Endnotes on 2020: Crypto and Beyond

I'm writing this sitting in Singapore, the city in which I've now spent nearly half a year of uninterrupted time - an unremarkable duration for many, but for myself the longest I've stayed in any one place for nearly a decade. After months of fighting what may perhaps even be humanity's first boss-level enemy since 1945, the city itself is close to normal, though the world as a whole and its 7.8 billion inhabitants, normally so close by, continue to be so far away. Many other parts of the world have done less well and suffered more, though there is now a light at the end of the tunnel, as hopefully rapid deployment of vaccines will help humanity as a whole overcome this great challenge.

2020 has been a strange year because of these events, but also others. As life "away from keyboard (AFK)" has gotten much more constrained and challenging, the internet has been supercharged, with consequences both good and bad. Politics around the world has gone in strange directions, and I am continually worried by the many political factions that are so easily abandoning their most basic principles because they seem to have decided that their (often mutually contradictory) personal causes are just too important. And yet at the same time, there are rays of hope coming from unusual corners, with new technological discoveries in transportation, medicine, artificial intelligence - and, of course, blockchains and cryptography - that could open up a new chapter for humanity finally coming to fruition.

And so, 2020 is as good a year as any to ponder a key question: how should we re-evaluate our models of the world? What ways of seeing, understanding and reasoning about the world are going to be more useful in the decades to come, and what paths are no longer as valuable? What paths did we not see before that were valuable all along? In this post, I will give some of my own answers, covering far from everything but digging into a few specifics that seem particularly interesting. It's sometimes hard to tell which of these ideas are a recognition of a changing reality, and which are just myself finally seeing what has always been there; often enough it's some of both. The answers to these questions have a deep relevance both to the crypto space that I call home as well as to the wider world.

The Changing Role of

Economics

Economics has historically focused on "goods" in the form of physical objects

: production of food, manufacturing of widgets, buying and selling houses, and the like. Physical objects have some particular properties: they can be transferred, destroyed, bought and sold, but not copied. If one person is using a physical object, it's usually impractical for another person to use it simultaneously. Many objects are only valuable if "consumed" outright. Making ten copies of an object requires something close to ten times the resources that it takes to make one (not quite ten times, but surprisingly close, especially at larger scales). But on the internet, very different rules apply.

Copying is cheap. I can write an article or a piece of code once, and it usually takes quite a bit of effort to write it once, but once that work is done, an unlimited number of people can download and enjoy it. Very few things are "consumable"; often products are superseded by better ones, but if that does not happen, something produced today may continue to provide value to people until the end of time.

On the internet, "public goods" take center stage

. Certainly, private goods exist, particularly in the form of individuals' scarce attention and time and virtual assets that command that attention, but the average

interaction is one-to-many, not one-to-one. Confounding the situation even further, the "many" rarely maps easily to our traditional structures for structuring one-to-many interactions, such as companies, cities or countries;. Instead, these public goods are typically public across a widely scattered collection of people all around the world. Many online platforms serving wide groups of people need governance, to decide on features, content moderation policies or other challenges important to their user community, though there too, the user community rarely maps cleanly to anything but itself. How is it fair for the US government to govern Twitter, when Twitter is often a platform for public debates between US politicians and representatives of its geopolitical rivals? But clearly, governance challenges exist - and so we need more creative solutions.

This is not merely of interest to "pure" online services. Though goods in the physical world - food, houses, healthcare, transportation - continue to be as important as ever, improvements

in these goods depend even more than before on technology, and technological progress does

happen over the internet.

But also, economics itself seems to be a less powerful tool in dealing with these issues

. Out of all the challenges of 2020, how many can be understood by looking at supply and demand curves? One way to see what is going on here is by looking at the relationship between economics

and politics

. In the 19th century, the two were frequently viewed as being tied together, a subject called "political economy". In the 20th century, the two are more typically split apart. But in the 21st century, the lines between "private" and "public" are once again rapidly blurring. Governments are behaving more like market actors, and corporations are behaving more like governments.

