accepting greater risk through assuming autonomous code as a counterparty instead of traditional counterparties. Many services are also not offered by traditional counterparties for certain crypto-assets, making DeFi necessary in these cases. What this means is that growing DeFi usage today is not necessarily a trend that should be expected to continue.

HOW BITCOIN IMPACTS FINANCE

A consistent message from Multicoin Capital and similar investors is a desire to use blockchain to help bank the unbanked and increase access to financial services around the world. We share this goal. However, we think that the key to increasing access is to increase efficiency and transparency. The lack of access to these services for much of the world is much more likely an issue of costs and benefits and not an issue of trust or censorship. We believe that Bitcoin's efficiencies will reduce these costs and make providing services to more of the world economically feasible. We also think that the centralization of information on Bitcoin will make coordination by financial institutions far easier

and that this will expand the reach of existing services and make new products and services possible. Increased transparency will help make the financial world more reliable. Replacing businesses with autonomous code will not.

As an example of a business increasing transparency, DXSapp (formerly TDXP) is a platform for leveraged derivatives trading that uses BSV's highly efficient immutable ledger to settle trades virtually instantly with fees as small as a fraction of a penny on the Bitcoin ledger. On DXSapp, anyone with some Bitcoin can enter into trades on stocks, crypto, commodities, forex, or stock indices with margin in trades sized as small as $0.01. Active traders looking to enter and exit positions quickly can benefit from near instant settlement on the Bitcoin blockchain, removing the need to wait for T+2 settlement on legacy platforms.

The speed, efficiency, and flexibility of using DXSapp offers traders used to legacy platforms a substantial UX improvement, but for traders in emerging markets these advantages could be the difference between having exposure to these investments and being priced out. As a result, DXSapp has been focused on these underserved markets where the ability to access once impossibly-small trade sizes and low fees make all the difference. DXSapp has had significant traction in Nigeria, where internet technology is widely accessible but access to financial instruments holds significant friction.

Speaking of increased transparency in financial services, another focus of DXSapp is auditability. This is emphasized through its revolutionary liquidity engine which pools funds for its insurance pool from liquidity providers, offering them a stake in "the house" in return. DXSapp users who love the UX of the platform and anticipate its growth in the future can provide liquidity for DXSapp to pay out winners in periods where winners outpace losers, something that in the long-run does not persist on these platforms. In exchange for their provisions to the liquidity pool, users are paid out a portion of trading losses, a major revenue source for platforms like DXSapp. As with the simple placement of trades on the platform, all of this is easily accessible through DXSapp's web app or mobile experience and publicly auditable on the Bitcoin blockchain, which gives liquidity even greater transparency in the process.

CHAPTER TEN
NFTs

CRYPTO CONSENSUS VIEW

The popularity of NFTs demonstrates the potential of DApps.

UNBOUNDED CAPITAL VIEW

The popularity of NFTs to-date has largely been due to speculative fervor: another flavor of digital gold, a use case informed by the unscalability of the projects' underlying blockchains which prioritize decentralization over efficiency.

NFTs, or non-fungible tokens, have existed in the crypto space for several years. Crypto Kitties, the project mentioned in Chapter 2, was so popular that it temporarily rendered the Ethereum network effectively unusable in 2017, simultaneously becoming an early NFT success story and unscalable blockchain cautionary tale. Unfortunately for its users and creators, its success became its own demise as the blockchain it depended on was unable to accommodate the high transaction volume demands of any successful internet application. Since the days of Crypto Kitties, and the original publication of this book in May 2020, NFTs have grown in popularity – both in terms of their reach and market value. In 2022, it's not uncommon to see NFTs sold in commercials while watching nationally televised NBA games, and the **prices that the highest ticket items demand today dwarf the cost of big ticket Crypto Kitties from 2018**. This all sounds

very positive for DApps, but are NFTs proof-positive of the market's desire for applications leveraging decentralized technologies?

Drawing this conclusion may be a mistake. Are NFTs an example of a novel application built on decentralized blockchains or are they simply a variation on the theme of digital gold? The most financially successful NFT projects like Crypto Punks and Bored Apes have risen in price from sub $100 mint fees (the price to purchase them on day 0) to ~$340,000, the price of the cheapest Bored Ape on the market today. While these projects emphasize the community aspect of their NFTs, this value prop is clearly secondary to the ROI that investors have seen and expect to continue. The Bored Ape physical events may be very enjoyable today, but their attendance would likely drop if the ROI on the NFTs turned red, indicating that the community aspect is less a value prop of its own, and more accurately a side effect of their real value prop: massive appreciation.

