Atoms, Institutions, Blockchains

0.

After 7 years of writing and thinking about blockchains, I struggle to explain them.

I can explain how blockchains work, and what their properties are. I can explain how specific applications function, and why. I can explain why hundreds of millions of people use applications like cryptocurrency, defi, NFTs, and why those people find them useful.

But when I reach for words to compare blockchains to the other hard things we have used to build our civilization, I struggle. It is not that blockchains are difficult to explain in isolation, but that we seem to lack a language for speaking about a broader category to which blockchains belong. We do not even really recognize that there is such a category.

Here is one way of articulating what is missing:

What do blockchains and institutions have in common?

“Institution” here means formal institutions: groups of humans who behave according to certain rules, and who together cohere into an organization that has a distinctive permanence. Like governments, companies, central banks, and legal systems.

The reason we should be able to compare them is that we use them interchangeably. Both institutions and blockchains can enable *money*. Fiat currency is the product of a certain set of institutions working together - central banks, governments, legal systems. Cryptocurrency is the product of a blockchain. While these two types of money have different strengths and weaknesses, they are both used interchangeably as money by hundreds of millions of people.

If blockchains and some institutions can both create money, then they must share some property, some quality. Most things in our world are *not* capable of producing money - so what unites the few that are?

It is strange that there is no immediate answer. We have lots to say about how blockchains and institutions are different (decentralized vs centralized, non-custodial vs custodial), but we don’t have a consensus answer about what they have in common.

Compare this to another familiar question:

The SSD in my laptop, a piece of pressed vinyl, and a pattern of vibrations in the air can each contain the same song. What do they have in common?

They are all mediums for *information*. A piece of flash memory, a record, and a wave propagated through the air can all contain the same song, because a song is information. Even though these things are radically different from each other, they can each be mediums for a higher-order abstract property. They can be substitutes for each other - even if they might differ in some important ways, like their capacity or durability. We can make these statements, and compare mediums for information precisely, because we have the concept of information.

But this is a very new development. The *idea* of information in the modern definition - a measurable but abstract concept encompassing all structured data in any medium - is quite recent. This idea was not popularized until the 1950s, when advances in what became known as information technology lead to the development of information theory. This new concept provided us with new tools to make sense not only of new technologies, but large parts of a world that we thought we understood, but which were belatedly revealed in a new light as mediums, repositories, and instances of *information*.

It took years for this idea to spread into mass culture. Today, it is intuitive to most people that speech, images, films, writing, DNA, and software are all just *different kinds of information* rather than distinct and separate things that must be understood on their own terms.

I believe that we are in a similar situation today. A new technology has forced us to reconsider things we thought we understood, viewing them from a more distant vantage point. Things that once seemed unrelated are revealed to be part of a broader category, and our task is to articulate that category and remake our understanding of the world.

There is an analog to *information* hidden in the foundations of our civilization. Some general, abstract property that, once revealed, might be found everywhere.

1.

Let's call this property **hardness**.

Human civilization requires things that persist. Fixed, hard points across time that let us make the world more predictable in specific ways.

We need these hard points because it is impossible to coordinate at scale without them. Money doesn't work unless there is a degree of certainty it will still be valuable in the future. Trade is very risky if there isn't confidence that parties will follow their commitments. The bonds of social and family ties can only reach so far through space and time, and so we have found other means of creating certainty and stability in our relationships. Throughout history we have found ways to make the future more certain, creating constants that are stable enough to rely upon. We have found ways to create hardness.

One source of hardness has been physical stuff - Atoms - in the natural world around us. We found objects and systems that had some convenient properties which, we learned through experience, were quite hard to change. We picked up shells, rocks, and metals from our environment, possessed and defended them, and used them as a basis for commerce.

Over time we learned to create our own hardness, and not just borrow it from nature. We built institutions - groups of humans who work together, who behave in predictable ways over long periods of time. We learned to *design* these institutions to become very reliable - so that we could give an instruction to an institution, and be sure that those instructions would be followed - even years, decades, or centuries later.

Recently, we've invented a new way to create hardness: blockchains. Using an elegant combination of cryptography, networked software, and commoditized human incentives, we are able to create software and digital records that are *hard*.

