FAMILY

OUR FUTURE IN CYBERSPACE

The Family Corporation

Contents

Contents **2**

1 Introduction **7**

2 The elephant in the room **9**

3 Crypto **12**
3.1 Public ledgers 12
3.2 Cryptocurrencies 14
3.3 The Real Role of Distributed Consensus 15

4 Anarchy and Decentralization Theater **19**
4.1 Crypto Anarchism 19
4.2 Decentralization theater 22
4.3 America's Founding Fathers 24

5 The many things decentralization can't do **27**

5.1 The Fee Price Floor Problem 27
5.2 The Read Write Asymmetry problem 28
5.3 The Forkability Problem 29
5.4 Conclusion 30

6 Time, Space and Cyberspace 31

7 Liberty does not produce liberty 33

8 Culture 36

9 Information Dissemination Networks 39
9.1 Distribution 40
9.2 Impediments to Distribution in Cyberspace . . . 40
9.3 Why Traditional Players Can't Solve These Problems 43

10 Identity and Sovereignty 45
10.1 Individual Non-Sovereignty 47

11 Sovereignty not decentralization 49

12 Cybercorporations 51
12.1 Problems and solutions 52
12.2 Potential objections 56
12.3 Advantages 58
12.4 Cybercorporation model vs Web 3.0 60

13 The Fediverse 62

14 Bitcoin maximalism **65**

15 In defense of Satoshi **67**

16 Why a corporation? **69**

17 Censorship in name of "censorship resistance" **72**

18 Moral agnosticism **79**

19 Zawinski's Law of Centralization **83**

20 You'll have no apps, and you'll be happy **85**

21 Outro **91**

"The unity of government which constitutes you one people is also now dear to you. It is justly so, for it is a main pillar in the edifice of your real independence, the support of your tranquility at home, your peace abroad; of your safety; of your prosperity; of that very liberty which you so highly prize."

– George Washington

PREFACE

This is may be the most important book of this decade. You are free to share it with your friends. We encourage you to do so. You are also free to reproduce sections of this book as you please. It is imperative that these ideas be spread far and wide.

But first, read it carefully! The format of this book may be unique. We will spend as much time on introducing new ideas, as we will on defeating old ones that have lead us astray. We'll discuss quite a few topics. This is not an academic work. The goal is not intellectual self-aggrandizement. This was written by and for people who want to improve their lives, and want to do it *soon*. The information contained here has been carefully picked to enable any sufficiently dedicated layperson to understand and participate in this wealth creation endeavor.

Chapter 1

Introduction

As our lives are increasingly migrating to cyberspace, which some call *the Internet*, so do our concerns. Injustices and discomforts in cyberspace are as pressing as the more "traditional" ones. Improving our lives increasingly means improving our living conditions in cyberspace. Just a few years ago, the chronically-online may have been perceived as asocial shut-ins. Today, those who are *not* online are the odd ones. The average person is said to spend most of their waking hours on a digital device.

Many, if not most, agree a nearly total dominion over cyberspace by a few corporations is a big source of cyberspace injustice. But few agree on what should be done. Some want more government regulation. Some want less. But few can actually formulate what such corporations could be replaced with.

Crypto, in the most general sense, has been at the forefront of

creating hope for a better cyberspace. Bitcoin has done incredible things in digital finance. Many believe crypto can do the same for the rest of cyberspace and produce viable *replacements* for the tyrannical platforms we all use. But very little of that has materialized.

This book will explain what went wrong, and lay out a concrete plan of action. We will make important technical contributions, but the biggest contribution of this book shall be to our collective understanding. Before we tell you *what* to do, we want to tell you *why*.

We cannot improve our societies without active participation of the people. A well-informed populace is the foundation of every great society. Cyberspace is no exception. Our "mindware" is as important as the "software", and this "mindware" needs a major update.

We have accumulated centuries of expertise in building better societies. But in this new realm of cyberspace, we may find it hard to draw from past experiences. It is often implied, that since cyberspace relies on computer technology to exist, all cyberspace problems must be tech problems. It may seem one has to be an expert programmer to get involved. But cyberspace is not as foreign and otherworldly as it first appears. Many of the same principles apply. We'll try to connect the old with the new.

Many ideas in this book may go against "wisdom" of the crypto industry. It's not our intention to pick any fights, nor is it our intention to be "controversial". But when welfare of the people is threatened by bad ideas - no matter how popular - they deserve to be repudiated in the strongest possible manner.

Chapter 2

The elephant in the room

"It is too early for politicians to presume on our forgetting that the public good, the real welfare of the great body of the people, is the supreme object to be pursued; and that no form of government whatever has any other value than as it may be fitted for the attainment of this object. Were the plan of the convention adverse to the public happiness, my voice would be, Reject the plan. Were the Union itself inconsistent with the public happiness, it would be, Abolish the Union. In like manner, as far as the sovereignty of the States cannot be reconciled to the happiness of the people, the voice of every good citizen must be, Let the former be sacrificed to the latter. How far the sacrifice is necessary, has been shown. How far the unsacrificed residue will be endangered, is the question before us."

– James Madison, Federalist 45

Perhaps the crypto industry should be called the liberty industry. These projects, whatever their technical substance may be, promise to bring more liberty (and thus prosperity) to the people. The technical properties or "features", such platforms may boast, are means to that end. When such means fail to achieve the desired end, they lose their claim to usefulness.

Many crypto projects produce a document - usually called a "whitepaper" - that looks much like a work of science or mathematics. It usually purports to "prove", or at least provide evidence for, some desirable property about a given system's design. The prestige of mathematical formalisms or supposed scientific rigor, blinds many to the usual failure to address the **elephant in the room** - will it increase our liberty or will it not? Will it make us more prosperous or will it not? Such "proofs", about a bunch of whatever, are useless if they cannot establish a link between their supposed invention and real world consequences.

Bitcoin has given us a little bit more financial freedom. If you have a lot of money and you're worried about an evil government stealing it, you now have more freedom thanks to Bitcoin. But few people have that problem - and they're usually not good people. People aren't excited about cryptocurrencies because they all have millions of dollars they need to hide from the government. They're excited because they hope what Bitcoin did to finance, can be done to other industries. This is the promise of crypto. Hence any elaborations on Bitcoin, better cryptocurrencies, are assumed to have the potential to achieve that goal. But despite billions of dollars flowing into the space,

it's not obvious if we've improved that much on the original Bitcoin.

Many cryptos claim to enable "censorship resistance". Is the world any less censorious than it was before crypto?

Many cryptos claim "decentralization" is a check on tyrannical power. Is there any less tyranny around the world?

The elephant in the room must be addressed. How do we solve the real problem we're trying to solve?

Chapter 3

Crypto

Much of this book will have to do with crypto. There's no doubt - it's a confusing subject. Even the word "crypto" is confusing. Do we mean cryptography? Cryptocurrencies? We mean a little bit of both, and a little bit of neither! Much of what is out there on the Internet, confuses the general idea with specific implementations. Some of it is downright wrong.

We'll try to provide better explanations. But even if they're not better - at the very least - they will clarify what we mean by certain terms later on in the book. Too often people disagree simply because they misunderstand each other.

3.1 Public ledgers

A fundamental building block of every crypto platform is a **public ledger**. Essentially every well-designed public ledger *is* going to be a blockchain. But "blockchain" implies the implementation, not the *idea*. Every book *is* a "string of words",

but it's easier to talk about just "books". To understand what a public ledger is, consider this example:

Let's imagine we're creating a simple application in which users can vote on a proposal. The question may be: *"Do you want to eat pizza today?"*. A user can answer *"yes"* or *"no"*. When a user votes we store their vote in a database. Such a record may contain the username, the answer ("yes" or "no"), and perhaps the identifier of the question being asked. But even if we give the world full read access to that database, there is no way to verify these votes. Our database simply says so. Whoever has write access, can put anything they want in this database.

The user logs in with a password, we give them a token, and when they vote they show us this token to prove they're who they are. If our server is not compromised, and we're the only person maintaining this service, we, the admin, can be reasonably sure the data is authentic. But we cannot prove it to the world. As our service grows we'll have to hire people to help us. Inevitably, multiple individuals will have access to our servers. Eventually, even we ourselves, won't be sure everything's okay. Nobody will be.

This is where public-key cryptography comes in. Instead of authenticating a user session with a password, we can authenticate transactions themselves with a cryptographic signature. In our voting app example, in addition to storing the username, the answer and the question id, we'd also store a cryptographic signature attesting the vote. The user account, instead of having a password, would have an associated public key. Anybody could now verify if these votes are indeed signed

by the appropriate key. Only the user has the private key that allows them to produce a valid signature. It doesn't matter if our servers are compromised. Either there is a valid signature or there isn't.

What happens if a user votes twice? Let's say a user votes "no", but then they vote "yes". We probably don't want to count both votes. But should we count the earlier "no" vote, or perhaps the more recent "yes" vote? In a classical system, the server would decide for us. But if we want everybody to be able to verify the data, we need to agree on how it's *interpreted*. We could decide only the first vote counts. If the server sends us data that doesn't follow the rules, we'll just discard the invalid data.

Therefore public ledgers are really *public data*, *public rules* and *public-key cryptography*.

There are still a few ways the server could mess with us in this scenario. For simplicity. we will ignore these problems for now. But even with a few flaws, there's no question this system is infinitely more secure than the one we started with.

3.2 Cryptocurrencies

Bitcoin utilizes a public ledger to create a digital currency. We can think of it as a digital bank in which every public key is an account. To spend an account's balance one has to sign a check, or "transaction", with the corresponding private key. All transactions and balances in this bank are stored in a public ledger. This bank cannot steal your money because it would need to forge a transaction signature. Public-key cryptography makes

it impossible. Similarly, the rules of this ledger stop this bank from over-provisioning money ala fractional reserve banking. The sum of all balances is strictly capped at 21 million. Balances are public. Everyone can verify whether or not the sum of all balances exceeds the specified limit. You cannot get away with "creative accounting" under this scheme.