From our point of view, NFT projects focused almost entirely on the use case of creating rare collectibles that leverage cryptographic signatures to make digital ownership and resale simple on liquid online exchanges (sound familiar?) are especially vulnerable to a shift in market sentiment. If the blockchains that support these collectibles are unable to scale to their use beyond their collectible, speculative value, we think their long term potential will be severely limited. Projects like Crypto Kitties, which aspire to on-chain utility beyond speculation, in the form of fun gameplay, are likely better positioned for success, so long as the blockchains they are built on understand the necessity to prioritize efficiency and scale over decentralization.

Today, we see many such examples of applications that explore how NFTs can be used to enable more than digital gold in JPEG form. **NFTY Jigs**, and its flagship game, **Duro Dogs**, are exploring what efficient and scalable NFTs can unlock for games and the creator economies that develop around gaming. Unlike Bored Apes or Crypto Punks (or Bitcoins), Duro Dogs are not valuable because they are limited in amount. In fact, the supply of Duro Dogs is uncapped, similar to other popular and highly profitable digital items like digital "skins" in a game like Fortnite, which generates billions of dollars in sales annually. In Duro Dogs, there can be hundreds of millions of dogs, but each one is a one-of-a-kind NFT with a unique combination of attributes. Because the dogs are NFTs, they are able to be sold directly to consumers, outside the context of any particular game. Their existence as NFTs doesn't stop at enabling uniqueness and tradability. Because the data that defines the Duro Dogs lives and references an immutable public ledger, they are easily accessible to game developers who want to leverage the user base of Duro Dog owners

to build games and apps which incorporate them. From the player perspective, this creates an interoperable gamespace where their dogs can play and move between a growing list of games and experiences. From the creator perspective, this provides a plethora of opportunities to add value by extending an existing franchise and monetizing it directly to end users who are excited to enter a new experience with their digital pet.

Platforms like NFTY Jigs and their application Duro Dogs have more value propositions to offer their customers from the innovation of NFTs because of the underlying blockchain's (BSV) scalable nature. Minting millions of NFTs, selling them for a median price of $0.99, and facilitating hundreds of millions of transactions updating, moving, and using those NFTs is only economically feasible when the underlying technology scales in such a way that the average fee paid for each of those actions is well under $0.01. Projects like Crypto Punks that use blockchains like Ethereum, and that have seen Crypto Kitties play out, know that high volume use cases are not in the cards. This economic reality has implications on what value proposition a project like Bored Apes can offer their customers. Thus far, most successful NFT projects have had the through lines of creating limited collections and measuring their success via the ROI for early owners. At Unbounded Capital, we think that, while interesting, these throughlines are indicative of a limitation. Are NFTs only valuable for speculative collectibles OR are most NFT projects building on platforms that limit their options to this digital gold 2.0 use case? Once unconstrained by the limitations imposed by unscalable blockchains, NFTs can be used to supercharge creator economies, as NFTY Jigs is focusing on, but the potential extends to myriad other use cases. All unique digital items that would benefit from operating on an efficient public database can be transformed. Think of event tickets, coupons, or even digital rights to goods like music, as discussed in our Spotify example earlier in this book. While NFTs have become a household word, their potential has barely begun to be realized when limited to the collectible use case.

CHAPTER ELEVEN

Why We Believe in Scalable Blockchains and BSV

CRYPTO CONSENSUS VIEW	UNBOUNDED CAPITAL VIEW
BSV is a scam. It is insecure and not worth thinking about.	Scalable blockchains are the only blockchains built for long-term success, and BSV is currently the only scalable blockchain.

We are "pound-the-table" Bitcoin bulls for all the reasons stated in this ebook. We are extremely optimistic about scalable blockchains such as BSV because we think it is the version of Bitcoin that is by far the most likely to capture the full potential of Bitcoin. Currently, it is the only blockchain attempting to increase the scale of blockchain while also decreasing the fees paid by its users. In contrast, the crypto consensus widely views BSV as a scam, or at least sees it as something highly unlikely to succeed. In our view, there are two main reasons for this. First, BSV has a very different type of goal than the rest of crypto, massive scale without concern for trustlessness or censorship resistance. This goal is very difficult to understand for mainstream audiences who believe that Bitcoin is only valuable because of these qualities. Chris Burniske of Placeholder Capital puts the consensus view of BSV well, as he was quoted in a **Coinslate piece** saying, "we've never seen a compelling reason for it." The second reason BSV is dismissed is its heavy association with Dr. Craig Wright. Dr. Wright claims to be Satoshi Nakamoto, the creator of Bitcoin. The firm nChain, where Dr. Wright is Chief Science Officer, is playing a major role in the development of BSV.