The property that Atoms, Institutions, and Blockchains each have in common is their *capacity to produce hardness*. The ways that they do this, and the types of things they can create hardness about are vastly different, shaping their utility for different human purposes.

If government, money, and law are the infrastructure of our civilization, then Atoms, Institutions, and Blockchains are the raw materials this infrastructure is made out of. The choices we make about what infrastructure should be built with what combination of materials has profound consequences for how that infrastructure - the very basis of our civilization - functions.

2.

We don't have a good way of speaking about hardness. To do this more carefully, let's define some terms.

Each of Atoms, Institutions, and Blockchains can be a source of hardness. This means that they can be used to *make something very likely to be true in the future*. The "something" here can vary greatly, and different sources are good at making different "somethings" hard.

When speaking about hardness, there are three things we need to talk about:

1. What is the hardness ***about***? What is the "something" which is being made extremely likely to be true?

2. What is the ***source*** of that hardness? What is the *reason* it is very likely to be true?

3. ***How hard*** is it? How can we measure the degree of hardness?

First, what is the hardness about? What is its informational content? I will call this the "cast". The cast is the "thing that is hard", and it always takes the form of a statement about the future. I'm coining a term here because I do not think there is a suitable existing word for the concept. I use the word cast for its dual connotations in English of *a thing we throw ahead of us* and *a thing which hardens to protect or shape*.

For example, one important "cast" about gold is that its supply will remain predictable in the future. We could express this precisely as "between X and Y kilograms of gold will enter the market each year for the next 20 years".

Or, consider a loan agreement. The cast here might be something like "If Alice does not pay Bob back $100 before July 1, then the legal institutions of my jurisdiction will use increasingly severe threats and actions to force her to pay Bob".

In the case of a digital asset on Ethereum, one cast might be "this asset can only be transferred if a transaction is signed using the private key that corresponds to the public key X".

Casts are descriptions of some future state of the world. A cast is *hard* if that future state of the world is very likely to turn out to be true. These casts might be claims about something *not* changing ("the object in my security deposit box will still be there in 10 years"), or something changing at a certain rate ("The supply of Bitcoin will inflate predictably for the next 100 years"), or something that is conditional on other actions ("If we get divorced, here is how we will divide our assets").

In practice, we are usually interacting with bundles of interrelated casts, which woven together, create stability and predictability in our affairs. For instance, if you own gold but store it in a bank, there are many interlocking casts that matter to you: casts about gold's supply in the future, the integrity of the institution holding your gold for you, the physical properties of the vault where it is stored, the strength of the legal agreement between you and that institution, the reliability of the legal system in the jurisdiction where you live, and many others.

Second, there is the *source of hardness*. This is the *reason* that the cast can be hard in the first place. It is what the cast is *made out of*: atoms, institutions, or blockchains.

Sometimes the properties of our physical universe are the source of hardness. There just *is* a certain amount of gold contained within the earth, and only a portion of it is accessible to us with our current technology. That simple physical truth is the *reason* casts about the supply of gold are hard.

In other cases, the source of hardness might be an institution. A contract is only hard if there is an institution that makes it so. Groups of people - lawyers, judges, police officers - who share a common understanding of how to behave, and who have proven over time that they are likely to behave in a predictable fashion.

Or, the source of hardness might be a blockchain. The *reason* a smart contract will operate the way it was programmed is that blockchains provide very high assurances that this will happen, by creating incentives for people to maintain the network and making it extraordinarily expensive to censor or stop its function.

With these two components identified, we can ask: how *hard* is a particular *cast?* Hardness is always measurable in theory, even if it is difficult to do so in practice.

For example, take the example of gold. How *hard* is the cast "between X and Y kilograms of gold will enter the market each year for the next 20 years".

This is something we (as a species) know a lot about. People spend a lot of time and money trying to predict how much gold will be mined every year, based on what we know about the properties of our planet, the technology available, and the industry built to extract gold from the earth.

One way to measure the *hardness* of a cast is to estimate probabilities. If you had all the relevant data, you might come to a conclusion that there is an 80% likelihood that "between X and Y kilograms of gold will enter the market each year for the next 20 years".