Again, this is *not* an accurate description of Bitcoin's implementation. For example, there is no concept of "accounts" or "balances" in Bitcoin, there are only UTXOs, which are tricky to explain. But it's a decent high-level overview of what Bitcoin is.

3.3 The Real Role of Distributed Consensus

Now we're entering the *danger zone*. Distributed consensus. There is no Bitcoin server. Satoshi came up with a fairly elaborate scheme, for how Bitcoin's public ledger can be written to (appending new data) without a trusted third party. In a purely technological sense, this may have been Satoshi's most impressive feat. All previous distributed consensus schemes were hopelessly broken.

We've already described Bitcoin. Our description so far did not mention distributed consensus. What's the point? Well, Satoshi was afraid of the government. There are 195 countries in this world. There are many different banking laws. Some very restrictive. Some assert global jurisdiction. Even if this digital bank is perfectly legal in your country, somebody, somewhere may have a problem with it. Chances are, despite the way he

spelled some words, Satoshi was an American. Post 9/11 America was famously unfriendly to financial innovators. Satoshi didn't have to be particularly forward-thinking to worry about this. He makes that very clear in one of his first emails about Bitcoin:

> *>[Lengthy exposition of vulnerability of a systm to use-of-force*
> *>monopolies ellided.]*
> *>*
> *>You will not find a solution to political problems in cryptography.*
>
> *Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years.*
>
> *Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.*
>
> *Satoshi*

The problem with "centrally controlled networks" wasn't that they didn't work. There was a regulatory problem. Governments could destroy them. In fact, most pre-Bitcoin digital currencies were shut down by the government - the US government specifically. Nowadays, there may be a certain degree of tolerance for digital currencies - many forgot about this backstory. But before Bitcoin, it wasn't a sign of paranoia to

believe the government would shut you down for working on a digital currency.

When talking about distributed consensus, you'll mostly hear about security. But the point of distributed consensus is not to fix a security issue. We talk about security when evaluating distributed consensus schemes because - by default - **they're a security nightmare**.

Distributing or "decentralizing" the system gives it regulatory resistance. Governments cannot keep shutting down 1000s of random computers around the world. A bad consensus scheme can *introduce* security issues, a good one simply doesn't have any. Satoshi's distributed consensus scheme is notable because it doesn't fall apart like most do.

A "centralized" system utilizing a public ledger is just as, if not more, secure (in a technological sense) than Bitcoin and every other distributed consensus based cryptocurrency. Certainly more secure than questionable schemes like proof-of-stake (PoS). Such a hypothetical "centralized" system is **better in every possible way, except regulatory risk**.

To best understand the unimportance of distributed consensus - consider what happens when it fails. The only notable attack against Proof-of-Work schemes is the "51% "attack in which one actor controls over 50% of the hashing power. One player determines "consensus".

Can they steal money? No, they cannot forge cryptographic signatures.

Can they erase data? For the most part - no, the ledger is public, people have copies.

There are only 2 viable things an attacker can do: execute a "double-spend", or discriminate in processing transactions - a denial of service attack. That's about it.

Satoshi understood that very well:

> *Even if a bad guy does overpower the network, it's not like he's instantly rich. All he can accomplish is to take back money he himself spent, like bouncing a check. To exploit it, he would have to buy something from a merchant, wait till it ships, then overpower the network and try to take his money back. I don't think he could make as much money trying to pull a carding scheme like that as he could by generating bitcoins. With a zombie farm that big, he could generate more bitcoins than everyone else combined.*

Such attacks are rather unlikely to do any long term damage to the network. Many major cryptocurrencies are, in fact, under constant 51% attack conditions - usually nothing ever happens.

The idea of a public ledger is so deceivingly simple, it may be hard to believe nobody came up with it before. Indeed, one can find many prior works that *seem* similar. But much like Da Vinci's "helicopter" design , they only look that way with the benefit of hindsight. The truth is, there has been no real public ledger system before Bitcoin. Satoshi invented digital public ledgers. It's not as if Satoshi's consensus mechanism was the "missing part". Satoshi gave us many "missing parts".

The idea that distributed consensus, in and of itself, is somehow a "feature", a virtue, beyond it's regulatory role, is **the foundational misconception** plaguing the world of crypto…

Chapter 4

Anarchy and Decentralization Theater

To understand where these misconceptions around distributed consensus are coming from, we should examine Bitcoin's and crypto's ideological roots. These people are no dummies - they're some of the smartest people of our time. It's not their lack of intelligence or lack of technical understanding, but their ideological preferences that bias them to love distributed consensus, or "decentralization", a little too much.

4.1 Crypto Anarchism

Long before Bitcoin, many "crypto anarchists" were trying to create a digital currency, or "e-cash". There's every reason to believe, Satoshi was directly inspired by "crypto anarchist" thought. At many points Satoshi references crypto anarchist works.

There are many kinds of anarchists. Socialist, communist, capitalist… You can go on and on. Crypto anarchism is yet another flavor. These groups may often dislike each other. For example, in *Crypto Anarchy and Virtual Communities*, Timothy May, often recognized as the father of crypto anarchism, specifically disavows some anarchist groups:

> *First, the "anarchy" here is not the anarchy of popular conception: lawlessness, disorder, chaos, and "anarchy." Nor is it the bomb-throwing anarchy of the 19th century "black" anarchists, usually associated with Russia and labor movements. Nor is it the "black flag" anarchy of anarcho-syndicalism and writers such as Proudhon. Rather, the anarchy being spoken of here is the anarchy of "absence of government" (literally, "an arch," without a chief or head).*

But just a few paragraphs before, he gives a more general definition of anarchy. It's pretty much in-line with the common sense understanding of the term:

> *"The Net is an anarchy." This truism is the core of crypto anarchy. No central control, no ruler, no leader (except by example, reputation), no "laws." No single nation controls the Net, no administrative body sets policy.*

Our goal here is not to morally evaluate different kinds of anarchism. The ***substance*** of anarchy is simple. Whether one imagines it will result in a capitalistic or communistic society shouldn't matter to us. Every anarchist will be opposed to the

idea of government. And as Timothy May specifies, it's not just governments - they also dislike *"central control"*, *"rules"* and *"leaders"*. It's fair to say every flavor of anarchism shares these beliefs.

Thus, it's not surprising distributed consensus is the part they love the most. Cryptography is a technical detail, it's fairly neutral ideologically. A public ledger outright goes *against* a lot of the early crypto anarchist ethos. Most of their pre-Bitcoin efforts focused on private currencies and privacy in cyberspace.

Distributed consensus in its "decentralization" is ideological opium to anarchists. Anarchism has always been derided as Utopian and unpragmatic. If they can make the case that "decentralization" is a technical necessity - not a moral imperative - for the first time, they can make a pragmatic case for anarchy.

That's exactly what they're doing - and they're winning. Crypto anarchists dropped the moralizing. Instead they present it as an inevitable and stable outcome of crypto systems' wide adoption. You may not like it, but this is what's going to happen. You don't have to "support" it, you just have to be smart enough to understand it. You don't have to be an "anarchist", you just have to be a technologist.

You'd probably never call yourself an "anarchist". But if you've been in crypto long enough - chances are - you've adopted some of their ideas as hard technical truths. They are not.

4.2 Decentralization theater

Instead of rallying against the government, crypto anarchists rally against "centralization". Instead of calling for anarchy, crypto anarchists call for "decentralization".

Like true anarchy, true decentralization is a pipe-dream. Even Satoshi's beautiful and ground-breaking scheme does not remove the fact that some individuals have more influence over Bitcoin than others. Most post-Bitcoin cryptocurrencies are even less "decentralized". But proponents of decentralization are often very uncomfortable about these facts. They like to go to great lengths to hide any "centralization" in their systems. We call this **"decentralization theater"**.

In decentralization theater world, crypto projects have a transcendent quality. They have no human creators. They work perfectly with no human intervention. "Centralization" is the ultimate evil and "decentralization" is the ultimate good. Forces of decentralization are at war with the evil world of centralized corporations trying to enslave humanity. Developers are prophets channeling divine decentralized insight into computer code.

Humans themselves are subsumed into a mechanistic mass that becomes one of the many cogs in a decentralist machine. Perfectly designed game theoretic incentives built into the system - not free will - drive human behavior. This magic of Darwinian spontaneous order results in a perpetual prosperity machine.

"Centralized" systems without this design are crude and

fundamentally insecure. You're supposed to associate them with the "central planning" of the Soviet Union, with totalitarianism and tyranny. Decentralized systems are supposed to be the free markets cyberspace.

But the truth is, decentralization theater simply transposed anarchistic hatred of governments onto "centralized" systems. Their seemingly compelling arguments against "centralized" systems fall apart in exactly the same way anarchistic arguments against the government do. Sooner or later, you find things that simply cannot work. What about the military? Police? Courts? Anarchists hate these questions because they cannot answer them.

Would Facebook do better if it had a 100 different clients or "front-ends"? Or does it make more sense to have just one? Decentralization tells you it's a tremendous idea. Ethereum points to 40 different clients/wallets on their website - all with vastly different user experiences. Common sense suggests something's not right.

Is it really so great to have no leaders? Or to have them, but pretend they don't exist? Would Amazon do better if Jeff Bezos owned just 5% and made some suggestions once in a while?

Can you simply launch a platform without any apps and hope 3rd party developers will do the job for you? Without any obvious profit incentive? How stupid was Zuckerberg to do all the hard work, instead of designing an social-media "protocol"?!

In fact, why have a company at all? Just open-source! People from all around the world will write the code. Decentralized software-dev. Perhaps we need more cooks in the kitchen?

4.3 America's Founding Fathers

Decentralists like to imply decentralized governments are somehow linked to liberty. Many agree America is probably the most liberty-loving country in the world. Not just loving, but unlike others, possessing or having possessed some semblance of liberty. How convenient would it be if America was decentralized in some way?! United States, right? States - that's decentralization?!