The crypto consensus almost universally thinks that Dr. Wright is lying and is not Satoshi Nakamoto. This makes the likelihood that BSV will have value extremely low in their minds.

Our belief is that regardless of whether Dr. Wright created Bitcoin, he is absolutely correct in his convictions about Bitcoin. We strongly agree with his view that Bitcoin is capable of massive scale and that it was not created to operate outside of the law. nChain has poured massive resources into this vision to great success. We think that pursuing this vision through the restoration and professionalization of the original Bitcoin protocol is the most valuable direction for Bitcoin and all blockchains. We have such conviction in this vision that we have made BSV the exclusive focus of our fund. Many others share our convictions. Hundreds of entrepreneurs have flocked to BSV to build on the original Bitcoin, in many cases abandoning other protocols. These developments in BSV are truly exciting, and in our view it won't be long before the consensus view in crypto is that Bitcoin is the future and BSV is the version worth building on and investing in.

DEVELOPMENT OF BSV

BSV became independent in November 2018 when it split from Bitcoin Cash (BCH). In spite of being the black sheep of the crypto world, BSV has seen tremendous progress since that time. The primary goal in BSV's development was two-fold: return to the original Bitcoin rules while professionalizing the code. Since Bitcoin's launch in 2009, the code for the mining software has been maintained by passionate volunteers. This has resulted in an extremely messy codebase that has proven time-consuming to restore without breaking. Fortunately, nChain employs dozens of developers who have been diligently working towards restoring Bitcoin's functionality. This restoration made a huge leap with the recent Genesis upgrade. In February 2020, the Genesis upgrade made two major restorations to Bitcoin: the removal of any block size limits and the restoration of the original scripting language. Miners are now free to scale to meet demand on BSV, something not possible on any other PoW chain. Not only are miners free to scale transaction throughput, they are doing it. Since these constraints were removed, BSV has generated the majority of transactions on public proof of work blockchains by a large margin. BTC, which hovers around 200k transactions processed per day, has been left in the dust as BSV regularly does 10M+ transactions in a day (as of April 2022). We expect this number to grow exponentially over the coming months and years.

WHY WE ARE BULLISH ON BSV

Our conviction that BSV will be a transformational network and that the native currency on BSV will have immense value is rooted in our belief in Bitcoin's potential. We think the efficiencies Bitcoin offers via the centralization of information will transform the internet into something better. BSV is the only network pursuing that goal. We think that the network being formed by the individuals and businesses working towards that goal on BSV will be difficult to overcome for potential competitors. A tremendous amount of infrastructure has already been built on BSV. The incentive for other developers is to shift to building on Bitcoin. Why reinvent the wheel when you can use the wheel? The incentive for investors is to shift their investment in chains like BTC and Ethereum to BSV. Why own something relatively expensive which does not work and is pursuing a less valuable vision when you can own something relatively cheap that works and is pursuing a more valuable vision?

Further, BSV has a distinct advantage in IP via nChain and other businesses building on BSV. **nChain has a patent portfolio** approaching 1000 unique patents related to Bitcoin. Because their understanding of Bitcoin is superior to that of their competitors, this patent portfolio has outsized value due to both its size and relevancy. It is unclear to what degree they will be able to enforce these patents, but it is known that use of these patents will either be open or far more favorable to applications being built on BSV. This is a powerful incentive for start-ups and medium-sized businesses to build on BSV rather than risk legal action or pay increased licensing fees, particularly since BSV is the most functional blockchain anyways.

WHAT IS BEING DONE ON BSV TODAY (April 2022 Edit)

BSV has already achieved scale and efficiency not thought possible for a PoW blockchain, and this is only after three years of independent operation with limited adoption. To date, the largest blocks on any blockchain have been mined on BSV. The largest block on the BTC network to date is 2.26MB. This is about 2000x smaller than the record on BSV, **4GB**. BSV fees today (April 2022) fluctuate, but are typically tens of thousands of times cheaper than on BTC. BSV has significantly higher daily transaction volume than does BTC, with a price that is 530 times lower.

At Unbounded Capital we have never been more bullish about the future of the Bitcoin SV ecosystem. The vast majority of crypto investors continue to overlook this ecosystem's

progress, distracted by all-time-high prices in otherwise struggling networks like BTC and Ethereum. We think the strong foundations laid in Bitcoin SV in 2021 will support enormous value creation in 2022 and beyond.