We see this merge happening in the crypto space as well, as the researchers' eye of attention is increasingly switching focus to the challenge of governance. Five years ago, the main economic topics being considered in the crypto space had to do with consensus theory. This is a tractable economics problem with clear goals, and so we would on several occasions obtain nice clean results like the selfish mining paper. Some points of subjectivity, like quantifying decentralization, exist, but they could be easily encapsulated and treated separately from the formal math of the mechanism design. But in the last few years, we have seen the rise of increasingly complicated financial protocols and DAOs on top of blockchains, and at the same time governance challenges within

blockchains. Should Bitcoin Cash redirect 12.5% of its block reward toward paying a developer team? If so, who decides who that developer team is? Should Zcash extend its 20% developer reward for another four years? These problems certainly can be analyzed economically to some extent, but the analysis inevitably gets stuck at concepts like coordination, flipping between equilibria, "Schelling points" and "legitimacy", that are much more difficult to express with numbers. And so, a hybrid discipline, combining formal mathematical reasoning with the softer style of humanistic reasoning, is required.

We

wanted digital nations, instead we got digital nationalism

One of the most fascinating things that I noticed fairly early in the crypto space starting from around 2014 is just how quickly it started replicating the political patterns of the world at large. I don't mean this just in some broad abstract sense of "people are forming tribes and attacking each other", I mean similarities that are surprisingly deep and specific.

First, the story

. From 2009 to about 2013, the Bitcoin world was a relatively innocent happy place. The community was rapidly growing, prices were rising, and disagreements over block size or long-term direction, while present, were largely academic and took up little attention compared to the shared broader goal of helping Bitcoin grow and prosper.

But in 2014, the schisms started to arise. Transaction volumes on the Bitcoin blockchain hit 250 kilobytes per block and kept rising, for the first time raising fears that blockchain usage might actually hit the 1 MB limit before the limit could be increased. Non-Bitcoin blockchains, up until this point a minor sideshow, suddenly became a major part of the space, with Ethereum itself arguably leading the charge. And it was during these events that disagreements that were before politely hidden beneath the surface suddenly blew up. "Bitcoin maximalism", the idea that the goal of the crypto space should not be a diverse ecosystem of cryptocurrencies generally but Bitcoin and Bitcoin alone specifically, grew from a niche curiosity into a prominent and angry movement that Dominic Williams and I quickly saw for what it is and gave its current name. The small block ideology, arguing that the block size should be increased very slowly or even never increased at all regardless of how high transaction fees go, began to take root.

The disagreements within Bitcoin would soon turn into an all-out civil war. Theymos, the operator of the /r/bitcoin subreddit and several other key public Bitcoin discussion spaces, resorted to extreme censorship to impose his (small-block-leaning) views on the community. In response, the big-blockers moved to a new subreddit, /r/btc. Some valiantly attempted to defuse tensions with diplomatic conferences including a famous one in Hong Kong, and a seeming consensus was reached, though one year later the small block side would end up reneging on its part of the deal. By 2017, the big block faction was firmly on its way to defeat, and in August of that year they would secede (or "fork off") to implement their own vision on their own separate continuation of the Bitcoin blockchain, which they called "Bitcoin Cash" (symbol BCH).

The community split was chaotic, and one can see this in how the channels of communication were split up in the divorce: /r/bitcoin stayed under the control of supporters of Bitcoin (BTC). /r/btc was controlled by supporters of Bitcoin Cash (BCH). Bitcoin.org was controlled by supporters of Bitcoin (BTC). Bitcoin.com on the other hand was controlled by supporters of Bitcoin Cash (BCH). Each side claimed themselves to be the true Bitcoin. The result looked remarkably similar to one of those civil wars that happens from time to time that results in a country splitting in half, the two halves calling themselves almost identical names that differ only in which subset of the words "democratic", "people's" and "republic" appears on each side. Neither side had the ability to destroy the other, and of course there was no higher authority to adjudicate the dispute.

Around the same time, Ethereum had its own chaotic split

, in the form of the DAO fork, a highly controversial resolution to a theft in which over $50 million was stolen from the first major smart contract application on Ethereum. Just like in the Bitcoin case, there was first a civil war - though only lasting four weeks - and then a chain split, followed by an online war between the two now-separate chains, Ethereum (ETH) and Ethereum Classic (ETC). The naming split was as fun as in Bitcoin: the Ethereum Foundation held ethereumproject on Twitter but Ethereum Classic supporters held ethereumproject on Github.