Should they read the Federalist Papers, they would be dismayed to learn the Constitution is essentially a **rejection of decentralism**. This masterclass in pragmatic political philosophy, in which some of America's founding fathers advocate for the yet to be ratified Constitution, is very much **one big argument against a decentralized America**. Those who opposed the Constitution were not totalitarians. They were no enemies of liberty. It was their supposed love for (but misunderstanding of) liberty that made them oppose the Constitution. They feared Constitution's stronger central government would result in tyranny.

The founders didn't have to waste any time convincing people that liberty was good. They had to go on offensive against those who professed to be greater lovers of liberty:

> *An enlightened zeal for the energy and efficiency of government will be stigmatized as the offspring of a temper fond of despotic power and hostile to the principles of liberty. An over-scrupulous jealousy of danger to the rights of the people, which is more commonly the fault of the head than*

of the heart, will be represented as mere pretense and artifice, the stale bait for popularity at the expense of the public good. It will be forgotten, on the one hand, that jealousy is the usual concomitant of love, and that the noble enthusiasm of liberty is apt to be infected with a spirit of narrow and illiberal distrust. On the other hand, it will be equally forgotten that the vigor of government is essential to the security of liberty; that, in the contemplation of a sound and well-informed judgment, their interest can never be separated; and that a dangerous ambition more often lurks behind the specious mask of zeal for the rights of the people than under the forbidden appearance of zeal for the firmness and efficiency of government. History will teach us that the former has been found a much more certain road to the introduction of despotism than the latter, and that of those men who have overturned the liberties of republics, the greatest number have begun their career by paying an obsequious court to the people; commencing demagogues, and ending tyrants.

They understood these bad ideas couldn't be defeated with a concise argument. If one has come to believe such an absurdity, simple logic will not suffice. So instead they went for breadth. They made sure to overwhelm with every possible example of the absurdities their opponents were effectively arguing for. Almost to the point of being boring. They only begin to discuss the actual virtues of the Constitution once they're done exposing anti-federalit fallacies.

Leave America divided into thirteen or, if you please, into three or four independent governments–what armies could they raise and pay–what fleets could they ever hope to have? If one was attacked, would the others fly to its succor, and spend their blood and money in its defense? Would there be no danger of their being flattered into neutrality by its specious promises, or seduced by a too great fondness for peace to decline hazarding their tranquillity and present safety for the sake of neighbors, of whom perhaps they have been jealous, and whose importance they are content to see diminished? Although such conduct would not be wise, it would, nevertheless, be natural. The history of the states of Greece, and of other countries, abounds with such instances, and it is not improbable that what has so often happened would, under similar circumstances, happen again.

It's a great question. They asked many such question. So shall we throughout this book. We will show you that "decentralization" doesn't just have a few flaws here and there. **It simply doesn't work and never will**.

Chapter 5

The many things decentralization can't do

The three problems described in this chapter are by no means the biggest. Or even the most interesting ones. User experience issues and organizational dysfunction are, for example, way more interesting. And we'll get back to them. But they can be derided as "opinionated" (they're not) or "soft" because one cannot "prove" them with simple logic. So we'll discuss three problems that are **serious**, **impossible to fix** and purely technical in nature.

5.1 The Fee Price Floor Problem

Transaction fees are a problem every crypto is struggling with. Ideally, transactions should be free. Many interesting, probably the most interesting, use cases are simply "priced-out". Many hope that expanding capacity or throughput is going to solve

this problem. But they're wrong. Unless that capacity expands to infinity, increasing throughput will never solve this problem in a decentralized system. There is no such transaction price, that is cheap enough for legitimate users, but expensive enough to deter spammers and abusers. Any capacity below a certain price, without some form of discrimination, will get filled for totally useless or malicious purposes until it's expensive enough, at which point we'll be back to square one. There is no solution to this problem given the constraint of permissionless access that a decentralized network requires.

The only solution is to throttle those who abuse the service, which cannot be done in a decentralized system.

5.2 The Read Write Asymmetry problem

Consider another similar problem: Mining and other such schemes coordinate "writes" to a public ledger. They may ensure there is no discrimination in adding data to the system. But there is no corresponding mechanism on the "read" side. There is no way to ensure one can always retrieve the data. This problem seems irrelevant when most ledgers are so slow they cannot store significant amounts of data. When everybody can just download the whole thing themselves, it's not a real problem. But when throughput expands to the levels necessary to operate the most basic Internet services, the amount of data will become too big to be served for free out of sheer charity. Ethereum, even with it's poor scalability, is already starting to approach this point of no return. Nearly all "reads" in the Ethereum world are handled by

Infura - most reads in Ethereum already depend on this trusted 3rd party. **There is no solution to this problem.**

The obvious objection that a "centralized" system has the same problem on a technical level is an absurd tautology. A central entity has the same *technical* lack of a mechanism to ensure fairness in reads. However, it is obvious it has more real reasons to be fair. When there's one entity, its unfairness reflects on the entire platform. Such an entity stands to lose from its discrimination. In a decentralized system there is no moral or practical imperative to be fair in "reads". The centralized system is better.

5.3 The Forkability Problem

Forkability is a key feature of public ledgers. Whenever something goes wrong with the system, it can always be rolled back and "restarted" from a point in time when the system state wasn't compromised. For example, imagine that cryptocurrency developers planted a backdoor allowing them to create coins out of thin air. If they tried to exploit this backdoor, sooner or later the people would realize, fix the bug and do a fork without their ill gotten gains. In a very simple decentralized system that has only one feature, say Bitcoin, there's no major problem with forkability. But when you use a public ledger to do many different things, decentralization starts to work *against* forkability.

For example: consider what it would take to fork Ethereum. You can readily copy its public ledger. But you cannot copy much of its decentralized ecosystem. Most so called "dApps" would

break in your fork. They rely on their own infrastructure, servers and domains. These would not carry over to your fork. You fork would also have no RPC servers like Infura that Ethereum relies so heavily on. Or consider tokens like USDT. If you fork Bitcoin, perhaps your Bitcoin will be worth some fraction of the original Bitcoin. A forked USDT can only be worth $1 or $0. It's simply technically impossible to fork Ethereum the way you can fork Bitcoin. But it doesn't mean Bitcoin is better, it simply does less. A Bitcoin-based "Web 3.0" would be just as unforkable.

If all Ethereum services were operated by one entity it would be easier to fork. It may be hard to imagine this now, but don't worry, we'll discuss this later.

5.4 Conclusion

The decentralist gambit is to always compare "centralized" systems *without* a public ledger, to "decentralized" systems with a public ledger, and then claim all the obvious benefits of public ledgers as benefits of decentralization. But when we compare apples to apples, decentralization, almost universally, loses to centralized systems on technical merits. Every desirable property of crypto is thanks to public ledgers - not decentralization.

Chapter 6

Time, Space and Cyberspace

When talking about "cyberspace", We're not talking about 3d virtual worlds of the "metaverse". Cyberspace is not in any way separate from the so-called "real world". Cyberspace is the human informational realm. Much of human existence has always been a combination of both the informational and the material. Before the Internet and modern media, perhaps we'd read books, read letters or simply talk to people. But before the Internet, these informational activities were constrained by the material world - they were part of it. What the Internet did, is it freed the informational from the material - thus "cyberspace" was born.

One of the most persistent trends in the progress of human economies has been the annihilation of time and space. Trains, cars, airplanes and other means of physical transport have compressed time and space considerably by making it easier to travel vast distances in less time. This has allowed economies to expand by leaps and bounds allowing for trade arrangements

that were not possible before.

Because the material and informational realms used to be interdependent, these developments in transportation technology affected both. The economic growth they produced was a result of improvements to both realms. But now, that the informational happens almost exclusively in cyberspace, physical transport cannot possibly do much to facilitate transmission of information.

Nowadays improvements to transmission of information have to be cyberspace technologies. These are Internet platforms like Amazon, Facebook, Google and others. They make it easier to reach and deliver information in cyberspace.

These Internet platforms did as much to grow our economies as have previous transportation technologies.

Chapter 7

Liberty does not produce liberty

If you want something - you don't have it. If you want to have it - you have to find a way. You need to learn. That's how you grow your personal wealth. By learning. The economy grows when people learn. Accumulation of knowledge is accumulation of wealth.

That's hardly a controversial thing to say. But much of economics is busy pretending it's worthwhile to apply the materialist outlook of physics to our human societies. You'll never hear about learning. You'll never hear about hard work. You'll never hear about anything that actually produces results. As if at some level, humans stop being free-willed individuals and become inanimate matter that can be perfectly predicted with an equation.

Cyberspace is the ultimate realm of human free will. There is no matter, only information. Only information *created* by humans. There is nothing else. Even if the materialistic delusion

may otherwise seem intuitive, it's completely indefensible in cyberspace.

Claude Shannon's information theory tells us that information is surprise. It's something we did not expect. Information is unpredictable. If the channel is unpredictable itself, there's no way to distinguish between information and noise. A good communication channel is perfectly predictable and boring.

Economic growth - expansion of knowledge - cannot possibly be generated by a mechanistic model. It's fundamentally unpredictable. We can only "predict", or rather *know* about, the things that *prevent* economic growth.

The underlying informational network of the economy must be stable. A chaotic environment cannot possibly breed innovation. We cannot predict inventions. We can only create an environment that doesn't stop them from happening.

The idea of spontaneous order, the linchpin of decentralism, predicts a specific invention. It doesn't state that *some* government or *some* order of things will "emerge" - everybody agrees with that. It predicts an order with some specific and desirable qualities will emerge. Yet they cannot define it - it will "emerge" spontaneously. This is exactly what they're promising us in cyberspace. They don't know how it's going to work, but they somehow know, decentralization will replace Big Tech with something better. That's a big claim.

The idea of a small and stable government doesn't have this problem. It doesn't try to predict the unpredictable. It simply tries to increase the likelihood of *some* innovation happening by providing enough stability. We don't know and don't care what

this innovation may be.

