Limpwar: Bitcoin is not digital warfare

Achim Warner

April 28, 2023

Contents

1

Introduction

Universally that person's acumen is esteemed very little perceptive concerning whatsoever matters are being held as most profitably by mortals with sapience endowed to be studied who is ignorant of that which is the most doctrine erudite and certainly by reason of that in them high mind's ornament deserving of veneration constantly maintain when by general consent they affirm that other circumstances being equal by no exterior splendor is the prosperity of a nation more efficaciously asserted by the measure of how far forward may have progressed the tribute of its solicitude for the proliferent continuance which of evils the original if it be absent when fortunately present constitutes the certain sign of omnipotent nature's incorrupted benefaction.

– James Joyce, Ulysses

Ground control to moon mission: Bitcoin is not a weapon.
Bitcoin is a peer-to-peer electronic cash system.
Always has been.

In Nakamoto consensus, proof of work was designed to provide a beacon without choosing a leader, in particular the leaderless environment for which Bitcoin was designed. It's not meant to be a tool for leaders to lead. Leaders have ample tools at their disposal, Bitcoin is for those who are neither leaders nor followers.

Nonetheless, some who have discovered Bitcoin in the last few years as a surging store-of-value asset have put forth arguments that proof of work will become a proxy for war. A summary of these arguments:

- Bitcoin will become **the** global reserve currency. Nations who have stockpiled bitcoin will be advantaged. Those who don't will be left out.
- Bitcoin mining, as a way of displaying energy use, is an effective means of physical power projection, a superior form of human organization and so can serve as a proxy for war.
- This is all going to be so bullish you won't believe it so you better buy lots of bitcoin right now.

In a free world, you can't force someone to ante in to a game with rules they find unfavourable. If one can choose to not play a high stakes game they are likely to lose, they will choose to not play the game. When the security mechanism for a system is up for auction those who can't win the auction won't cede any authority to this system.

Providing hashes to protect the network is an act of opting in to Nakamoto Consensus, a consensus that millions have opted into by transacting in or mining Bitcoin. If the territory becomes hostile, users can opt out. If someone has better options of transacting or storing value, they should and will use these. Bitcoin is designed for those who may not have better options for transacting or storing value or doing finance, not as a weapon of domination.

2

How does Bitcoin work?

A blockchain is a chain of blocks

– Peter Todd

Bitcoin is cryptocurrency. This means that the underlying units, which are abstract, made-up units, are sent from one user to another via signed messages. These message cannot be forged unless you are the owner of the private key, which is essentially a very long password. The cryptography has been understood for decades, but it wasn't until 2008 that Satoshi Nakamoto, whoever they are, combined ideas in a novel way to allow signed messages to make this work as a currency: Each Bitcoin originates in some block of transactions that is mined, each block appends to the previous block and puts all the transactions in order. Thus you can tell if someone sending you a Bitcoin has already sent the bitcoin to somebody else. Each time a miner mines a block, they credit themselves some Bitcoin, and then they can spend or sell that Bitcoin and that gets out into the ecosystem. Once you spend it, whoever you sent it to has to create a new transaction in order to send it to the next person. You can't spend it again, that's the point of having all the transaction sitting in order on a chain. If you try to send it again, the miners and nodes will ignore the transaction as it's incompatible with the current state of the chain.

So in order to use cryptography to create a cryptocurrency, you need some way to order the transactions, in a way that everybody can see and agree upon. There's an extremely easy way to do this; designate a few computers listening for these transactions, and publish these transactions on a ledger in the order they're received. This is quick and efficient, and for a cryptocurrency with the throughput of Bitcoin, it could be done for a few dollars a month using Amazon Web Services.

Of course, Amazon Web Services Coin would be unattractive for so many reasons. The problem solved by Satoshi was a means accomplish the ordering the without choosing a designated leader.

Satoshi Nakamoto's fantastic idea was to set up probabilistic auction for the right to create the next block. Each blocks orders the latest transactions, and the creator of the block is rewarded with bitcoin.

There were a combination of innovations that came together to form Bitcoin in 2008. One of these is this idea of proof of work: If you compute a mathematically deterministic function that has chaotic outputs, you can "prove" that you've spent a lot of energy by publishing hard-to-find hashes. It works something like this; if I want to prove to you that I've computed a trillion hashes, which are just expensive computations, I would present to you a one-in-a-trillion hash output. It's not exact, but on average it works well to demonstrate who is computing the most hashes.