Another way to measure hardness is to estimate *how much it would cost* to create a world where the cast turns out to be false. Is there a price that someone could pay to create a world where less than X, or more than Y kilograms of gold enter the market? What does it cost to *break* the cast?

There is a price of course, though it is probably very high. Someone with the resources of a nation state could disrupt global gold production over an extended period to bring it below X. And it is also conceivable that in the next 20 years, someone could obtain a near-earth asteroid that contains a large amount of gold, causing the production to exceed Y.

In the example of a legal contract, we can also measure the *hardness* in terms of probabilities and costs. If Alice does not pay Bob back, and Bob sues her for breach of contract, Bob's lawyer might advise him that there is a certain chance of success. Because the final outcome is at the discretion of a person (like a judge), these probabilities can be very hard to estimate.

As with the gold example, we might also express this in terms of cost. what would Alice have to *pay* to change the outcome? She could flee the jurisdiction, or she could spend a large sum on expensive lawyers that diminish Bob's chances of success.

It's important to keep in mind here that the *content of the contract* is not the *content of the cast*. A legal contract is a tool used within a broader institutional context, but it does not contain or express all of our implicit expectations about the future state of the world we are trying to create using this tool. The *cast* is about how the whole system will behave in the future, and the words

of a contract are just one part of that system. The contract itself cannot tell you if you can afford a lawyer to enforce it, or whether the legal system will behave in a corrupt fashion.

3.

Atoms, Institutions, and Blockchains are all different from each other. As a species we have been very opportunistic, and creative, in how to find or create hardness that enables human coordination.

AIB are not the only things that humans use to create durable relationships and coordinate with each other. Within a small social graph of a few hundred people, the bonds of family or social ties are often sufficient to create durable relationships around value, shared ownership of property, and more. In larger numbers, human culture and belief systems influence how we behave - for instance cultural taboos around theft, or breaking promises, or respect for authority figures.

AIB are artificial supplements we have built to solve coordination problems that extend beyond the family, social, or cultural group. They are in a real sense technology - social technology - that let us build structures strong enough to reach across great distances in time and space.

Atoms

“Atom” hardness refers to hardness that is sourced from the physical properties of our universe. This includes more than literal atoms (i.e. matter, physical stuff), but all other properties of nature like physical laws and constants. “Atom” is just a convenient shorthand.

The easiest example is early money. Humans found objects in our environment - shells, gems, rocks, metals - that had a collection of useful features.

One feature was that they were scarce. This meant that there was a better chance that these objects would retain their value over time. The cast “shells of this type appear on the beach at a consistent rate of X” was *hard*, because of a predictable natural process in the local ecosystem of a society.

Another feature is that these objects were small enough to be easily possessed, transferred, and defended. By exchanging these objects, and placing them in the possession of different people, we could in effect record information about a social relationship relating to money, value, or social status. The ability to possess and defend those objects conferred *hardness* to those relationships. Physical reality stores information, and we can manipulate that information by manipulating the environment.

We have so far relied on examples of casts about the supply of objects - gold, shells, etc - but atom-hardness includes all of the ways that we use physical reality to create hardness about casts that are socially important to us. We create walls, barriers, homes, and other secure structures to increase the hardness of casts about ownership of physical things and other social relationships.

Atom-hardness has advantages and disadvantages. One great virtue of atom-hardness is that it is *automatic*. To state the obvious, a wall just *is*. You do not need to depend on some other party to enforce the wall, or enforce the supply of gold within the earth. Another virtue is that atom-hardness is not subject to human discretion. There is no person you can bribe or corrupt to subvert physics.

But atom-hardness is limited in frustrating ways, making it increasingly unreliable as a source of hardness for human civilization.

First, we are limited to what nature provides: we can only *find* properties in nature, and use them where those properties happen, by accident, to fit some social need. We cannot say to the universe “we’d like another type of shiny rock, with a supply curve a bit different than gold, spread more evenly among these nation states”. We’re stuck with what we have.

Second, atom-hardness doesn’t allow for very expressive or customizable hardness. Over time, humans have developed a need for complex casts, like “in the event of a decrease in price in the underlying asset, the parties shall pay…” or “if Alice and Bob divorce, the rule for splitting their assets shall be…”. We can’t give nature specific instructions about complex and subtle human relationships.