Under perfect circumstances, a microwave link will always be faster than fiber optic. Totally unrestrained, the signal can travel at nearly the speed of light from point to point in a straight line. It wouldn't be inaccurate to say, the signal in a fiber optic cable is "restrained" by its enclosure and more convoluted path. Yet, a reasonable person understands this is what makes fiber optic cables more reliable for large scale deployments.

In the same vein, one can cite examples of how basic rules of societal order can restrain liberty. But a reasonable person has to concede that some base level of order is a prerequisite for liberty to flourish. It is a logical contradiction for that order to be an "emergent" result of liberty itself. It has to be imposed.

Liberty does not produce liberty. Good people have to produce and safeguard liberty. We have to *act*.

In the traditional world you need rule of law. A stable government. An able military to defend against threats. So on and so forth.... These things don't simply emerge out of nowhere - they have to be created and maintained. Cyberspace is no different. There are many basic things that don't simply take care of themselves.

Chapter 8

Culture

When you have a decent communication channel, you will not see big gains in the physical layer. Modern information transmission technology utilizes elaborate encoding schemes. If you examined the radio signal coming out of your phone. it would look like total noise. Without the software, you couldn't make sense of it.

Humans are not as sophisticated at encoding. But we do have some obvious encoding schemes - language and culture. Without a common language our inter-human informational bandwidth grinds to a halt.

Tower of Babel perfectly illustrates the importance of language in determining our productive capacity. To stop humans from completing a misguided construction project, they were all made to speak different languages:

> *6 And the Lord said, "Lo! they are one people, they all have one language, and this is what they have commenced to do. Now, will it not be withheld from them, all that they have planned to do?*
>
> *7 Come, let us descend and confuse their language, so that one will not understand the language of his companion.*

The European Union serves as a present-day example. With 447 million people (before Brexit), around 110 million more than the United States, its economy is still significantly smaller. EU's economy is approximately 70% of America's size. The richest sizable constituent states of the EU would be poor, or at best average, states of the US. Its greatest cities are rather unspectacular. It dominates in almost no industry. It depends on the United States for military protection. The EU creates very little knowledge. The markets and borders are open, a Frenchman can readily go and start a business in Berlin. But it never happens. EU may have a decent physical link layer, but without a common language it cannot be utilized. The European Single Market only applies to material goods - the least important part.

Many who rightfully criticize the EU, are way off base in calling it "centralized". There is no strong central EU government.

There is no EU military. There is no unified foreign policy. The growth of the EU bureaucracy did not result in smaller governments across individual EU states. It's exactly the kind of "design" you get when you don't do any design. There is no overarching idea behind the EU. It's a creation of pure chaos and happenstance - it's exactly the kind of "spontaneous order" decentralization breeds. Should the EU disintegrate with the same spontaneity, rather than via application of *intelligence*, one shouldn't expect any increase in prosperity or liberty.

Chapter 9

Information Dissemination Networks

Social networks are probably the most important, yet most misunderstood, technology of the 21st century. Much has been written about their supposed negative externalities. You will hear about addiction, depression, disruption of the democratic process and so forth. But you will not hear much good said about them.

So why do they exist? How can a social media company be one of the most valuable companies in the world? Haters think they simply get people addicted and sell them to advertisers. But when you understand that these simply are the information dissemination networks of cyberspace, there's nothing strange about them making a lot of money. They're probably generating an order of magnitude more wealth for our economies. There's also no reason to make much of a distinction between "social

media" and other kinds of Internet platforms. Google, Facebook and Amazon are essentially in the same business of transporting information.

Many hate these so-called "Big Tech" companies because of the seemingly tyrannical things they do. Decentralists often claim it's their centralized nature that allows them to be "evil". As you'll soon understand, this is completely false.

9.1 Distribution

Distribution is the lifeblood of every business. Your product cannot create value without reaching customers. It needs distribution.

"Annihilating the time and space" is such an important theme because it means better distribution. Without sea freights many parts of the traditional economy would grind to a halt. Without information dissemination networks the informational cybereconomy would grind to a halt too.

Perfect distribution for physical goods would mean the ability to teleport any object to any location at will. Perfect distribution of information would mean the ability for humans to instantly transmit any information to anybody else at will.

We're far from perfect in either case. There's a lot of room for improvement.

9.2 Impediments to Distribution in Cyberspace

Information dissemination networks like Facebook, Linkedin, Alibaba, Twitter, Paypal and many others are the current state

of art. They boast massive userbases and make it simple to communicate with other users of these platforms. But they are very far from being perfect information networks. Let's define a few criteria that can help us evaluate them:

1. narrowness: These systems are thematically narrow in the kinds of information they transmit. Twitter may allow you to distribute political information, Linkedin might not. Alibaba may allow you to buy and sell pharmaceutical materials, Facebook probably won't. Paypal lets you transmit money, Twitter does not.

2. stability: Current networks aren't stable. If there are any, APIs can and do change arbitrarily. Terms of service are unclear and ever-changing. Users don't understand why they've been terminated. In that sense they are far behind their physical counterparts. No business worries about not being able to use sea freights tomorrow. In cyberspace, a business cannot rely on Facebook to reach its customers. All business recognize the power and convenience of social media. But how many businesses have given up on email, phones and websites?

3. direct access, switching costs: If you don't like your logistics provider you can find another one. In cyberspace this if often impossible. Information networks don't just transmit information, they "own" their users. If your customer is only on Facebook, you cannot reach them via another channel.

Very few businesses maintain their own logistics operations. Physical distribution infrastructure isn't perfect, but for most businesses it's good enough. They can readily rely on external infrastructure.

In the informational economy of the cyberspace, information distribution is everybody's core competency. Businesses have to maintain their own information distribution channels. Email infrastructure, mailing lists, websites, servers, lists of physical addresses and so forth.

Most small businesses and startups are not equipped to maintain this infrastructure. Every business suffers as a result.

For example, let's say you create a Facebook app to represent your retail store, you won't have to maintain your own website. The integration with Facebook will provide you with a natural, native distribution channel. Your Facebook page will be your website, Facebook followers will be your customer list, Facebook messenger will be your support line. You can just focus on your business instead of maintaining tech infrastructure of your own.

But everybody knows not to do that - your business can go bankrupt overnight.

It is therefore self-evident current-gen information networks are still in their infancy. Cars have replaced horses, nobody rides a horse anymore. Social networks did not replace old-gen cyberspace infrastructure, companies still maintain websites, email and other such things.

9.3 Why Traditional Players Can't Solve These Problems

Let's go though the same criteria and consider why current players cannot improve on them:

1. narrowness: All notable information dissemination systems are operated by non-sovereign legal entities (corporations). They're subject to myriad of rules and regulations from multiple jurisdictions around the world. Big corporations cannot arbitrarily introduce new features without facing legal scrutiny. When Facebook tried to introduce its own cryptocurrency, Libra, many regulators around the world said "no" - the plan had to be scrapped. A general purpose information dissemination network is virtually impossible legally. Only a thematically narrow information network can manage legal issues.

2. stability: The stability problem is also in large part a result of the regulatory environment. What's legal today may become problematic tomorrow. Tech companies have to be smart about navigating regulatory risk. This often means sacrificing the utility of the network to mitigate regulatory risk.

3. direct access, switching costs: The business models of all current networks fundamentally depend on limiting 3rd party access to their userbases. Their revenue streams, like advertising, depend on having exclusive and privileged

access to their userbases. Without this there is no business. Unmitigated access is also a regulatory nightmare.

It should be self-evident the biggest problem is regulatory. Very few issues have to do with malice or incompetence. We can't solve them by simply creating a better product operated by the usual Delaware corporation.

Utilizing public ledgers would solve every single one of these problems almost entirely. But they *cannot be* utilized for the very reason these problems exist! One cannot serve two masters - the order of public ledgers competes with the order of traditional jurisdictions. As much as these "Big Tech" platforms may appear government-like, the very problem is they're not real governments. They *should* enforce their own order - but they cannot. Neither can traditional governments since political boundaries don't overlap with cyberspace boundaries in a logical way. Nobody can enforce order. Disorder is guaranteed.

When Facebook tried to launch its own cryptocurrency, Libra, governments told Facebook they shouldn't even try. Telegram went through a similar ordeal.

Chapter 10

Identity and Sovereignty

Every human being has a natural identity. In fact every living being and even inanimate matter can be said to have an identity. We can observe a thing and then observe it again and know it is still the same thing. We may make errors. Say, there are 2 identical quarters: A to the left and B to the right. You close your eyes and have someone shuffle them around. You open your eyes again and there may be no obvious way to tell which one is A and which one is B. Such a distinction may not even seem to have any practical purpose. The coins are truly identical. What do we care?! Nonetheless, nearly everybody would recognize that they are distinct coins, they have separate identities.

We have almost no control over that natural identity. We cannot transfer it. We cannot destroy it. Nobody can take it from us. We may be able to make others believe we are now a different thing. However this is hard and would almost universally be considered immoral, in some cases criminal fraud. This identity

may be "ours", but it's certainly not our property.

Our legal personhood usually, in spirit, closely mirrors that natural identity. However it does diverge in some ways. We may have a legal name, but we may be able to change that name. We may have a state-issued ID number, it may also be mutable. This identity could now be revoked by the issuer. Others may have an easier time impersonating us. Somebody could know our legal identity but they may not recognize us in-person. Legal identity appears to be more flexible, but our control over it is also less certain. If we don't own our natural identity, we certainly don't own this one. In matters of commerce this synthetic identity is probably more useful than our natural one though.

Before public-key cryptography, identity in cyberspace has been a tough problem. Websites had no natural way to determine identity. When two network requests are sent to a server, it's not obvious how to determine whether they're the same natural person or even the same device! Much like states issue ID cards, websites had to issue their own form of identities. Usually it's an "account" secured by a "password". Each time you give a website this same password they know there's some sameness about you. This identity is not strictly linked to our natural identity. We can transfer it simply by giving someone the password. We may have many of them. It may allow for a lot of mutability. It can be deleted by the party that issued it. We can readily be impersonated by that issuer. Yet again, we do not own this identity.