An innovation in Bitcoin was the difficulty adjustment, which adjusts the proof of work needed in order for miners to find a block. The goal is to make blocks expensive to find: As long as blocks are expensive to find, they will come out in a steady drip so that everyone can keep track of what's going on from their own PC. It also forces miners to make sure that their blocks are compliant; otherwise they may spend greatly on energy when finding a block that the network will ignore.

Nakamoto consensus requires a miner must produce a "proof of work" in order to write the next block. Producing a proof of work is costly, it requires heavy computing power. But to incentivize the miners to do this, whoever writes the next block gets to write themselves a small number of Bitcoin. The difficulty adjustment, which occurs after roughly two weeks, ensures that blocks are not written too quickly - as blocks are written more frequently by more powerful sets of miners, the difficulty adjusts so that it becomes more and more difficult to write blocks. Thus on average blocks are only found about once every ten minutes.

Now it's possible that two miners could write the "next" block at the same time. It's also possible that a miner could deliberately choose to write a block that is not the "next" block, but rather a competing block: On the blockchain all blocks must go in order and each block must be unique: there can be only

one block 4567 and it must come after 4566. Block 4568 cannot be written until the hash from block 4567 is produced, in fact it's the hash from block N-1 that provides the "chain" link to block N. If two blocks are produced at the same time, there is a (usually temporary) chain split. Miners can decide which to append to; the next block must append one and only one of the two chains. At this point the tie is broken, and miners now follow the simple rule that underlies Nakamoto consensus: The longest chain is the correct one. (Technically, it's the chain with the most cumulative proof of work, which in practice is almost always the longest one.) Now a simple and elegant game theory kicks in. The only blockchain that matters is the blockchain with the most work. The only way to create a block on this chain is to create the next block, which will be the chain tip. Attempting to mine on a shorter blockchain will probably result in miners wasted costs, the Bitcoins created will exist only on a chain that nobody regards as useful. So miners continually front-run the chain and the chain moves forward. There is one chain, all the transactions are in order, and miners are always trying to create the next block on the system to earn more rewards.

In theory, someone with a large amount of computing power could begin mining an alternative chain from several blocks back. If they are lucky and powerful, eventually their chain may catch up and surpass the original chain. At this point, according to the rules of Bitcoin, the challenging chain is the now true chain, and miners will now switch to mine on this chain-tip, not wanting to be left out.

Why would someone do this? The classic example is the so-called double spend: Alice sends Bob a Bitcoin, essentially signing a message saying that the bitcoin she owned has been transferred to Bob. The miners mine this transaction into a block, and blocks continue after that and Bob looks and according to the blockchain, the bitcoin is now under his control. However Alice may be sneaky; suppose she then writes a transaction giving the same bitcoin to Charlie. Now miners and nodes who run the network would reject or ignore this as it's incompatible with the true chain, but if Alice is able to convince miners to go back to before the first transaction was mined, the miners can start a new chain which is internally consistent. If they mine faster they may be able to make their chain longer. At this point Bob looks and sees that he no longer owns the bitcoin, his transaction is now rejected and Charlie is considered the true owner

of the bitcoin.

2.1 Cryptography vs Proof of Work

The ticket takers will not board For the ticket takers are tied
– Low Anthem

It's important to distinguish between the roles of proof of work and cryptography. Proof of work is simply an arbitration mechanism that (pre-emptively) settles disputes when different orderings of transactions would result in different outcomes for participants. While we may one day see miner extractable value emerge on the Bitcoin blockchain, most imaginable scenarios in which a dispute needs to be settled involve attempts to double-spend.

Asymmetric cryptography is essentially free. It's also essentially unbreakable, when used as prescribed. Anyone can download a short python script to run asymmetric cryptography allowing them to decrypt, encrypt and check signatures from and to anyone in the world. These could include messages which promise Bitcoins, dollars, or goats. These messages may or may not have binding significance, but when a Bitcoin transaction is confirmed on the blockchain it represents a transfer of ownership of some amount of Bitcoin. Everyone can see this transaction on the blockchain and knows it is the unique transaction sending that particular coin. If we could trust parties to not double-spend, or if we have legal protections against double-spending, we wouldn't need an expensive mechanism such as proof of work.

When Bitcoin first emerged, people were using Bitcoin intentionally anonymously, and they didn't want to know who their counterparty was, or where they had been, and so in order to do this securely, double-spend protection is necessary to make sure that the kind Craiglist bro who just bought some items from you in the Walmart parking isn't going to double-spend. Now if you have a KYC relationship with an exchange who operates in your jurisdiction, there is no good reason to worry about double-spending, if you try to double-spend on your exchange, this might be considered fraud in your jurisdiction. Your exchange knows who you are and they can come after you.