Some on the Ethereum side would argue that Ethereum Classic had very few "real" supporters, and the whole thing was mostly a social attack by Bitcoin supporters: either to support the version of Ethereum that aligned with their values, or to cause chaos and destroy Ethereum outright. I myself believed these claims somewhat at the beginning, though over time I

came to realize that they were overhyped. It is true that some Bitcoin supporters had certainly tried to shape the outcome in their own image. But to a large extent, as is the case in many conflicts, the "foreign interference" card was simply a psychological defense that many Ethereum supporters, myself included, subconsciously used to shield ourselves from the fact that many people within our own community really did have different values. Fortunately relations between the two currencies have since improved - in part thanks to the excellent diplomatic skills of Virgil Griffith - and Ethereum Classic developers have even agreed to move to a different Github page.

Civil wars, alliances, blocs, alliances with participants in civil wars, you can all find it in crypto. Though fortunately, the conflict is all virtual and online, without the extremely harmful in-person consequences that often come with such things happening in real life. So what can we learn from all this? One important takeaway is this: if phenomena like this happen in contexts as widely different from each other as conflicts between countries, conflicts between religions and relations within and between purely digital cryptocurrencies, then perhaps what we're looking at is the indelible epiphenomena of human nature - something much more difficult to resolve than by changing what kinds of groups we organize in. So we should expect situations like this to continue to play out in many contexts over the decades to come. And perhaps it's harder than we thought to separate the good that may come out of this from the bad: those same energies that drive us to fight also drive us to contribute.

What motivates us anyway?

One of the key intellectual undercurrents of the 2000s era was the recognition of the importance of non-monetary motivations. People are motivated not just by earning as much money as possible in the work and extracting enjoyment from their money in their family lives; even at work we are motivated by social status, honor, altruism, reciprocity, a feeling of contribution, different social conceptions of what is good and valuable, and much more.

These differences are very meaningful and measurable. For one example, seethis Swiss study on compensating differentials for immoral work - how much extra do employers have to pay to convince someone to do a job if that job is considered morally unsavory?

As we can see, the effects are massive: if a job is widely considered immoral, you need to pay employees almost twice as much for them to be willing to do it. From personal experience, I would even argue that this understates the case: in many cases, top-quality workers would not be willing to work for a company that they think is bad for the world at almost any price. "Work" that is difficult to formalize (eg. word-of-mouth marketing) functions similarly: if people think a project is good, they will do it for free, if they do not, they will not do it at all. This is also likely why blockchain projects that raise a lot of money but are unscrupulous, or even just corporate-controlled profit-oriented "VC chains", tend to fail: even a billion dollars of capital cannot compete with a project having a soul

.

That said, it is possible to be overly idealistic about this fact, in several ways. First of all, while this decentralized, non-market, non-governmental subsidy toward projects that are socially considered to be good is massive, likely amounting to tens of trillions of dollars per year globally, its effect is not infinite

. If a developer has a choice between earning $30,000 per year by being "ideologically pure", and making a $30 million ICO by sticking a needless token into their project, they will

do the latter. Second, idealistic motivations are uneven

in what they motivate. Rick Falkvinge'sSwarmwise played up the possibility of decentralized non-market organization in part by pointing to political activism as a key example. And this is true, political activism does not require getting paid. But longer and more grueling tasks, even something as simple as making good user interfaces, are not so easily intrinsically motivated. And so if you rely on intrinsic motivation too much, you get projects where some tasks are overdone and other tasks are done poorly, or even ignored entirely. And third, perceptions of what people find intrinsically attractive to work on may change, and may even be manipulated.

One important conclusion for me from this is the importance of culture (and that oh-so-important word that crypto influencers have unfortunately ruined for me, "narrative"

). If a project having a high moral standing is equivalent to that project having twice as much money, or even more, then culture and narrative are extremely powerful forces that command the equivalent of tens of trillions of dollars of value. And this does not even begin to cover the role of such concepts in shaping our perceptions of legitimacy and coordination. And so anything that influences the culture can have a great impact on the world and on people's financial interests, and we're going to see more and more sophisticated efforts from all kinds of actors to do so systematically and deliberately. This is the darker conclusion of the importance of non-monetary social motivations - they create the battlefield for the permanent and final frontier of war, the war that is fortunately not usually deadly but unfortunately impossible to create peace treaties for because of how inextricably subjective it is to determine what even counts as a battle: the culture war.