Third, atom-hardness relies on implicit limitations of human capabilities. But as human technology has improved, we have overcome many of these limits, undermining the hardness of some atom-casts.

Using shells for money works for a while, until your society expands into an ecosystem where those shells are plentiful. Once a civilization expands outside of a certain ecosystem, the assumptions they made about what is *hard* might change. Humanity might someday face that problem with gold, whose supply is limited on earth, but abundant throughout our solar system.

New technology sometimes undermines atom-hardness completely. Sometimes we replace it with institution-hardness.

For instance, limitations on the speed of travel and communications were once relied on as a source of hardness for casts that shaped our political systems.

In the early 1800s in North America, there was a hard cast with the content “the fastest information can travel is roughly at the speed of a pigeon”. This cast was *hard* because the

physical properties of our universe seemed to prevent, as far as we knew at the time, communication traveling any faster than this.

One way this cast was socially useful related to elections. The results of voting on the east coast of North America could not be reported fast enough to influence voting on the west coast, ensuring that later voting periods were not influenced by this information.

But eventually, we had technology that undermined this hardness and broke the cast. But we wanted to keep the cast, so we just remade it by substituting institution-hardness where atom-hardness had failed us. In Canada, there are now laws that prevent reporting election results or exit polls before a certain time. In the United States, there is a long-standing convention about the same among media organizations (not a law, but a different form of institutional hardness).

This has been a common pattern over time. As our control over nature increases, things we once believed were hard have crumbled away, and we have patched the holes using institution-hardness.

Institutions

Over time, humans developed a need for a different kind of hardness. Hardness that could be used for casts that were specific, complex, and conditional. To do this, we used institutions: groups of human beings who together act in sufficiently predictable ways to be a source of hardness themselves.

“Institution” here is an extremely broad category, including:

- Legal systems
- Legislatures
- Police forces
- Governments
- Central banks and other monetary authorities
- Private banks
- Corporations
- Startups
- Religious institutions

The details of every case are different, but all of these share the same basic property of being used as a foundation for *sufficiently hard constraints* to enable social, political, and economic activity. Groups of humans who are motivated and organized to behave in a certain way, such that the institution itself outlives the participation of any particular group of people.

One key advantage of institutional hardness is that it is extremely *customizable*. The design space of possible casts built with atom hardness is very limited. But the design space of

possible casts built with institutional hardness is limited only by what rules you can convince people to enforce. When we needed hardness that could create more complex casts, we created what we needed out of what we had: people.

Thus we built institutions, and they provided sufficiently customizable casts to enable grander and more complex forms of human activity and coordination. We created casts that gave order to our societies, punishing antisocial behavior ("if you harm others, retribution will be taken"). We created flexible all-purpose systems that let anybody create casts related to commerce ("if you write down your promises in a certain format, we will force your counterparty to abide by these terms"). We created casts that spawned new assets, and provided sources of credit to growing economies ("this piece of paper is backed by the full force of the United States"). Using institutions, we built the hard foundations on which human civilization has grown and expanded.

This category extends to institutions who we might not always think of as rule-making bodies. Today, many private American corporations act as institutional sources of hardness that govern massive amounts of human activity. Facebook (now Meta) is an institution that controls and defines casts that apply to anyone using its platform, and is capable of enforcing those casts. This is also true of Twitter, Google, Apple, and other companies.

But institutional hardness has its limitations. Some of these have become more apparent, as the scale of human civilization begins to test them:

- Most institutions, and the things that they can make hard, are bounded by nation-state borders. There is one set of rules in one place, and another set of rules in another place. This introduces complexity and cost for a civilization and economy that spans many international borders. Relying only on institutions for hardness means access to that hardness is demarcated along nation-state boundaries.

- Many institutions depend on a central state of some kind. In some cases this means that the institution's function as a source of hardness can be undermined by the state that controls it. A judiciary that serves only as a function of political interests loses its *hardness*, because it can no longer reliably or predictably enforce consistent rules. Or worse, people *believe* these systems remain hard, and the state can exploit individuals' reliance and expectations when it chooses. And if the state falls, it might bring down all of the institutional sources of hardness that enable other parts of society to function, like commerce.