It's impossible to create a valid Bitcoin transaction with the proper

keys. No amount of proof of work will change this. The validity of Bitcoin transactions are not protected by proof of work, they are protected by cryptography. Proof of work only serves as an arbitrator in the case that there are multiple valid transactions. It does not determine the monetary value for the coins created in the block: this is determined by the market.

2.2 Why does Bitcoin work?

It's a mystery to me; we have a greed to which we have agreed
– Eddie Vedder

Bitcoin works because people all around the world have collectively decided it is worth putting their energy and money into a cryptocurrency that is outside of the standard banking system and central banks. Bitcoin is essentially an opt-in, unenforceable contract, in which each participant implicitly agrees that the network they are engaging with is valuable and will continue to be valuable in the near future.

People had sought for this long before Satoshi created Bitcoin, the demand was there. Nakamoto consensus is how Bitcoin works, but why Bitcoin works is just as crucial: Bitcoin is something people want to use and have available so they retain the option to use it. If the demand were to dry up, the network would fail.

It was designed to fill roles in which the other available options come up short: Cross border payments, payments between parties that the government might choose to interfere with, a store of value that banks can not freeze in response to a court order, or simply payments that you don't want going into the standard databases. The demand for these and many other use cases is real and positive.

It's important to emphasize that part of the demand for Bitcoin is the demand for a currency that does not have a leader. If leaders could be chosen, it would be a much faster systems with much more bandwidth, and would not require the massive energy expenditures.

2.3 Can anyone control the blockchain?

It's in my nature

– The Scorpion

According to the consensus rules governing Bitcoin, if one miner is able to marshal over 51% of the hashrate, they can be successful (with high probability) in writing their own chain which contains only their blocks. This chain will be longer and have more work than other chains so will be *the* chain. The miners who create the blocks then "control" the blockchain in the sense that they can choose which transactions to allow on and in what order. They can't create new valid transaction with signatures they do not control, for example they cannot sign a transaction spending Bob's bitcoin if they do not have Bob's keys. They have the power of censorship: If Bob sends a transaction to Charlie, the 51% miner can simply ignore it if they don't like Bob or Charlie, or could ask for a bribe.

In the monopoly 51% attack (as opposed to a one-off 51% double-spend attack) a miner or group of miners begins mining blocks and ignoring all other blocks. They do this in the open, perhaps even loudly, declaring their intentions days or weeks ahead. Because their chain will be the longest, all efforts by other miners will go by the wayside. Other miners are forced to close up shop.

Of course, a monopoly mined blockchain is unattractive to most Bitcoin users, who generally didn't sign up for centralized money. At this point they may opt out of Bitcoin altogether, choosing a different cryptocurrency, or they may continue to use it. A third option is for Bitcoin users to find some extraprotocolar means of communication that rejects the longest chain - in fact, there is a command users can run called 'invalidateblock.' If enough users agree to invalidate the blocks of the monopoly miner, in other words agree to break the first rule of Bitcoin, their nodes will show that *the* blockchain is the strongest competing chain. This response is quite problematic - users would want to do it in a way that avoids creating a new set of de facto authorities, and this can be tricky without the longest chain rule.

There is an important principle here: **The longest chain is just one way to order transactions in order to keep Bitcoin functioning.** It's the best way if you are optimizing for decentralization, provided the longest chain is not

monopolized. If the non-monopolized option is not available, there are other options the community can choose. Being permanently and religiously bound to the longest chain rule affords any party who controls it the ability to abuse the chain.

Many Bitcoin users will claim that such an attack will never happen. Such an attack has not been seriously attempted and is unlikely to happen soon. (Attacks were threatened in the 2016-27 Blocksize war, but never carried out.) However, in the context of "Bitcoin as digital warfare" one must consider such attacks a real possibility.

2.4 Mining and the security budget

And eternity, my friend, is a long fucking time.

– Greg Graffin

When Bitcoin began in 2009 each miner who mined a block was rewarded 50 bitcoins. After a few years, at block number 210,000, this number was cut in half to 25. It was cut in half again at block 420,000 and again at block 630,000. It will be cut in half again in 2024 at block 840,000 to a block reward of 3.25 bitcoins per block. Students of mathematics will recognize this as a geometric series: Because the number of new bitcoins is cut in half approximately every four years, the total of all bitcoin created ever is 21 million. Now while this does mean that the total number is finite, at the same time this means that the amount of money paid to miners to mine blocks in decreasing in absolute bitcoin terms. While the value of a bitcoin has been trending up in dollar terms, the bitcoin rewards will continue to decrease. As of 2022 on order of $10 billion worth of bitcoin was produced. While this is a large number, it is considerably smaller than many numbers, in particular the defense budget of nations, the cash being held by major corporations, or the net worth of many individuals.