Big X is here to stay, for all

X

One of the great debates of the 20th century is that between "Big Government" and "Big Business" - with various permutations of each: Big Brother, Big Banks, Big Tech, also at times joining the stage. In this environment, the Great Ideologies were typically defined by trying to abolish the Big X that they disliked

: communism focusing on corporations, anarcho-capitalism on governments, and so forth. Looking back in 2020, one may ask: which of the Great Ideologies succeeded, and which failed?

Let us zoom into one specific example: the 1996 Declaration of Independence of Cyberspace:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

And the similarly-spirited Crypto-Anarchist Manifesto:

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

How have these predictions fared? The answer is interesting: I would say that they succeeded in one part and failed in the other. What succeeded? We have interactions over networks, we have powerful cryptography that is difficult for even state actors to break, we even have powerful cryptocurrency

, with smart contract capabilities that the thinkers of the 1990s mostly did not even anticipate, and we're increasingly moving toward anonymized reputation systems with zero knowledge proofs. What failed? Well, the government did not go away. And what just proved to be totally unexpected? Perhaps the most interesting plot twist is that the two forces are, a few exceptions notwithstanding, by and large not

acting like mortal enemies, and there are even many people within governments that are earnestly trying to find ways to be friendly to blockchains and cryptocurrency and new forms of cryptographic trust.

What we see in 2020 is this: Big Government is as powerful as ever, but Big Business is also

as powerful as ever. "Big Protest Mob" is as powerful as ever too, as is Big Tech, and soon enough perhaps Big Cryptography. It's a densely populated jungle, with an uneasy peace between many complicated actors. If you define success as the total absence of a category of powerful actor or even a category of activity that you dislike, then you will probably leave the 21st century disappointed. But if you define success more through what happens than through what doesn't happen, and you are okay with imperfect outcomes, there is enough space to make everyone happy.

Prospering in the dense

jungle

So we have a world where:

- One-to-one interactions are less important, one-to-many and many-to-many interactions are more important.
- The environment is much more chaotic

, and difficult to model with clean and simple equations. Many-to-many interactions particularly follow strange rules that we still do not understand well.

- The environment is dense

, and different categories of powerful actors are forced to live quite closely side by side with each other.

In some ways, this is a world that is less convenient for someone like myself. I grew up with a form of economics that is focused on analyzing simpler physical objects and buying and selling, and am now forced to contend with a world where such analysis, while not irrelevant, is significantly less relevant than before. That said, transitions are always challenging. In fact, transitions are particularly challenging for those who think that they are not challenging because they think that the transition merely confirms what they believed all along. If you are still operating today precisely according to a script that was created in 2009, when the Great Financial Crisis was the most recent pivotal event on anyone's mind, then there are almost certainly important things that happened in the last decade that you are missing. An ideology that's finished is an ideology that's dead.

It's a world where blockchains and cryptocurrencies are well poised to play an important part, though for reasons much more

complex than many people think, and having as much to do with cultural forces as anything financial (one of the more underrated bull cases for cryptocurrency that I have always believed is simply the fact that gold is lame

, the younger generations realize that it's lame, and that$9 trillion has to go somewhere

). Similarly complex forces are what will lead to blockchains and cryptocurrencies being useful

. It's easy to say

that any application can be done more efficiently with a centralized service, but in practice social coordination problems are very real, and unwillingness to sign onto a system that has even a perception

of non-neutrality or ongoing dependence on a third party is real too. And so the centralized and even consortium-based approaches claiming to replace blockchains don't get anywhere, while "dumb and inefficient" public-blockchain-based solutions just keep quietly moving forward and gaining actual adoption.

And finally it's a very multidisciplinary world, one that is much harder to break up into layers and analyze each layer separately. You may need to switch from one style of analysis to another style of analysis in mid-sentence. Things happen for strange and inscrutable reasons, and there are always surprises. The question that remains is: how do we adapt to it?