- Institutions are often very opaque. This makes it hard to tell how hard a cast actually is. It is very difficult for any person to predict precisely how a legal rule will be applied, and also very hard to predict how expensive it is to break an institution-made cast. We have built entire professions (lawyers) whose function is, in part, simply to guess at these things, and they are often wrong.

- Institutions are made of people and people are fallible. They are cruel, evil, stupid, and prejudiced. In most places, in most times, consistently throughout our history, institutions have only been reliable sources of hardness for some people, and not for others. Using institutions as a source of hardness for critical social infrastructure turns that infrastructure into a tool of oppression wielded by those who control the institution.

- Institutions are extremely expensive and difficult to create. The institutions that we rely most on for institutional hardness have today evolved over centuries and millennia. We cannot easily experiment, invent, or test new institutions, which means the rate of innovation proceeds slowly, over decades.

Over time, a greater and greater share of the systems that are socially important to us have become grounded in institution-hardness, rather than atom-hardness.

Consider the privacy of your personal communications. For most of human history, people had a strong expectation that their private communications could not be easily monitored (cast: “If I criticize the government while speaking to my family, the state will not learn about it”).

Until very recently, casts about your personal privacy had a strong foundation in atom-hardness. A private conversation in a home could not be easily monitored, assuming a listener was not physically present in your home. As technology enabled new kinds of communication, more and more of our private communications passed through a wire that was controlled by an institution.

But even then, the simple physics of it made it extremely expensive to do this at scale. J. Edgar Hoover did not spy on every American in the 1950s not because he didn’t want to, or because he wouldn’t have been able to get away with it, but because it was *simply impossible to do*. There were not enough FBI agents in America to spy on the private communications of every American. The cost of breaking the cast was too high.

But new technologies, and the architectures of control we built on top of those technologies, have radically reduced this cost. Today, the material costs of mass surveillance are cheap. The US government, and others, already conduct surveillance on a mass scale. Today, casts about your personal privacy are made *only* of institutional hardness, and they are broken constantly.

The rapid development of internet and software technologies have increased our dependence on institutional hardness - and made us more exposed to its failures. The problem with software eating the world, is that behind most software is an institution. We are hollowing out the infrastructure of civilization, and replacing it with forms of hardness that may not be up to the task.

The internet has let us build the early stages of a global, digital civilization. But today it is built on weak foundations. The internet we have reflects the shortcomings of institutional hardness. It is increasingly balkanized, carved up along nation-state boundaries. It is a fragile and unstable

foundation, as the individual companies that control it rise and fall. And most of it is owned by a handful of companies, controlled by a small group of people, who live in one country.

Blockchains

Satoshi's invention was a new source of hardness. It was the first *new source* of hardness that humans have invented in thousands of years.

Satoshi will not be remembered primarily as the inventor of Bitcoin. What Satoshi gave us was a kernel of something grander. It is the insight that through clever design, we can create systems bounded by cryptography, and fueled by simple human incentives, which together provide a source of natively digital hardness. Satoshi used this new source of hardness to create the first blockchain application: Bitcoin.

The same design that makes Bitcoin possible was extended and expanded into a broader design space, giving rise to the first and most widely adopted programmable blockchain, Ethereum. Just as institutions let us create hard casts with any arbitrary content that can be interpreted and executed by humans, Ethereum lets us create hard casts with arbitrary content that can be interpreted and executed by a computer.

Like Atoms and Institutions, Blockchains have strengths and weaknesses that make them appropriate for certain use-cases but not others:

- Blockchains are natively digital. They create hardness about software, data, and programs. Anyone with an internet connection can access, and interact with, a blockchain. This is also a limitation, because blockchain hardness depends on a sufficiently technological civilization that can maintain the internet and other infrastructure.

- Blockchains do not depend on any institutions, even if they do require human *maintenance*. Blockchain hardened casts will remain hard if a government fails, a judiciary succumbs to corruption, or a police force refuses to enforce the law. Blockchains do depend, to some degree, on the behaviour of groups of humans - for instance, to maintain client software that facilitates the protocol, or wallet software that lets humans interact with it. But these services can be performed by anyone, anywhere, anonymously - a loose, decentralized community of engineers. And it is not an exclusive right - anyone can create and maintain an Ethereum client.