Miners also obtain revenue from fees, which are paid from transactors to the miners. Fees are typically determined by the market for transactions. Because the blocksize is fixed, miners will put transactions with the higher fees first, and this means typically there will be a market rate to put transactions on the blockchain. On average this number has not been very large in comparison to

the block subsidy.

Note that an individual mining at home is extremely unlikely to mine a block. Commercial miners each spend tens or hundreds of thousands of dollars over weeks: these are the competition. So the notion that individuals can meaningfully participate in the process by mining their own transactions is farfetched.

The security method for Bitcoin is essentially a probabilistic auction. Miners are bidding on blocks. Blocks are worth some amount of Bitcoin. However if they are ever worth more than the Bitcoin, the auction is no longer for Bitcoin - it will be for the leverage provided by being in charge of the security.

2.5 Who controls Bitcoin, the nodes or miners?

If it takes a bloodbath, let's get it over with,
– (California Governor) Ronald Reagan

This question of power versus miners is more subtle than many afford. Both are somewhat necessary for a functioning ecosystem. Miners have the leverage to destroy the consensus mechanism.

It's somewhat like the relationship between capital and labor. A union can threaten to strike, the capitalist can then decide if the striking coalition determines an economically significant force. If the capitalist can bluff well or find enough folks to cross picket lines, the union's threats are weakened. Obviously, there is no universal principle declaring unions have or do not have the upper hand; one would not expect there to be such universal principle deciding between nodes and miners.

A similar relationship exists between corporations and consumers. Consumers can threaten to boycott corporations, but at the end of the day, they may have little choice without collective organization or viable competition.

Does Bitcoin have competition? Many claim it does not. Perhaps paradoxically, this would give the miners a decisive edge. If miners make a move that nodes do not like, they can only opt out. If the options for opting out are limited, they may be forced to stay in.

3

Power and Property

Strange women lying in ponds distributing swords is no basis for a system of government. Supreme executive power derives from a mandate from the masses, not from some farcical aquatic ceremony.

– Dennis, (Monty Python and the Holy Grail)

Animals have used intimidation through power projection as a method to organize themselves and create pecking orders. The most powerful animals project power, and this establishes dominance and discourages attack. Power, taken literally, are given in units of watts which are joules per second. One *could* take this quite literally, but this would be a bit silly. An animal's power is not literally how many watts they are able to project. An animal's ability to expend wattage correlates with their ability to cause you harm, but this is not a direct relationship.

Rigid power structures enforced by the threat of violence can result in less violence: if each animal knows their place in the pecking order and do not challenge those above them, violence within a group can be minimized.

Humans, triumphantly, have created abstract power structures; these structures are enacted without continual physical violence. These structure also lead to less animalistic forms of authority: Kings are kings because their father was king, presidents may become president simply by winning an election according to rules determined in a 240 year old constitution. Superior physical specimens like John Cena yield power to aging members of the 5'11 club like Xi Jinping. This is not a perversion of nature; it's a major advance. Such abstract power structure are clearly imperfect and have resulted in many poor leaders and exploitation by self-serving leaders. However, these structures have also allowed the human race to develop civilizations in which we have artists, philosophers,

social media influencers, and C++ programmers. It's a better world: we can all specialize and contribute without puffing up like a blowfish every time we encounter another human.

3.1 Property rights

> *It appears that sandwiches have developed an unfortunate habit of getting nicked from the fridge. To be fair, sometimes it's me who's doing the nicking*
>
> – John Conway *Princeton, NJ.*

Blockchain can confer property only in the situation that individual agents who control property in meat-space agree to be bound by the blockchain as a arbitration mechanism. This requires an abstract power structure that defers to the blockchain. In theory, a government could require that, say, homeowners register their home on a blockchain, rather than with the county clerk. This would be a silly Rube Goldberg machine: If you can't trust the county clerk to not give your home away, there are basic corruption issues at play in your county.

If someone comes to your house and claims they own your home, you want to impose physically prohibitive costs to make them leave, or you want to appeal to an abstract power structure to impose physically prohibitive costs - usually this abstract power structure will have more coercive means at their disposal. If the intruder persists, the abstract power enforcers will use abstract methods to arbitrate: This would typically involve the county registrar, and perhaps the abstract court system, which imposes abstract law. The arbitration method could also be a blockchain, provided that at some point the rightful owner of the home had deeded it to a transaction on the blockchain. Of course, this would have to be recorded with the county clerk, otherwise how would anyone determine which of any of the blockchain transactions have anything to do with your home? Clearly, people who do not own a home cannot simply declare they own a home by creating a transaction.