Public-key cryptography changed everything. By generating a private-public key pair we issue an identity to ourselves. By

sharing our public key and utilizing cryptographic signatures we can establish an identity that is demonstrable to others. We can transfer it. We may not mutate it. We can have many of them. We cannot be readily impersonated by others. Nor can others delete this identity. Finally, we have an identity that we do own. It is our property.

Much like our legal personhood extends our natural identity, we can also build on top of this cryptographic identity to give it new properties. An entity can assign it a name, a unique number, a picture and so forth. We can combine multiple cryptographic identities to form one logical identity (multisig). We can do all of that without giving up on the ownership property. A 3rd party gains no control over our identity.

10.1 Individual Non-Sovereignty

We are born with some natural sovereignty. We have free will. We can attempt to do whatever we want. However, practical considerations force us to waive it by pooling this sovereignty with others to enjoy fruits of civilization. It is very hard to meet our most basic physiological needs without relying on society. There may be different societies around the world, but we have very little freedom in picking them. Even less freedom in trying to form a new one.

In cyberspace this natural sovereignty extends further. We're not forced into any kind of a society by default. Now we can choose which civilization to join. If we don't like any we can create a new one. At any time we can change our mind. As a

result, we owe less to societies and they owe us less too.

We have more choice, but we cannot not make one. All the good stuff will happen when people work together - as it always has. Cyberspace is no different in that respect. What's different, is that it's easier than ever to assert sovereignty and create better societies. You don't need a powerful military anymore. In the informational realm, you only need powerful minds.

Chapter 11

Sovereignty not decentralization

As much as decentralization appears to mitigate the regulatory issue, as we've discussed, it destroys everything else. It may allow us to utilize public ledgers to enforce some order, but it breeds all kinds of new disorder! We must do something else.

The solution is *sovereignty*, not decentralization. Instead of replacing viable organizational structures with Utopian pipe-dreams, we must insulate them against external threats. In decentralized systems every participant distrusts every other participant. The system must be secured against every threat - both internal and external. In the system we're proposing, so as long the system can defend itself against external threats, there is no real threat internally. Without external pressure and without distributed consensus, a public ledger is enough to ensure internal security.

To be sovereign is to not depend on others. It's to have organizational free will. We should do things because we want to do these things. Not because somebody told us to. Sovereignty may be won, but it must be defended. It is our duty to maintain it.

The first rule of sovereignty is - never concede it, not an inch. We are free people. We have an inalienable right to self-determination. Some may try to illegally and immorally impose their will on us, but they shall never have the moral mandate to do so. Simply knowing that is a very important first step.

Of course, conviction is not enough - we need real security. No country in the world has a perfect defense strategy. It's a never-ending cat and mouse game. In fact, it's never a good idea to put all your cards on the table. But in the next chapter we'll describe the basic idea well-enough to show you that it's not only workable to assert cyber sovereignty, but infinitely superior to the strategies offered by decentralists.

Chapter 12

Cybercorporations

What we're proposing is the "cybercorporation" model. Don't take the word "corporation" too seriously. You could call it many different things. You could say just "cyberorganization". Maybe even "cybergovernment". But ultimately it shares many design features with corporations, and perhaps it's a good way to weed out those who hate corporations a little too much.

A cybercorporation has a board. It has owners. It has a profit motive to some extent. It creates and maintains platforms, products and services. But instead of relying on legal systems of other sovereigns, a cybercorporation - with help from the people - maintains its own security and its own legal order. It will utilize public ledgers in much the same way most cryptos do, except without too much distributed consensus. The people will not have to worry too much about the cybercorporation violating their rights.

12.1 Problems and solutions

We'll go through some of the main design elements by considering possible problems and solutions.

Continuity

The main problem with a "central" entity is *continuity*. If the board disappears for whatever reason the system must recover. We cannot stake everything on a few people doing everything right. Every sovereign in the world has a way of rotating leadership - we have to have that too.

We'll use a layered ledger design. The first layer will be the cybercorporation ledger. It has one purpose - to define the current state of the cybercorporation. A cybercorporation's board is simply a list of public keys. This layer is tiny. Every client will have a complete copy. This layer may be called decentralized, but only a transaction signed by the current board itself or the incoming contingency board (more on that later) will be considered valid. No central party will be coordinating writes to this ledger, but the writes themselves will inevitably come from the 2 possible central parties.

The second layer will be used for core features. Writes to this layer must be valid transactions signed by both the user and the cybercorporation. Hence, you need the first layer to validate the second layer.

The board will have to write something to the cybercorp ledger every liveliness period (say 30 days) to remain a valid board. If it fails to do so, it becomes an absentee board. A *contingency board*

will then replace the *absentee board*. The initial liveliness period for the contingency board will be much shorter, say only 7 days. If they become active within this period they become a regular board. Otherwise, the process repeats.

If the board specified a replacement, it will be given the first preference. Otherwise, a *contingency board* shall be the 3 largest Coins holders. Then the next 3 and so on.

We'll discuss continuity more later, other parts of design consider continuity, but this tackles it directly. If the board happens to be in one room (they never should be!) and a bomb goes off - the people will mourn - but they'll be just fine! Presumably this will stop our enemies from ever trying to assassinate the board. But if they do, we're going to be just fine.

Technological attacks

We'll adopt the "mega-app" model. That is - everything will be accessible from a single standalone application. Unlike the "decentralized web" you will not interact with a 100 different websites - just one app. Obviously this is simply good design, that's how all sane non-decentralist platforms work. But what may not be obvious is that it has tremendous security implications. Our application can use its own networking stack, which unlike website based apps, will not be vulnerable to a whole class of attacks. We will not use DNS, certificate authorities, trusted 3rd parties (like Infura) and other potential single points of failure. We'll use a judicious amount of permissioned pseudo-decentralization for some networking functions - the app will be able to reach cybercorp infrastructure

without relying on any single points of failure beyond our control. Those users who opt-in will also be able to themselves serve as parts of the cybercorp infrastructure.

This combines the operational efficiency of a centralized system, with the sovereignty benefits of decentralization.

Disruptions, cheating and continuity cont.

All functionalities that don't strictly require central coordination, should support two modes of operation - the efficient and convenient "central" implementation and a peer-to-peer (p2p) fallback. For example, when participants already know each others' public keys, they can communicate without any central coordination at all. This may seem strange and trivial - it's not - it has many important properties.

First, should something happen to the cybercorporation, the platform will be able to function in a degraded mode - enough to recover and reestablish full order. As we've discussed, there may be a period in which we're trying to pick a new board. This may not happen quickly. It's important that the platform continues to work when that happens.

Second, it's an additional deterrent (public ledgers are already a big one) against any cheating by the cybercorporation. Whatever it does, it cannot stop people from talking.

Third, it also helps when disruptions unrelated to continuity occur. For example: should a massive DDoS attack be successful, it will lessen the impact.

Financing, ownership

Since we're not pretending nobody's in charge, we cannot pretend we don't need money to keep running the network. Decentralists pretend you only need to pay miners (or witnesses). Development needs to be financed. Basic operations need to be financed. Staff needs to be maintained. You need a non-trivial amount of money. Many cryptos generate a lot of money for their insiders, but the platform itself rarely benefits from that money.

Coins, our cryptocurrency component shall be dual use. They will be a currency - but they will also be tokens of ownership. You need over 50% of Coins, alone or pooled with others, to elect a new cybercorp board. Most Coins will be owned by the cybercorp itself. The cybercorp will be put on a very long vesting schedule. Hence for at least the next decade, and likely much longer, the cybercorp can essentially keep electing itself. But it can never simply take the money at one go. It can only spend it gradually. A good and honest cybercorp will use most of the funds to work on the platform (not for the personal benefit of its board members). But if it is corrupt, the people will have enough time to force it out via a fork and they likely won't have to make any controversial seizures. The new board will inherit all the unvested coins.

Social attacks

By having our own platform-native information network - and not using others - we can avoid most social attacks. For example,

you could easily destroy most crypto communities by simply banning their top people from information networks. They cannot ban us from our own.

12.2 Potential objections

Since we are likely to attract the ire of decentralists, some likely objections should be addressed in advance:

The most likely class of absurdist objections may have to do with some of the theoretical ways a cybercorporation may sabotage the network. For example, it *may* refuse to process nearly all transactions - but enough to not trigger the contingency replacement mechanism. It indeed *may* do that, but what circumstances could cause this to happen? What does the cybercorporation have to gain, while risking so much? What circumstances exactly will cause that to happen *and* stop the people from replacing the cybercorporation? Note that the p2p fallback will continue to work. The people will be able to freely discuss what's going on. Bitcoin miners could collude to keep mining empty blocks essentially DDoSing the network. Yet should we really care about this "vulnerability"? If that happens to Bitcoin it's game over. In our model the people would simply have to fork the cybercorp.

Some objections may mistakenly believe issues of badly designed distributed consensus schemes may apply to our system. For example, proof-of-stake systems have significant issues with chain reorganizations. In Bitcoin one simply accepts the chain with the most "work" as the valid one. Since mining is very

expensive, if you wait long enough, transaction finality is a near certainty. In a PoS system there's no "cost" associated with creating an alternative chain, various mitigations must be employed to prevent bad actors from exploiting this. It's not obvious if any of them truly work, in fact most ironically tend to be centralization in disguise. So one may claim our system has this problem too. If the cybercorporation is the consensus-maker, surely it can execute these malicious reorgs at will! But in a system without distributed consensus, there is no reason to allow for non-trivial reorgs at all. Reorgs must be accepted in a decentralized system because no party can be trusted to provide an authoritative record. If one entity creates the record why should it ever walk it back? There's no reason for clients to blindly accept reorgs. This problem simply doesn't exist.