- Measuring Blockchain *hardness* is extremely transparent. The specific cryptographic tools used by blockchains are public and available for study, and generally their properties are very well understood. The cost of attacking the system to subvert it - i.e. through a so-called "51% attack" - is known, and we can estimate it accurately.

- Blockchain casts are made using software. Software can be poorly written, include errors, and most people cannot read software or write it themselves. Without the convenience of human discretion (as exists in institutions), small mistakes that differ from our intent can be severe. On the other hand, the opportunity to learn to write and read software is available to anyone on earth. Anyone can upload a contract to Ethereum, virtually no one can write a law.

- Blockchains let us create new casts that, if they were grounded in institutional hardness, would require creating entirely new institutions. Anyone can create an asset, and define the parameters of that asset, in a way that would be impossible through any other means.

Understanding Blockchains as a source of hardness helps us make sense of the dizzying array of narratives and buzzwords that have been used to make sense of them over time.

Blockchains can be *credibly neutral* because their rules are transparent and verifiable, and casts about those rules are made hard by the blockchain itself.

Bitcoin is *digital gold* because a blockchain can create an asset whose supply is extraordinarily expensive to change. Casts about the supply of Bitcoin can be very hard.

Ethereum enables *composability between applications* because its basic properties and structure are *hard*. There is an extremely high assurance that the protocol will not radically change, and applications that are deployed onto mainnet will remain so. This lets developers build on what has already been built, with high confidence that those foundations will not crumble beneath them.

Ethereum enables *decentralized finance* because it lets us create software with *hardness*, providing the necessary foundation to build a complex web of intersecting relationships among parties across time and space. Traditional finance accomplishes a similar thing relying on institutional hardness (e.g. legal contracts).

Blockchains are *trustless* in the sense that they create hardness without any reliance on the behaviour of individual people or institutions. People also like to say that blockchains are "trust machines" or that they create trust. The mystery of these two contradictory explanations is unravelled once we are armed with the concept of hardness: blockchains are *trustless* in the sense that their hardness does not depend on *people*, but they are *trustworthy* in that they are still capable of producing hardness.

Ethereum enables *hyperstructures* - protocols that can run forever - because blockchains provide a native source of *hardness* that makes hyperstructures built on top of them extremely likely to persist into the future.

Ethereum enables *web3:* an ecosystem of web services, protocols, applications, and communities whose foundations are built primarily on blockchain hardness, rather than institutional hardness. A digital environment where people's identities, their possessions, their means of commerce, the way they govern themselves collectively, and the way they publish information to the world, all of it grounded in blockchain hardness, rather than institutions.

Humans have a natural *need* for hardness in the systems we use to coordinate through commerce, trade, governance, and communicate. One factor in the increasing backlash against big tech is that it has become clear that the institutions that control the internet today are *not* suitable sources of hardness, and the casts we try to make with them keep breaking.

We want a foundation for the global civilization we are trying to stitch together which is stable, firm, and reliable. One that will not change under our feet with each election, or the rise and fall of individual American companies.

4.

Think about Atoms, Institutions, and Blockchains like a system of checks and balances. Using them together to build our civilization's critical infrastructure makes it more resilient, and less exposed to the limitations of any one of them. They are a set of building materials that, used together in aggregate, make a stronger whole.

But that system of checks and balances is changing beneath our feet. Most of the time, we don't even realize it. The last protections of atom-hardness are crumbling as new technology lowers the cost of rights infringements that were once impossible at scale. The growth of a global digital civilization mediated via the internet has accelerated our reliance on institutions, stretching and testing them past their breaking point.

Blockchains will not replace institutions as our only source of hardness. But they will compete with and complement each other. Humans now have options: for the first time, there is a market for hardness that can be used to produce the complex casts necessary for modern civilization. Blockchain-hardness will be used where institutions falter or cannot go, and institutions will fill the gaps where human discretion or intent is necessary to create a system usable by humans. A new dimension of our politics has opened up. We will debate not only which systems to use - what forms of governance, what kinds of markets - but also what sources of hardness should be used to *construct* those systems.

What do we want our civilization to be made out of?