It's not obvious that putting control of property (other than bitcoin or blockchain native things like NFTs) on a blockchain would be a good idea. You

have to ask: who will accept that I own this property if it's on the blockchain, that would not have accepted my ownership without it? If you're traveling to Kenya from Japan and need some means to transfer money, obviously Bitcoin is a solution. The ledger is respected in both places. Bitcoin is also a fungible token used by many people. But your house? If you live in a place of law and order, your records at the county registrar suffice. If you live in a place without law order, there's little the blockchain can do for you.

Now for the sake of argument, suppose that there may be some efficiencies gained with blockchain technology - there may be a day in which the deed to your home is registered on a public blockchain instead of at your county registrar. But this would be done with cryptography, and unless you've double-spent your home, there is no way anyone with control over the chain tip can send your home somewhere else, unless they erase a chunk of the chain that predates your acquisition of the home. So let's take this hypothetical situation: You bought a house, and you live in it, and then a geopolitical adversary erases months of the blockchain (winning a temporary hashwar) and you no longer own your house. The previous owner is able to double-sell your home: They sell your home to someone else, and now someone else owns your home. Now if you've agreed to this determination of ownership, in a world where hashwars pose a credible threat of rolling back parts of the chain, you are an idiot.

This situation is already farcical enough, but we can also ask who is going to buy your home from someone, given that a foreign adversary may have just allowed this to be stolen. Do you walk into a home in Wyoming and declare it's yours and not expect to be shot at? If you're bringing the police or courts to help you, we're in a situation in which local police and courts are doing the bidding of people in China, Iran or Russia or whoever attacked the blockchain, hence local authorities have ceded authority to global adversaries, which is very un-sovereign.

If there is real possibility that something important to you can be stolen by putting that thing on a blockchain, you will not put that thing on a blockchain, unless you have some special motivation to expose yourself to this risk.

One situation in which a blockchain makes sense: Your county could choose to run a centralized blockchain, protected by cryptography. This would not require proof of work. Proof of work would be not only inefficient, but would

put the security of the system up for auction to anybody in the world.

People in meat-space control property. If someone walks into your home in a hostile manner, you can't use the deed to your home to force them to leave. You have to call the police, or use force available to you. If you have no way to threaten the attacker with force, you are out of luck until the forces materializes. The deed to the house does nothing.

Importantly, if the government comes into your home and says they are going to take it, the best the deed can do is convince a judge in a court of law that they cannot. In law-abiding countries with good balance of power this may stop the government from taking your home, but in others it will not. The latest chain-tip has the same power. While you may have a contract which is signed on the blockchain declaring you own a certain piece of property, if someone takes that from you, you still need to go ask a court or law enforcement for relief. The actual blockchain does nothing.

3.2 But what if we link hardware to the blockchain?

Milk was a bad choice.

– Ron, *Anchorman*

Now suppose, maybe, there was a device that could only be controlled by the blockchain? Like, suppose you put a security device on your car, so that the only way that it can be unlocked is with a signed transaction? What about ~~Ethereum~~ if some clever people figure out how to use blockchain to create a world computer that all devices are connected up to maybe?

The main security mechanism at play in software is cryptography. **Cryptography does not rely on proof of work.** Proof of work is no more than an arbitration mechanism to determine an absolute order of transactions. It is not something that can create or revoke valid cryptographic signatures. Because the blockchain could be in flux for innocent as well as malicious reasons, it would be silly (and also needlessly complicated) to write high-stakes security software for devices that depend on the blockchain somehow, for applications that are not directly related to Bitcoin itself.

Indeed it's possible to engineer a car that requires cryptography, but remember blockchain validity is relative: The question of which blockchain is correct is only determined by comparing all possible blockchains and looking for the one with the most proof of work. You cannot determine today a criterion for whether information that appears tomorrow is from the correct blockchain - it could be from an inferior blockchain which contains a transaction that is a double-spend of a widely accepted transaction. In particular, you cannot determine today the condition for winning a hashwar tomorrow.

Happily, there's a much easier way: Simply engineer the device to accept any signed transaction that the current owner provides - in the order that the device receives it. No blockchain involved, and no possibility to double-spend.