We are gaining confidence that there is unlikely to be a serious competitor to the original version of Bitcoin as a blockchain that can achieve global scale. There are two metrics we think are indicative about the future of blockchain adoption:

1. Is the network getting faster and/or cheaper with increased usage?
2. Which protocol is attracting the smartest developers and entrepreneurs?

There is not another public blockchain network we are aware of that is getting cheaper over time with meaningfully greater usage like Bitcoin SV.

While networks like Avalanche and Solana are attracting a larger amount of the VC dollars being invested in what are known as scalable blockchains, we are confident this will be another one of the many short-lived trends in crypto. These ecosystems are crashing with increasing frequency as they attempt to scale. There is a widening knowledge gap between investors and builders. These networks, while still relatively cheap today compared to non-blockchain solutions, have soared in cost, putting aside the immense stability and security concerns. There have been significant profits for investors in these blockchains that are not poised for long term adoption, something we think is reminiscent of many of the dotcom companies in early 2000.

We are seeing most entrepreneurs building on Bitcoin SV not trying to make a quick dollar, but instead focusing on long-term value creation. This is reflected in the growing number of companies, projects, developers, building on Bitcoin SV over the past several years. Earlier this year we published the **first comprehensive list** on what is happening in our ecosystem. Depending on what metrics you look at, Bitcoin SV is the 2nd or 3rd largest blockchain entrepreneur and developer ecosystem today behind Ethereum and neck and neck with Solana. And while we can point to dozens of companies that tried to build on Ethereum, Hyperledger, and other blockchains that have since moved to build on Bitcoin SV, we are not aware of a single example the other way around.

When Unbounded Capital began focusing on the Bitcoin SV ecosystem in 2019, we were particularly busy doing due diligence on, and taking meetings with founders of, infrastructure companies. We were excited by Bitcoin SV's layer-one efficiency and scalability,

but the infrastructure required to support the development products was still nascent. For builders and investors, this presented an opportunity. Seizing on this opportunity, Unbounded Capital largely invested in these infrastructure companies from 2019 to 2021, which improved the Bitcoin SV developer experience. These investments included **RUN**, **HandCash**, and **TAAL**, to name a few. Now, most of those companies in our portfolio have raised capital at higher valuations and have meaningfully increased their users and customers.

After years of the BSV ecosystem's (and our own) focus on infrastructure, we are entering a phase of companies building on BSV with the purpose of serving customers. For example, new media and social media companies have launched that take advantage of cheap payments on Bitcoin. Twetch is a standout in adoption, both in BSV and in the wider crypto sphere. Twetch takes on frustrations with traditional social media by offering a Twitter alternative, where all actions have a financial component. Writing a twetch, liking a twetch, following another twetcher all cost somewhere between 2 and 10 cents. Most of those payments go to other users who are responsible for the content being liked or followed. This gives users an opportunity to earn money from the platform and keeps the quality of content high. It's an experiment in a new kind of online community, and it is also a platform that lets users retain control of their own data. All twetches live in Bitcoin's database. If Twetch dies, the twetches survive, and if a competitor emerges, users can take their twetches with them to a different platform. Ultimately, we believe that this type of model will become ubiquitous. The specifics of Twetch may not work, but we think applications providing different views and methods of engaging with the same set of content, the Bitcoin database, will proliferate. User lock-in will no longer be a competitive option.

Some of the larger businesses building on BSV include UNISOT, a supply-chain management solution. They launched the Seafood Chain in 2020, and are using it to track the shipment of Norwegian salmon across the world. EHR Data is an enterprise in the electronic healthcare space partnering with nChain to build a tool which helps doctors, patients, and pharmacies coordinate on the proper prescription of opioids. These sorts of enterprise initiatives are what we believe will create the necessary incentive for Bitcoin to continue scaling to its potential. Bitcoin miners like Coingeek, TAAL, Mempool, and Matterpool are preparing for this future already, expanding their operations through new features like the Miner API and Miner ID and making investments to facilitate real scale.

In 2021 we began to see the positive consequences of the decreased developer friction provided by these companies. This led to a major uptick in meetings with, and ultimately

investments in, companies that leveraged those infrastructure providers' tools to deliver value to businesses and end-users. These companies include **Haste**, **DXSapp**, **Tokenized**, and others. In many ways most of these new companies are fundamentally infrastructure companies in the long-term, but ones that, upon launch, also had consumer-facing products.