Another seemingly reasonable objection, may be that under some circumstances the contingency rules may not work perfectly and a split may occur. That's true but it also doesn't matter all that much. First, let's acknowledge that every crypto platform has the continuity problem too. They just hate to acknowledge it. Even if our scheme cannot guarantee 100% leadership consensus at all times, it's still better than nothing. Second, board rotation by definition is not supposed to happen often. It's not as if it's something that will kick-in every week, month or even year. When it does happen it will inevitably attract a lot of attention. It's not such a big deal if people have to apply a little bit of common sense and make the determination themselves. The mechanism can simply act as a guiding principle. In fact, such reliance on social consensus is everywhere in

decentralized crypto too. Whenever one downloads a Bitcoin client, they implicitly decide to believe they're downloading a "real" client - they may not be. Many people have lost millions that way. Yet, nobody cares.

When evaluating possible objections, one should consider these basic criteria: Is the problem exclusive to this system? If not exclusive - is it *worse* in this system? If exclusive or worse - is it so bad as to render the absolute brokenness of decentralized systems more viable?

12.3 Advantages

If we now understand there are no real downsides, let's discuss the numerous and significant advantages of this design. These should be obvious, they're not advantages of *our* design, but advantages of every sane non-decentralized design. Nonetheless, for clarity, it's worth going over the most important ones:

1. There are no middlemen in this scheme. Technical changes can be made swiftly and without appeasing special interest groups like miners, self-proclaimed "community leaders", "developers" and many others. Only the people should get to have a say - the only group that's never consulted in the world of decentralization.

2. There is no unnecessary fragmentation in this system. There will be no 10s or 100s of different clients that result in terrible UX and unnecessary security risks for no good reason.

3. All the important features will get first class treatment rather than be implemented by potentially malicious third parties. In the world of smartcontracts every simple interaction is an "opportunity" to get scammed or defrauded.

4. The platform can have it's own "voice". It can manage its own PR.

5. The UX and overall design can form one logical whole that makes sense, rather than a hodgepodge of incoherent 3rd party apps.

6. The mega-app model eliminates Web 3.0's numerous privacy issues. Browsers are fundamentally leaky privacy-wise. The privacy model of each dApp is different. Our platform can guarantee uniform privacy standards throughout the network. This doesn't mean perfect privacy - this is a non-goal (and simply impossible). But it means a stable privacy profile, you don't have to wonder how this or that thing works.

7. Ironically, reliance on many potentially malicious "central" parties like Infura or dApp creators is reduced. There are fewer central parties in our system. Should we call ourselves "decentralized"?

8. Social attacks against the network are much harder since it will not rely on external platforms to host its community.

9. High performance/throughput without the usual security trade-offs. We're fast without a highly questionable consensus scheme.

10. Free transactions up to a certain level of use.

11. No reliance on benevolent "devs" who may or may not stay around.

12. Easy forkability

12.4 Cybercorporation model vs Web 3.0

Yet another source of objections may have to do with the mega-app model. Decentralization proponents may try to contrast the "open" model of Web 3.0 dApps with cybercorporations' "closed" model. The supposed openness of Web 3.0 may be cast as analogous to free markets, compared to cybercorporations' apparent central planning.

First, we should look at not-so-distant history. The "open" Web 1.0 already lost to Web 2.0 over a decade ago. Before that, the openness of open-source and Linux lost to Microsoft's "closed" model. One can pretend evil corporations keep conspiring to enslave humanity, or one can consider the good reasons for the victory of these "closed" systems. The reasons are nearly identical to the decentralization vs decentralization debate - these "open" systems never worked and never could have.

If such openness doesn't result in more output or prosperity then the comparison to free markets is just clever word play.

One may as well argue McDonald's is a communist joint because they don't let you bring your own potatoes.

Web 3.0's decentralization is the worst possible kind - it's really a network of small central actors. Every "dApp" developer must host their own app. How can they make money on their creation? There's no obvious way to charge for tiny pieces of Web 3.0 infrastructure. Charging fees just doesn't work. The obvious impetus is to become a little tyrant, to somehow gain control over your userbase and extract money from them in an indirect manner. The kind of features you need to operate an information network cannot be separate one-feature apps. It must all come together as one logical whole. Any dApp that would become a viable alternative to existing cyberspace infrastructure will inevitably separate from the host network and become its own thing.

In fact, those who care about this openness so much, should very much like the cybercorporation model. For the first time, something that's open-enough can win. Its "closedness" is constrained by the inherent "openness" of public ledgers.

Chapter 13

The Fediverse

To understand the importance of public ledgers, we should examine decentralized systems that *do not* employ public ledgers. Fediverse is a perfect specimen. It's loose network of independent cyberspace communities. Imagine that Facebook was broken up into thousands of little Facebooks that could talk to each other - that's the Fediverse. Proponents of decentralization would have you believe this competition would result in a spontaneous tendency for liberty, for better user experiences - more overall goodness. But instead, Fediverse proved the Federalist founding fathers right - there was no exaggeration in their unflattering predictions about confederacies. "Mutual animosities" between these little communities resulted in an environment *more* censorious than their Big Tech counterparts. Instead of removing tyrants, the Fediverse multiplied them. Instead of fostering individuality, you're forced to pick a faction. The absolute breaking point

came when Gab, an alternative social network, decided to join the Fediverse. While both Gab and most of the Fediverse shared a hatred for Big Tech, their politics couldn't be more different. Gab unleashed a Fediverse civil war. It wasn't just about banning or not banning Gab, but banning those who wouldn't. Every community had to decide - are they with the anti-Gab faction or the pro-Gab faction. Neutrality was considered implicitly pro-Gab. The "neutral" crowd was in the toughest spot. Gab was and is a big platform. There's no question their leader, Andrew Torba, is a guy everybody has an opinion about. But as any big platform, Gab has all kinds of users. If you ran a Fediverse community, some of your users probably connected with perfectly average and uncontroversial Gab users. Why should they be punished? But if you didn't punish them, others may punish you and your users for not banning Gab. There was no way to win. Whatever you decided to do - somebody was going to get banned.

Eventually Gab left the Fediverse altogether. Today, Gab likely has more active users than the entire Fediverse combined. Gab's UX is not particularly remarkable, but it's fair to say it's much better than the rest of the Fediverse. The Gab codebase is Mastodon fork (the most widely used implementation of the Fediverse). The Gab codebase is nominally open-source too - for legal reasons - but they develop it like any proprietary shop would. Gab has just a few developers on staff, likely less than 5. Mastodon has thousands of "commits" from hundreds of developers around the world. How did Torba's tiny team out-compete them?

There's nothing remarkable or surprising about this. As you'll

see - perhaps already saw - throughout this book, this is the rule, not an exception. It should also be clear to you, decentralization, in and of itself, has no redeeming value.

Chapter 14

Bitcoin maximalism

It just so happens, that sometimes the best criticisms come from within. Bitcoin maximalists, or "maxis", are a group of hardcore Bitcoin supporters who believe Bitcoin is the only crypto that works. They're unique in being the one notable group in crypto willing to talk about the problems with decentralization. So as long they don't have to admit there's anything wrong with Bitcoin, maxis are perfectly willing to see decentralization theater in *other* cryptos for what it is. They would likely agree with many points made in this book:

1. They know decentralization is incompatible with big ledgers or high throughput - Bitcoin knows not to even attempt scaling
2. Maxis recognize all the problems with Web 3.0 and dapps, infura etc - Bitcoin knows not to attempt any non-currency usecases

3. They know most distributed consensus schemes (other than theirs) are fundamentally broken - they kept Bitcoin as simple as possible

It would seem almost defeatist to admit these things. Aren't they arguing against themselves? By reducing Bitcoin's scope to being just a store of value and nothing else, in a way, they turn these issues into their main strength. As broken as decentralization is, if all you want to do is have a low-throughput database of balances (or UTXOs), it may work! Short of some assumptions about Proof-of-Work collapsing, it's hard to find a major issue. In this way, Bitcoin exceptionalism may as well be justified - it's the only crypto that's not hopelessly broken.

But Bitcoin can't do much.

Chapter 15

In defense of Satoshi

Was decentralization Satoshi's biggest mistake? We're not going to worship the guy, we find this distasteful. But we're not going to unduly defame him either. Satoshi could not have gotten it "right"!

Put yourself in his shoes. It was 2009. There was no crypto. Information networks were hardly a thing, he was working on creating an e-cash system, not something else. How would he raise money for a cybercorporation. How would he pay for goods and services? Why would he be concerned about downsides of decentralization? E-cash is just simple enough to work. Performance would be one concern but he couldn't even be sure anybody would use his system. Premature optimization is never good. In fact, perfromance is the one issue that may have some good solutions. Satoshi may have been drinking decentralization kool-aid. For example: when he calls Tor "pure p2p" that's simply not true - the security of the Tor network

depends on hard-coded "central" directory servers operated by Tor insiders - Tor is a decentralization theater creation. But it simply didn't matter. Whatever he thought of decentralization, he couldn't have done any better. For all the problems with decentralization, Bitcoin with its limited scope may still be a sound cryptocurrency. The Bitcoin model simply cannot be extended for anything beyond that. We certainly shouldn't blame Satoshi for inspiring the deranged Web 3.0 idiocy.

Would he like what we're proposing? We have no idea. Given his likely crypto-anarchist background - probably not. But his invention of Bitcoin and the effect it has had on the world is the very thing which enables cybercorporations to exist today. Would not have been possible without him.

To Satoshi, we say: "Thank you!".

Chapter 16

Why a corporation?

With pragmatism as the guiding principle we simply have to pick the only organizational structure with a solid track record for delivering cyberspace products. Corporations work. We know that the leaderless open-source style model simply doesn't work. Other than these two, there aren't many other governance models known to cyberspace.

Given that cyberspace information networks are analogous to governments, it may be enticing to mimic organizational structures of governments. It's an idea worth exploring, but it just seems like pointless skeuomorphism. Anything too democratic is simply unworkable - we cannot identify who the natural persons in cyberspace are. The only marginally workable voting system would be a well-distributed shareholder democracy - at this point we're really back to being a corporation albeit with an over-diluted cap table. Over time, our cap table will become more distributed too. But it's always a red flag when

a corporation starts off this way on day one.