It's possible to require proof of work to give access to a network or system, this is like the proof of work that existed prior to Bitcoin - it provided spam deterrence. But this is only necessary for un-permissioned systems. By design, un-permissioned systems allow access the network anonymously. **Proof of work was to be provided precisely so users did not need to reveal their identity.** In contrast, you do not want anonymous users to access your home router, your Roku, your phone, your computer or anything else that belongs to you. In these cases, a locally stored, hashed and salted password will be sufficient. There's no reason to demand a proof of work for people accessing your phone, because you don't want other people accessing your phone, full stop. Also you don't want to demand proof of work from yourself, (unless you are embarking on some sort of technology fast) as this would impose cost on yourself and nobody else. **Nor do you want to make access to your personal computers, phones, or networks a market auction.** Cryptography (in particular passwords) is sufficient.

3.3 What about future innovation?

> *I think Bigfoot is blurry, that's the problem. It's not the photographer's fault. Bigfoot is blurry, and that's extra scary to me. There's a large out of focus monster roaming the countryside*
>
> – Mitch Hedburg

Bitcoin is a breakthrough: It demonstrated that decentralized money can exist, not only theoretically, but empirically and demonstrably. Bitcoin is something that is socially supported. While quite clever, Nakamoto consensus is a relatively straightforward protocol that accomplishes what it set out to do quite well. **Bitcoin does not do every novel thing you can think of, just because Bitcoin is novel.** If there's a need for someone to invent something in the future for your thesis to be true, you probably don't have a good thesis.

3.4 Logical versus physical barriers in cyberspace

I can't. I - I - simply can't.

– Cletus *The Simpson's Movie*

Proof of work can protect against certain kinds of brute force denial-of-service attacks, when the surface being attacked is open to any attacker. However, proof of work is completely unnecessary to secure a system against forbidden attackers - this is a job for cryptography. If only authorized folks have the electronic credentials (passwords, 2FA, etc.) then no unauthorized person can access the system, unless they are able to physically coerce an authorized user, or, are able to exploit a flaw in the security software. For systems like Bitcoin where the security is relatively simple, it's practically impossible to steal, say, Satoshi's Bitcoin. This is not due to lack of proof of work by the would-be thief, it's due to the fact that Satoshi's keys belong to Satoshi.

In fact, nearly every digital security system we have operates this way - proof of work only is used when the system intended for use by anonymous users. If the lack of proof of work rendered a system insecure, nearly every system would be insecure. Proof of work does not significantly increase the cost-to-benefit ratio of a password secured system. The cost of moving Satoshi's coins is near infinite, because there is no known method for obtaining Satoshi's keys. If the we add proof of work to that, this only slightly increases the cost.

Adding proof of work to a system secured by cryptography is like putting chicken wire around a castle. It's a tiny barrier to overcome.

4

Actual game theory

Ours is a world governed by the aggressive use of force.

– Rush Limbaugh

4.1 Coalitional Game Theory

Coalitional game theory is a sub-field of game theory which considers games where players have interests that can be sometimes divergent and sometimes convergent, and the outcomes of the game are determined by which players decide to form coalitions. The assumption is that they can negotiate and perhaps even make threats.

Game theorists study *solutions concepts.* These are types of outcomes of games that seem reasonable according to one set of criteria or another. For example, in many traditional two player non-cooperative games, the Nash equilibrium is the most well-known solution concept, as it describes a situation where all players have chosen the best move provided no other players alter their moves. For most of the interesting games in coalitional game theory, you won't find something like a Nash equilibrium, because now you have to consider legal moves in which multiple players can switch coalitions and rebargain.

A classic example of a coalitional game is the weighted majority game, where each player has a certain percentage of the vote, and any majority coalition wins. Such games are often described by payoff tables which describe how much each coalition would win for themselves (in utility units, generally speaking.) Bitcoin mining tracks this closely, but to give it proper care you have to consider that a grand coalition may (tacitly) decide to collude by (tacitly) agreeing to not

collude. For Bitcoin, this might be a wise choice; Agreeing to collude could damage faith in the ecosystem. So even if three miners with 20% hashrate each are open to communication, they may make the decision to never seize control over the network.

One can model the motivation to collude easily as an inequality that holds or does not hold. The reward that a set of majority miners get depends on whether or not people care that miners have colluded to take over the blockchain. Under typical operations, profits to miners are incredibly low, even though revenues may be high. So if miners are making 5% profit margins, and miners with 60% of the hashrate decide to take over, they're now getting 100% of the revenue but collecting this is only costing them just under 60% of the cost, so their profit margins have leaped quite considerable. Of course, this is provided that the price doesn't collapse: If the revenue drops by 40% the miners are no better off. However, if the price falls by 40% and no more, they could continue to collude, making arms agreements to slowly reduce their hashrate, and this would allow them to increase their profit margins by quite a bit.