The maturation of the ecosystem's infrastructure and tooling not only bodes well for Unbounded Capital by rapidly expanding the pool of companies building on this technology, but it also radically transforms the value of Bitcoin SV ecosystem companies to both builders and investors. The companies we invested in in 2021 and those leveraging earlier portfolio company investments provided tangible experiences of our vision for the future of the internet, supercharged by micropayments and novel types of data ownership. What in 2019 and 2020 were largely theoretical pitches about the future of the web became more real in 2021. Rather than describing the internet to an investor in 1990, we are now showing live demos of email and extrapolating this into a future boon for online connectivity, commerce, entertainment, and more.

The successes of 2021 and the massively positive trajectory of ecosystem development in conjunction with increased investor interest are setting the stage for a breakout 2022. What are some of the things we expect?

- **More acquisitions (e.g. Moodys buying Kompany)**

BSV RegTech KYC/KYB platform Kompany recently agreed to acquisition by Moodys to be closed in the coming months. We expect this variety of exit for BSV companies to become more of a trend in the coming years as the utility of micropayment and novel data applications built on scalable blockchain infrastructure continue to demonstrate their disruptive potential. While many enterprises have been sidetracked by the decentralization red-herring since a boom in blockchain interest in 2017, we think the value provided by companies, those with an infrastructure focus in particular, that leverage Bitcoin SV's unique properties will be impossible to ignore.

- **App growth (e.g. Duro Dogs, Cryptofights, and DXSapp)**

In addition to early BSV-infrastructure exits in 2022, we anticipate consumer-facing startups to see a major uptrend in addition as the friction on onboard users to this growing sector of the economy continues to plummet. HandCash's recent addition of seamless fiat on-ramps has already significantly lowered the barrier to entry to BSV gaming

companies, like Duro Dogs and FYX Gaming, which are targeting typical, non-crypto gamers. Because of the ecosystem's emphasis on interoperability and the ability for onboarded users from one application to earn and use BSV in other, connected applications, we think these improvements will be a tide that lifts all boats in the ecosystem. A rising tide will have an especially positive impact on BSV infrastructure companies, which are providing tools and services for applications across the sector.

Improved investor sentiment from high penetration of content

The transformative potential of Bitcoin SV has begun to show rather than tell. Every month new applications are launched which attract new cohorts of users and demonstrate additional functionality now possible thanks to Bitcoin SV's scalable blockchain foundation. The benefit of these applications are compounded by continued investment into content creation and education by Unbounded and others in the space. In 2021 we saw a major increase in both the quantity and quality of the publications that this content was reaching. We expect this trend to continue in 2022 as Bitcoin SV, and the applications that leverage it, continue to pick up steam.

The pace of BSV's development is extremely exciting, and we expect it will only increase. Since it became independent, BSV has seen an astonishing number of new and existing businesses begin to use Bitcoin's database. Having a functional Bitcoin is an extremely new phenomenon. Many of these projects and companies won't amount to anything, but we believe that some have the potential to develop into billion dollar companies. Further, we have strong conviction that this space will generate many new billion dollar companies and that Bitcoin will accelerate the growth of existing companies who can adopt it successfully.

In our view, the flawed assumptions of the crypto consensus and the confusion they have generated have likely resulted in the waste of millions of man-hours and hundreds of billions of dollars. Because of the cryptocurrency consensus' misunderstanding of the value of decentralization, the role of law, and the technical capabilities of Bitcoin, they have routinely made decisions that accept enormously high costs for no apparent benefit. At Unbounded Capital, we are investing in a future of Bitcoin at scale, a more efficient and accessible financial system, a better internet where users maintain greater privacy

and control, and a better future. We hope that other investors in the crypto community can get behind this vision and start working towards Bitcoin at scale, not just digital gold and trustless, censorship resistant platforms. We look forward to building a future on Bitcoin or a yet-to-emerge scalable blockchain, and we hope that some of you will join us in helping to achieve that goal.

2-PDA: Two-Stack Pushdown automaton, the computational structure used to execute Bitcoin script

51% Attack: The ability of someone controlling a majority of network hash rate to revise transaction history and prevent new transactions from confirming.

Algorithm: a procedure for solving a mathematical problem in a finite number of steps that frequently involves repetition of an operation

Backend: the part of a software system that is not visible or accessible to a user of that system

BCH: The Bitcoin Cash blockchain, a fork of the bitcoin blockchain that shares a history with BTC and BSV (among other, less significant forks)

Big O Notation: Big O notation is a mathematical notation that describes the limiting behavior of a function when the argument tends towards a particular value or infinity.

Bitcoin: a digital currency, and network, released in 2009 for use in peer-to-peer online transactions

Block: One or more transactions prefaced by a block header and protected by proof of work. Blocks are the data stored on the block chain.