It's not obvious there even is a strong moral case for democracy in cyberspace. It's not easy to move to other countries. Most citizens are natural-born - it wasn't their choice. Thus there is a natural obligation to give some power to the people unconditionally. For example, we're usually fine with immigrants having limited political rights - nobody forced them to come and presumably they have somewhere else to go. In cyberspace there are no natural-born "citizens" and you can "move" at will. Even the kind of "lock-in" platforms may exploit is greatly reduced thanks to public ledgers and forkability. You cannot fork Facebook or Amazon. You can fork a cybercorporation. So there already is a tremendous pressure on the cybercorporation to respect the people.

Another important thing to understand about our model is technological flexibility. We should not adopt decentralists' transcendental attitude towards software development and systems design. We need to maintain a stable environment for the people, not the underlying implementation. Cyberspace is not a stable environment at all. Our strategic assumptions will inevitably change. Consider the transaction fee problems many cryptos face. People may have joined the network never expecting the fees would simply sky-rocket one day. The underlying implementation may not have changed. But for the actual end-user, everything has changed! The stability is at the wrong level. It's like having a conservative military - the worst possible idea.

It's hard to predict what's going to happen in the next 20

years. Chances are cybercorporations may, over time, transform to resemble regular corporations less and less, and we'll simply call them something else.

Chapter 17

Censorship in name of "censorship resistance"

Decentralization proponents love to talk about "censorship resistance". Every lover of liberty will surely like this term. Censorship is bad thing. It may seem hypocritical that Jack Dorsey, the King of Censorship, happens to be Bitcoin's biggest cheerleader.

Like "decentralization", "censorship resistance" is yet another term that sounds great in vernacular, but means something different. It has nothing to do with the ability to disseminate information. "Censorship resistance" is when a blockchain can guarantee no transactions will be unfairly rejected and history won't be rewritten. That's all it is.

So why does Dorsey love Bitcoin? We don't know why. But we can guess. There's something interesting on his right ankle. It features a tattoo of a red-black star - the symbol of anarcho-

syndicalism. Perhaps you remember from a previous chapter, that Timothy May specifically disavowed anarcho-syndicalism as not the kind of anarchism he likes. Kind of ironic.

Dorsey makes it clear he's not a "crypto" guy. He's a Bitcoiner. Perhaps because Bitcoin is the most consequentially anarchistic. At times he's attacked other cryptos for not being "decentralized" enough.

Twitter may not be the biggest social network, but it is the most opinion-forming one. In politics, crypto and many other areas. Dorsey has a long history of utilizing his control over Twitter to promote his preferred politics. Therefore, one has to wonder… Given his strong opinions on crypto, is he manipulating crypto discourse too? How come all these proponents of "decentralization" and "censorship resistance" don't see the irony of conducting all the crypto discourse on this censorious and centralized platform?

When protesters trespassed into the US Capitol on January 6th 2021, Dorsey went on his biggest censorship spree yet, eventually banning President Trump himself along with most of his loyal supporters.

Vinay Gupta (@leashless on Dorsey's platform), one of the early Ethereum insiders, saw the writing on the wall and understood that Ethereum had no real "censorship resistance":

> *If Parler was been built on Ethereum instead of AWS, RIGHT NOW we would be losing ALL of the non-blockchain infrastructure the Ethereum community depends on*

web sites exchange licenses bank accounts IPFS infrastructure Infura

No fascists!

…

So if we take a very public hard line and make it very clear that every door which CAN be closed WILL be closed, the neonazis may well take the hint and go somewhere else: one of the privacy coins maybe. Or gold.

Because a Parlercoin on Uniswap could be deadly legally for ETH. …

I think we have a LOT of power at every level except the protocol layer.

The surrounding system is filled with choke points.

To list five: Infura, exchanges, the defi ecosystem, programmers, and audits.

Ethereum, without access to any of these services, is so much less useful. …

Ethereum: not a safe haven for Nazis, fascists, and the kind of people that try to take elected officials hostage.

We understand the Paradox of Tolerance, and are prepared to stand our ground.

You want a Nazi friendly Ethereum? Fork the code ratface.

…

Because if Ethereum is IN ANY WAY involved in the financing or operations - including propaganda, like Parler - of an ongoing insurgency, they will ***kill our technology globally****.*

I mean they will blackbag Vitalik in Singapore and dump the core devs in Guantanamo Bay, for reals.

Now, you have to understand - Gupta is not talking about National Socialists here. He's talking about supporters of President Trump. Gupta is not stupid - he's *afraid.* If Gupta wanted to censor them for something they really are, out of *his own* conviction - that would have been one thing. But he makes it clear - he's simply *afraid.* Ethereum has exactly the same problem traditional corporations have. If Ethereum's decentralization provides no sovereignty - what's the point?

Even if he's wrong in thinking that Ethereum would be *legally* attacked over this - he may be - perhaps it reveals a greater issue. Because these crypto platforms don't have their own information networks, they're not even immune against basic social attacks. They can't think for themselves. Like all Twitter users, they're Dorsey's minions - at the very least - they have to pretend to be his minions.

Long before Ethereum's weak decentralized infrastructure, America's Federalist founders understood this problem:

One government can collect and avail itself of the talents and experience of the ablest men, in whatever part of the Union they may be found. It can move on uniform principles of policy. It can harmonize, assimilate, and protect the several parts and members, and extend the benefit of its foresight and precautions to each. In the formation of treaties, it will regard the interest of the whole, and the particular interests

of the parts as connected with that of the whole. It can apply the resources and power of the whole to the defense of any particular part, and that more easily and expeditiously than State governments or separate confederacies can possibly do, for want of concert and unity of system. It can place the militia under one plan of discipline, and, by putting their officers in a proper line of subordination to the Chief Magistrate, will, as it were, consolidate them into one corps, and thereby render them more efficient than if divided into thirteen or into three or four distinct independent companies.

What would the militia of Britain be if the English militia obeyed the government of England, if the Scotch militia obeyed the government of Scotland, and if the Welsh militia obeyed the government of Wales? Suppose an invasion; would those three governments (if they agreed at all) be able, with all their respective forces, to operate against the enemy so effectually as the single government of Great Britain would?

We have heard much of the fleets of Britain, and the time may come, if we are wise, when the fleets of America may engage attention. But if one national government, had not so regulated the navigation of Britain as to make it a nursery for seamen–if one national government had not called forth all the national means and materials for forming fleets, their prowess and their thunder would never have been celebrated. Let England have its navigation and fleet–let Scotland have its navigation and fleet–let Wales have its navigation and fleet–let Ireland have its navigation and fleet–let those four

of the constituent parts of the British empire be under four independent governments, and it is easy to perceive how soon they would each dwindle into comparative insignificance.

Apply these facts to our own case. Leave America divided into thirteen or, if you please, into three or four independent governments–what armies could they raise and pay–what fleets could they ever hope to have? If one was attacked, would the others fly to its succor, and spend their blood and money in its defense? Would there be no danger of their being flattered into neutrality by its specious promises, or seduced by a too great fondness for peace to decline hazarding their tranquillity and present safety for the sake of neighbors, of whom perhaps they have been jealous, and whose importance they are content to see diminished? Although such conduct would not be wise, it would, nevertheless, be natural. The history of the states of Greece, and of other countries, abounds with such instances, and it is not improbable that what has so often happened would, under similar circumstances, happen again.

– *FEDERALIST NO. 4*

It's almost a prefect description of Ethereum's vulnerability. There are too many independent parts with different leaders and different motivations to operate under "uniform principles of policy". You can attack its constituent parts without any kind of a response from the rest of the network.

The cybercorporation model doesn't have this vulnerability. If bad actors want to destroy a cybercorporation, they have to

bring the whole thing down - and there's no easy way to do it. They can try to temporarily disrupt it. But to really destroy it, they'd have to turn the Internet off.

If you found this chapter "controversial", perhaps it's an indictment of today's crypto. There's nothing untrue about these facts. There's nothing repugnant about mentioning them. People are simply afraid to talk about them - there's very little "censorship resistance" in today's world.

Chapter 18

Moral agnosticism

If we need sovereignty, why not create a new country instead?

As long as there is no world government - and there shouldn't be for good reasons - chaos in cyberspace cannot be solved by traditional territorial sovereigns. This is not to say one couldn't or shouldn't create a new "country". But to tie such efforts to cyberspace issues would be misguided. Cyberspace injustices have to be solved in cyberspace. Trying to impose "solutions" externally is the very source of these injustices.

Thus, this entire anarchistic war on the legitimacy of nation states is not helpful at all. The issue of legitimate rule over cyberspace should be the only source of potential contention that is worth fighting over. Everything else is irrelevant. For example: Bitcoin maximalists often say the adoption of Bitcoin will destroy states' ability to wage war (supposedly because "fiat money" is the thing that enables war). How does this help anybody? Why can't one support liberty in cyberspace and be a

patriot to one's country? Our right to *independence* in cyberspace does not absolve us from basic moral duties. We are still of the same world, and if there *is* a war, perhaps a world war, with an obvious good and bad side - why shouldn't we support the good guys? In fact, if there is such a war and the system *just won't let us* help the good guys - then this system is a piece of sick junk!

Illegal drugs are another such issue. Some make interesting arguments against regulating drugs. But why can't countries decide themselves? Is it really the most pressing issue of our day? Don't these substances kill millions for no good reason? Don't they destroy even more lives? Regardless of the issue of *legality*, shouldn't every individual with a semblance of morality try to dissuade people from ingesting this poison? Do you really think a glorified drug dealer is the greatest cyberspace freedom fighter? Many crypto anarchists do.

Sovereignty does not mean we don't have any moral obligations. It means we don't have to listen to other worldly entities when we disagree. But we still have to listen to our conscience. What's wrong is still wrong.