This hasn't happened yet, largely because people believe that it would be a disaster for the ecosystem and miners with the power to enter such collusive agreements would be destroying their business model. However, this becomes much more interesting when business' reliance on the blockchain becomes agnostic of who is running it. In this case, if miners can predict that this catastrophic drop in price never would materialize, they are wise to start looking around for partners in collusion, especially considering that if you are left out of the colluding pool, your revenue can go to zero.

Revenue isn't the only reason to collude, and this important when modeling collusion of miners as a coalitional game. Miners in a single jurisdiction may have more convergent interests, or they may be incentivized by their local authorities to collude if their collusion results in censorship that is pleasing to the authorities. The composition of a coalition may also affect how the market responds: Wealthy Americans who hold Bitcoin may trust that a majority coalition all housed in Texas will remain "freedom loving" while maintaining much more suspicion for a coalition housed in China. Economic allies may wish to collude to control the blockchain, if they feel this will allow their economies to thrive, and they would like to have the ability to censor foreign bitcoin transactions at

will.

The payoffs could change rapidly with world events. For example, if the majority of mining was done by Western nation-states in February 2022, there may have been a quick agreement to collude for the purpose of enacting sanctions on Russia. Given the spirit at the time, it's hard to determine how unpopular this would have ended up being. Undoubtedly a similar situation will arise in the future. A majority takeover may happen during some geopolitical event in which it is deemed necessary, or *the right thing to do* according to the bien-pensants, and might even be sold as a temporary measure.

4.2 Backwards induction

Each day is better than the next!

– Woogie, *Something about Mary*

Backwards induction, together with game trees, is an important tool in game-theoretic analysis. Typically this involves considering a player's possible actions, thinking of other players subsequent responses to the actions, and so forth, until some sufficiently terminal set of events is arrived at. This is a natural reasoning process for many humans, but people often struggle to take this more than 1 layer deep.

Consider for example, the Market Fragility Hypothesis, which is often referred to as part of Bitcoin's security model: "Miners will not monopolize the blockchain, because this would cause holders to sell, therefore miners will not attack the blockchain."

Unfortunately this is not deep enough: One must actually question the assumption that holders would sell. Would they? Selling in mass would be a horrible outcome, for millions of people who have used Bitcoin as a store of value. They instead consider option B: Continue with the collective delusion that Bitcoin has value, and not sell.

It's also important for situations in which international powers attempt to control the blockchain. You can construct a tree. What would happen if China monopolized the Bitcoin blockchain? US users could abandon Bitcoin, could

continue to use it, or could develop an alternative that doesn't 100% rely on pure proof of work.

5

Will nations go all in on Bitcoin?

Our love is all of God's money

– Wilco

Some have suggested that Bitcoin will usurp the role of US Treasurys and gold, becoming the asset that every central bank holds in their treasury. There's some serious problems with this idea. The issue available to uninitiated people walking in the streets is the observation that Bitcoin is speculative, people are always herding to get it one year and then dumping it the next. The roller coaster may seem to be going up, but if ever it reaches a maximum capacity (locally in time), the speculative mania will work in the opposite direction; nations who FOMO'd into Bitcoin for speculative reasons will be equally as motivated to acquire as many US Treasurys as possible before the price drops. Generally speaking, stability is one of the main goals of any government, and Bitcoin does not fit this role.

A slightly more knowledgeable observer might point to another problem: security and the security budget. The block subsidy in 2053 (when a 30 year treasury bond bought today matures) will be about 3.5 Bitcoins per day. Yes, perhaps the price will have gone up by 2053 and also, blockspace could enjoy higher demand and transaction fees will make up some of the slack, but the ratio of market cap to security is expected to be quite a bit worse.

A couple things to note: Even if the price goes up, this doesn't help the fact that MicroStrategy's holdings today are about 100 times the annual block reward in 2053 - the ratio of damage to cost by an attacker becomes huge, and can be arbitraged by a resourceful attacker. Second, transaction fees can't pick up that much if the price is high. There are insane suggestion that banks and large financial institutions will be regularly paying $20,000 per transaction to

settle accounts. This is silly, just because banks have lots of money does not mean they want to waste it: Banks settle all the time with the Fed for a few cents a transaction. Every dollar spent on transaction fees in spent by miners, burning electricity into the ground. This sucks value of the ecosystem, especially at ridiculous valuations.

Now it's not clear the day or the hour when security may become an issue. But if it does, nations have a few choices. One option is to try to get out while the getting is good, front-running a market crash. You prefer to sell first, before everyone else. You also realize your adversary wants to front run everybody as much as you do. Another option is to build up a mining arsenal to protect the blockchain, perhaps at a loss, but this requires further considerations of how other nations will respond. Another option is to ignore it and hope everything is fine.