Block Header: An 80-byte header, or collection of data, belonging to a single block which is hashed repeatedly to create proof of work. Block headers grow linearly while the blockchain can grow exponentially, so users can track block headers to have a complete reference of the blockchain without keeping a full copy.

Blockchain: a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network

Brute-force Attack/Randomness: In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly.

BSV: The Bitcoin Satoshi Vision blockchain, a fork of the bitcoin blockchain that shares a history with BTC and BCH (among other, less significant forks)

BTC: The Bitcoin Core blockchain, a fork of the bitcoin blockchain that shares a history with BSV and BCH (among other, less significant forks)

Censorship Resistance: Censorship-resistance may refer to a specific property of a cryptocurrency network. This property implies that any party wishing to transact on the network can do so as long as they follow the rules of the network protocol.

Coin Mixer: Bitcoin mixers are solutions (software or services) that let users mix their coins with other users, in order to obfuscate tracing of the coins and provide anonymity.

Consensus Mechanism: A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record-keeping, among other things.

Crypto Asset: A crypto asset is a blanket term which isn't limited to cryptocurrencies. It is a tokenized asset which is issued in a public ledger, that doesn't necessarily derive its value from the chain and whose application isn't necessarily payments. It includes cryptocurrencies, utility tokens, platform tokens, and tokenized securities.

DApps: Decentralized applications (DApps) are digital applications or programs that exist and run on a blockchain or P2P network of computers instead of a single computer, and are outside the purview and control of a single authority.

Database: a usually large collection of data organized especially for rapid search and retrieval (as by a computer)

DeFi: DeFi stands for "decentralized finance" and refers to the ecosystem comprised of financial applications that are being developed on top of blockchain systems. DeFi may be defined as the movement that promotes the use of decentralized networks and open source software to create multiple types of financial services and products. The idea is to develop and operate financial DApps on top of a transparent and trustless framework, such as permissionless blockchains and other peer-to-peer (P2P) protocols.

Digital Permanence: Digital permanence addresses the history and development of digital storage techniques, specifically quantifying the expected lifetime of data stored on various digital media and the factors which influence the permanence of digital data. It is often a mix of ensuring the data itself can be retained on a particular form of media and that the technology remains viable. Where possible, as well as describing expected lifetimes, factors affecting data retention will be detailed including potential technology issues.

Digital Scarcity: The application of effective scarcity, or the state of being limited in amount, to digital assets which are typically trivially copied and multiplied.

Double Spend: A transaction that uses the same input as an already broadcast transaction. The attempt of duplication, deceit, or conversion, will be adjudicated when only one of the transactions is recorded in the blockchain.

Ethereum: Launched in 2015, Ethereum is an open-source, blockchain-based, decentralized software platform used for its own cryptocurrency, ether. It enables SmartContracts and Distributed Applications (ĐApps) to be built and run without any downtime, fraud, control, or interference from a third party.

Exchange: A cryptocurrency exchange is a digital marketplace where traders can buy and sell crypto assets using different fiat currencies or altcoins. A cryptocurrency currency exchange is an online platform that acts as an intermediary between buyers and sellers of the cryptocurrency.

Forking: The process by which a blockchain's code and database are altered which can create an alternate blockchain with a shared common history with the original.

Hashing: Hashing is generating a value or values from a string of text using a mathematical function. Hashes can be used to create a unique identifier for a piece of data. In Bitcoin, hashing is used in proof-of-work to find a unique identifier that makes a block a valid candidate to be added to the blockchain.

Hexadecimal: of, relating to, or being a number system with a base of 16

ICO: An Initial Coin Offering (ICO) is the cryptocurrency industry's equivalent to an Initial Public Offering (IPO). ICOs act as a way to raise funds, where a company looking to raise money to create a new coin, app, or service launches an ICO. Interested investors can buy into the offering and receive a new cryptocurrency token issued by the company. This token may have some utility in using the product or service the company is offering, or it may just represent a stake in the company or project.

Ledger: a book containing accounts to which debits and credits are posted from books of original entry

Merkle-Root: A Merkle-root is the hash of all the hashes of all the transactions that are part of a block in a blockchain network.

Merkle-Proof: A Merkle-proof is the smallest number of hashes needed to prove the presence of a hash in a merkle-root**.** In Bitcoin, merkle-proofs are used to prove that a transaction is contained in a specific block.

Micropayment: In the context of bitcoin, a micropayment is a payment as low as a fraction of a penny

Miner: Mining is the act of creating valid Bitcoin blocks, which requires demonstrating proof of work, and miners are devices that mine or people who own those devices.