To gain support of these who are not as morally agnostic - and most people rightfully aren't - anarchists often claim to do anything about bad behavior, universally means compromising the entire system - any attempt to police the system will do more harm than good. This is true - but it's a self-imposed constraint of these anarchistic designs. The fundamental lie is in pretending there's no other way to approach this issue. When presented with a viable alternative, anarchists will usually point out the nominally true possiblity of the innocent being punished.

Many of us certainly agree the innocent shouldn't suffer in the name of stopping crime. The Blackstone's ratio expresses this idea very well:

> *It is better that ten guilty persons escape than that one innocent suffer.*

Some may say 100 to 1 is a better ratio - but a *ratio* nonetheless. The anarchist argument is essentially "It is better to let ALL guilty persons escape than that one innocent suffer".

There exists no society without rules. When we don't know what the rules are, we waste time trying to figure them out. We may not be able to. We will be left questioning our every action. Is this okay, or is not? Will I get in trouble? Who knows?! Nobody knows *the* law of the jungle, but everybody knows it is law!

As much as laws may restrain us, a stable set of rules is what frees us from this tyranny of anarchy. To know what you cannot do, is to know what you *can* do. It's also to know what others will not do to you. Under a stable legal system, you can make long-term decisions about your life. You can embark on multi-year efforts without worrying about stability of societal order.

There's no reason why cyberspace should be any different. We need stability as much as anybody else. The kind of rules we care about cannot be enforced by computers, they don't understand human rules. We cannot use public ledgers directly to enforce such rules. But we can use public ledgers to enforce basic rules of due process. We can make guarantees about the actual process of enforcing human rules.

Many are so allergic to the idea of policing in cyberspace because there are no sovereign legal systems in cyberspace. The kind of rules you may see today are no rules at all. They are merely excuses to do whatever the ones in power want. It's not just malice - without sovereignty a platform cannot create a stable set of rules - we've discussed this already.

Decentralized systems can use public ledgers, but they cannot use them to ensure due process. There's no party in a decentralized system that can even begin to have a claim to impartiality or an incentive to be fair. In the world of decentralization everybody and everything is suspect. A system of rules would only result in more chaos.

If a desirable ratio - as in Blackstone's ratio - can be achieved why shouldn't we want such an ability? Also notice that while serious real crimes can be stopped in cyberspace, the maximum punishment a cyberspace entity can apply is relatively mild. A cyberspace platform can never sentence one to death or even prison time.

Chapter 19

Zawinski's Law of Centralization

The respected programmer, Jamie Zawinski, made a simple observations decades ago:

> *"Every program attempts to expand until it can read mail. Those programs which cannot so expand are replaced by ones which can."*

The observation is so accurate and timeless that many call it "Zawinski's Law". Many consider it to be an indictment of the software industry - perhaps evil corporations can't stop themselves from pushing useless features down users' throats. But reasonable people acknowledge it's simply the way things are. Most programs or software we use tends to be big. They tend to be platforms. There may be some small utilities we use, but

we probably don't even notice them or consider real programs at all.

There is very little middle ground. Non-trivial programs are non-trivial to make. You need to make money, you need to hire developers. If you do start making enough money, sooner or later, you'll have competition. If they're much better capitalized they can just copy whatever you're doing and roll your features into their presumably bigger app. Inevitably, to fight back, you'll have to do the same. You have to grow or die.

This is not in any way anti-user. Nobody wants a 100 different apps. It's easier to have many features packaged in a coherent manner.

Decentralist Web 3.0 visionaries don't understand this. They envision a loose network of medium-sized apps that peacefully coexist in this decentralist confederation. Whether for their own sake or their users' sake, dApp developers have the same reasons to always grow. It's hard enough to make money on dApp to begin with, let alone a small one. Users too don't like having to go to so many different websites to do simple things. Remember cryptokitties? What are the creators up to nowadays? They created their own NFT blockchain!

Chapter 20

You'll have no apps, and you'll be happy

The only "decentralized apps" with some adoption seem to be fairly self-referential. Like trading Ethereum tokens - basically cryptocurrencies within a cryptocurrency. Not that different form Satoshi dice years ago. It's hard to find something that actually extends beyond the currency realm. Some platforms don't even have these little toys, yet they promise a lot. Say, Cardano. Maybe you've heard of Cardano. But have you ever heard of a Cardano app? Don't google it! Try to think of one. We're not trying to put them down, but it's a good example to illustrate a point:

> *Cardano is a blockchain platform built on the groundbreaking Ouroboros proof-of-stake consensus protocol, and developed using the Haskell programming language: a functional*

programming language that enables Cardano to pursue evidence-based development, for unparalleled security and stability.

...

Cardano provides the template and toolset to a new age of innovation. It introduces leading-edge technologies, models, and methodologies to help individuals, developers, and enterprises discover a new possible, realize change, and enrich their lives.

Blockchain technology holds the answer to a number of legacy challenges, whether financial, societal, or technological. It disintermediates essential relationships, and redistributes power to alleviate costly dependencies, restrictive paradigms, and inefficient systems of transaction and exchange. Cardano is a realization of this potential. It is a platform with the security, privacy sustainability, and performance standards required to accelerate the mass adoption of the technology, and support a lasting ecosystem.

Cardano powers new, more secure, and globally scalable solutions. Its technology is continuously improved upon through evidence-based development methods, and guided by a democratic voting system, in which every member has a voice. The opportunity of Cardano is adaptable to your use case. It is an opportunity that creates other opportunities, continuously.

That's a short excerpt from Cardano's website. It's pretty

characteristic of how most crypto platforms present themselves. Mostly as technological building substrates, rather than something that can be used directly. Notice how Cardano even mentions the programming language they use.

The actual use cases are supposed to be spontaneously developed by 3rd party developers. The most obvious analogy would be to an operating system. The crypto platform is the operating system, and developers will write the apps. But there's a serious problem with this analogy…

It's perfectly true that a computer system may accrete features in a seemingly serendipitous manner. Say, a 3rd party developer may create a widely popular application that ends up benefiting the underlying OS. This is not in dispute. But what many of these platforms seem to be doing, is to not merely suggest some nondescript good thing will happen, but that something specific will happen; that the very value of the underlying system is predicated on that happening; yet, the creators of the systems are not working on that happening and cannot explain exactly how it's going to happen.

To make an operating system and say - *"Developers will make cool apps for my OS!"* - that's perfectly reasonable. But to say - *"Buy my OS because developers will create world class photo-editing software for it"* - that's a strange thing to say unless you're developing it yourself. Many crypto platforms seem to implicitly be making statements of that form. If the very value of the product is predicated on that somebody else, why wouldn't they make their own platform? Conversely, why aren't the platform creators working on it themselves, fearing that someone will

create their own platform?

Even this idea of an abstract operating system where every real feature is an app is a pipe dream. Linux is the only operating system that fits this bill. It's a total failure - probably for that very reason. Let's contrast it with the infinitely more successful Windows. Windows comes with a nice window manager, perhaps you don't even know what a window manager is. That's the thing that controls how app windows are laid out on your screen. Linux doesn't have a built-in one. There are many different kinds, all with that distinctive open-source "quality". Windows has a top-notch file explorer. Linux doesn't have that either. There many, none of them any good. The kind of people who use Linux probably couldn't care less, only "newbies" need a file explorer.

You see, Linux is a kernel, not an operating system. There are no decent Linux based desktop operating systems. Android is the best Linux operating system. Google took the Linux kernel and built a good operating system on top of it. Android has nothing to do with your desktop Linux whatsoever. Crypto platforms are more like that Linux kernel. They may be perfectly good kernels, but you shouldn't expect something to simply "emerge" on top of them. Somebody may take this code and build something - like Google has with Android - but a kernel-like platform cannot have much intrinsic value.

Back in the day, open source people were the decentralists of their era. They rallied against the closed and propriety nature of "M$" Windows. Closed-source software was simply wrong and immoral, much like "centralization" is supposed to be today.

They made many seemingly compelling technical arguments too. Open-source software was more secure - more people would find bugs in the code. That claim is contentious at best and there are many reasons to believe the opposite. Because everybody can contribute to open-source software it would be better, more people would work on it - we know how untrue that is. The few successful open-source projects are developed by private companies in a "centralized" manner.

Realizing that decentralism will never produce a compelling information network like Facebook, decentralists may say: *"Facebook is actually a bad idea, why would you want Facebook?!"* . This tendency is not new either. Many were ready to put up with some oddness of Linux, but perhaps they needed a good photo editing app like Photoshop…

"Don't worry there's GIMP!"

People would say - *"Well you know, I'm sorry but GIMP is nothing like Photoshop…"*

"You must be too used to Photoshop!"

"GIMP is just different, you'll get used to it!"

"Did you know GIMP has a LISP scripting system - Photoshop doesn't have that!"

You couldn't win with these people. Common sense tells us decentralist won't simply concede either.

Adobe has billions of dollars. Perhaps we should cut these open-source people some slack? Well, Ivan Kuckir didn't need much money. This lone-wolf Czech developer created Photopea - a free web-based photo editor that is a very faithful copy of Photoshop. That's exactly what people have always wanted.

Those who subscribe to open-source mythology may think Ivan must be the greatest genius out there. He is certainly a smart individual. But those who understand the software industry, know him being just one man is *exactly* what allowed him to deliver. A reddit user asked: *"How come Photopea can handle .psd files while Gimp still can't?"* Ivan replied: *"You should ask Gimp developers this question. There are probably too many of them, and they struggle to cooperate. I made Photopea as a single person, so I avoided such problems"*

You're exactly right, Ivan!

Chapter 21

Outro

We criticize decentralization because it doesn't work. Not because of what it stands for. If you are or were a proponent of decentralization because of all the good things you believe it can do for the world - **we're on the same team.**

The cybercorporation model is simply better. It's more secure. It's more private. More performant. More user-friendly. And ironically, relies on *fewer* central trusted 3rd parties.

We want to, and are, building something real. It's time to start playing to win.

We hope you will join us on this journey: **joinfamily.xyz**.