Opcodes: Operation codes, or Opcodes, from the Bitcoin Script language which push data or perform functions within a pubkey script or signature script.

Peer-to-peer: relating to, using, or being a network by which computers operated by individuals can share information and resources directly without relying on a dedicated central server

Proof-of-Stake: Proof of Stake (PoS) concept states that a person can mine or validate block transactions according to how many coins he or she holds. This means that the more Bitcoin or altcoin owned by a miner, the more mining power he or she has.

Proof-of-Work: A proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated.

Scalability: Scalability is the property of a system to handle a growing amount of work by adding resources to the system.

Schnorr Signatures: a planned technical feature for bitcoin, and other blockchains, to enhance anonymity

Scripting Language: a programming language that is designed especially for creating short programs to automate simple tasks

Stablecoin: A stablecoin is a new class of cryptocurrencies that attempts to offer price stability and are backed by a reserve asset.

Stack: The protocol stack, network stack, or stack is an implementation of a computer networking protocol suite or protocol family. Some of these terms are used interchangeably but strictly speaking, the suite is the definition of the communication protocols, and the stack is the software implementation of them

State: In computer science, the state of a program is defined as its condition regarding stored inputs.

Timestamping Authority: a trusted timestamp is a timestamp that should be issued by a Trusted Third Party (TTP) acting as a Timestamping Authority (TSA). The Timestamp proves that data (files, text, etc.) existed before a particular time.

Token: A token is a programmable digital asset with its own codebase that resides on an already existing block chain. Tokens are used to help facilitate the creation of decentralized applications.

Transaction: In computer programming, a transaction usually means a sequence of information exchange and related work (such as database updating) that is treated as a unit for the purposes of satisfying a request and for ensuring database integrity.

Trustlessness: A trustless system means that the participants involved do not need to know or trust each other or a third party for the system to function. In a trustless environment, there is no single entity that has authority over the system, and consensus is achieved without participants having to know or trust anything but the system itself.

Turing-complete: In computability theory, a system of data-manipulation rules (such as a computer's instruction set, a programming language, or a cellular automaton) is said to be Turing-complete or computationally universal if it can be used to simulate any Turing machine. This means that this system is able to recognize or decide other data-manipulation rule sets. Turing completeness is used as a way to express the power of such a data-manipulation rule set.

User-centric Data Ownership: A data paradigm in which users of online applications technically and legally own and control their data, rather than data being owned and controlled by third parties

Wallet: Software that stores private keys and monitors the block chain (sometimes as a client of a server that does the processing) to allow users to spend and receive satoshis.

Web3: Multicoin Capital defines web3 as empowering consumers to control their own data, as opposed to the status quo in which tech giants, credit bureaus, advertisers, healthcare providers, etc. hoard consumer data. As this paradigm shifts, incumbents will lose their primary competitive advantage—their data monopolies and associated network effects—creating massive opportunities for new value creation.

REFERENCES

In text citations (by category, in order of appearance)

- Secrets of A Successful Crypto Trader: Question Absolutely Everything
- Binance Academy
  - Trustless
  - Censorship Resistance
- Multicoin Capital Blogs
  - Mega Crypto Theses
  - Models For Scaling Trustless Computation
  - The Web3 Stack
  - The World Computer Should be Logically Centralized
  - New Models for Token Distribution
  - Why Decentralization Matters: A Response
  - An Overview of Stablecoins
- The Bitcoin (BTC) Wiki
- A16z Blog Post on Crypto Fund II
- BSV Case Study: Online Music Marketplace
  - Spotify Business Model
  - Taylor Swift WSJ op-ed on Spotify
  - Business Insider article on Streaming vs Ownership
  - Spotify's Transition to Google Cloud
  - Spotify Statistics
- Bitcoin Mining/Fee Stats
- DApp vs Apps
  - State of The DApps
    - Splinterlands
    - My Crypto Heroes
  - iOS App Store Stats
  - Google Play Store Stats
  - Candy Crush Saga Stats
  - CryptoKitties

- Alternate Blockchains/ICOs
  - ICO Fundraising Stats
  - Solana
  - Near
  - Dentacoin
  - Augur
    - Augur Vulnerabilities
- Bitcoin Whitepaper
- DeFi
  - Why DeFi's Billion Dollar Milestone Matters
  - DeFi Pulse Stats
  - Tether Collateralization
  - MakerDAO Lawsuit
- Bitcoin Talk Forum: Online Heroin Store
- E-Gold Founder Exposé
- EOS' Proof-of-Stake Vulnerabilities
- Lightning Network Vulnerabilities
- nChain Patents
- BSV Businesses/Tools
  - Teranode
  - Xoken Labs: Bitcoin's Scalability
  - EHR Data
  - Kronoverse
  - Planaria
  - Run
  - A.N.N.E.
  - Twetch
- Unbounded Capital Blogs
  - Why We Think Craig Wright is Satoshi, and Why That Matters
  - Own Your Data with BSV
  - Big Data is Dead, Long Live Big Data
- Warren Buffet on diversification
- Venture Capitalist Bearish on BSV

OTHER RESOURCES:

- Proof of Work vs Proof of Stake
- Jeremy Clark - History of Cryptocurrencies
- Bitcoin and Law
  - Why You Must Rethink FATF Now
- Videos
  - Block Size Debate
    - Roger Ver: Bitcoin Scaling Explained: Can Bitcoin Cash Scale on Today's Hardware?
    - Roger Ver Debates Charlie Lee - What is Bitcoin? (Pre BSV)
    - Roger Ver Debates Samson Mow - Can Bitcoin scale? (Pre BSV)
  - Lightning Network
    - How Lightning Network Scales For The World - Lightning Network Explained
  - Other
    - Bitcoin and Beyond Youtube Channel
      - Connor Murray: Bitcoin and Graph Theory
    - Isaac Morehouse: Big Block Bitcoin Series
    - Ryan Charles: Bitcoin is Turing-Complete in Three Different Ways

ACKNOWLEDGEMENTS

We would like to thank:

- Tommy Angelo, Sasha Bayan, Rich Belsky, Michelle Cahn, Ryan X Charles, Aymard Dudok De Wit, David Ernst, Evan Feng, Brenton Gunning, David Lambert, Mike and Sara Laskey, Jane Lippencott, Daniel Lipshitz, Isaac Morehouse, Mark Mullen-Muhr, Kevin Pham, Susan Resnick, Dori Rutkevitz, and Chris Shepherd for reading and providing valuable feedback prior to publishing.
- Ryan X Charles, Aymard Dudok De Wit, Daniel Lipshitz, Isaac Morehouse, and Kevin Pham for generously providing reviews.
- Lead advisor Mike Hennessey and core team members Zach Resnick and Avery Walston, for your support throughout the process that made this book possible. From the initial years of research and relearning about bitcoin that culminated in our fund's thesis to the recent months of constant assistance with the book's outlining, writing, and editing processes, you have been invaluable at every stage.
- The additional Unbounded Capital team members and advisors for your contributions to the research, writing, and editing processes.
- All of our LPs for believing in us and investing in our vision of Bitcoin.
- Dan Silverberg for clipping out and sending his grandson, Jackson, the Forbes exposé on Multicoin Capital which inspired us to think about our divergence and write this piece.
- Peter O'Neill for designing the book cover.
- Michelle Cahn for help with graphics and marketing.
- Lorie DeWorken for designing the pages and laying out the book.
- Chase Kuesel for editing the entire book (and staying up until 3 am to do so!)

ABOUT THE AUTHORS

JACKSON LASKEY is a partner at Unbounded Capital. As a former professional poker player/educator, a software developer, and a professional jazz pianist, Jackson is the beneficiary of a rather non-traditional background for a professional investor. Had Jackson, and by extension Unbounded Capital, come from a background similar to his investing peers, he likely would have stuck with the crypto consensus views and missed the potential of BSV as so many others have.

As a poker player and as a jazz musician, Jackson was forced to learn how to think beyond the readily available resources to establish a unique point of view to stay a step ahead of his peers. With this skill set, the risk management abilities requisite of any professional poker player, and strong computer science fundamentals, Jackson emerged well prepared to take on the challenge of investing in the rapidly changing world of Bitcoin investing with its unbounded opportunity and misinformation pitfalls. Jackson looks forward to continuing to learn about Bitcoin and helping to steer Unbounded Capital into a premier position in the future built on Bitcoin.

DAVE MULLEN-MUHR is a partner at Unbounded Capital, entrepreneur, writer, and ever-curious learner. After completing a degree in Economics from the University of Michigan, Dave worked on a series of projects and recognized the fundamental disconnect between academic economics and their practical applications. This discovery, in conjunction with his natural penchant for asking “why?”, shifted his focus towards heterodox subjects including Austrian economics, complexity theory, and sensemaking. These finally culminated in his passion for Bitcoin. At Unbounded Capital, Dave is focused on leveraging Bitcoin to integrate the wisdom of the past with the technology of the present to innovate the future.