Any national treasurer for a significant world power who looks to the horizon and sees such a situation even remotely possible will take steps to not be involved in it. Some small nations may take the risk. If they have nothing to lose, and much to gain, it might be worth this risk. A small nation may be able to get in and out without moving the market.

5.1 What if nations build hash forces?

> *He asks the girl, if they can both sit in the chair, but he doesn't get nervous, she's not really there.*
>
> – They Might Be Giants

National defense budgets would destroy the naturally competitive market for hashrate.

When functioning properly, miners will spend slightly less on producing hashes than they expect to recover in rewards. If they determine that the hashrate is too high relative to the price, they will stop mining. Miners are usually rational and profit-motivated. Now nation states who have national security goals aren't profit motivated, and will err on the side of overspending. Recent security budgets have been an order of $10 billion per year. This is a small fraction of the US department of defense budget, which is closer to $1

trillion. If the US decided to put 2% if their DoD budget into mining, this will make it unprofitable for almost every profit-motivated miner. The result will be that only the US is mining Bitcoin. Unless, of course, China and Russia and India etc. are all mining bitcoin, in order to protect their interests.

Now by this point there are no individual miners or profit motivated corporation mining bitcoin, only defense departments. **Who wants to put their money in this?** Most people who use Bitcoin would say this situation is very bad. The global military industrial complex controlling Bitcoin is pretty much the opposite of why Bitcoin was created.

Some may argue that this creates a perfect tension that keeps the network free and uncensorable. This is not so clear. Consider some simple observations from classical and coalitional game theory. First, consider any given nation's motivation to spend billions of dollars to contribute to this game. For any nation who would only provide a small fraction of hashrate, they are not expected to contribute a discernible edge, unless there is a coalition who is near 50% of the hashrate. So what we observe is a classical free-rider problem, if there are many small nations with no incentive to contribute, they won't. But then we say obvious things, like, but won't the larger nations demand that the smaller nations do their share? Well yes, just like in the fiat world, nations will form NATO, TPP, OPEC, etc. Groups with similar interests will form treaties and will end up operating as a unit. Very quickly, we have a very small number of economic interests, each acting as a unit, controlling a percentage of the hashrate. Such a world would mirror the power arrangements we have now. The instant any minority member acted out of line, the experiment would be over: Common interests would collude if that gave them significant advantages.

Disputes happen, wars happen, tension elevate. But this would not escalate in the sense that world powers would be increasing their hashrate to show force, they would be using traditional diplomacy, shoring up alliances, shaking hands, marrying princes to princesses, etc. It's a political war just like it's always been, but now any colluding interest with enough hashrate can shut down the blockchain at will.

Now maybe this is good; Russia decides not to invade Ukraine for the 6th time because they don't want to be sanctioned by nations with 80% of the hashrate. This could happen. Or, Russia could dump their Bitcoin on the

market and then invade Ukraine anyways.

In the olden days when people fought wars, they would try to control, bridges, channels, ports, and they would burn or destroy the ones they couldn't control. These principles don't change; they apply as well to money. Even small disputes with minor saber-rattling could involve a jockeying of position for the blockchain.

Ultimately however, there is likely to be a dominant superpower who has the most control, or has the influence to marshal the most control. In this case, their global adversaries are unlikely to even participate, or will have a centralized fork ready to go.

If one nation believes another nation will win a hashwar, they will not make themselves vulnerable. More likely, the nation will choose a time to rugpull their global adversaries, to maximize lulz.

5.2 Home field advantage is adaptive

> *Rest assured, our father, rest assured. The land is not to be sold.*
>
> – The Good Earth

Peace-loving folks will fight to the death to protect their home and family. Most humans would not hesitate to act aggressively when defending their own home, yet only a small proportion of humans would invade each others home. This is not a paradox - knowing that others will behave aggressively when encroached upon provides a stability in which only the most desperate find it rational to attack. From an evolutionary perspective it appears this is adaptive. To throw it all out into the an open field does not appear to be adaptive. Defense and offense are not the same. Humans want to be able to defend their own territory without attacking others.

There is a difference between offensive and defensive structures. Cannons attack while castle walls defend. The fact that cannons can also defend does not mean that castle walls are offensive weapons.

We have evolved in world dictated by physical space. Humans and other animals stake out their own domains, where they operate freely and fruitfully. Wars are fought on battlefields. Bringing the war to everywhere is a horrible idea.

6

Permissioned bitcoin as a failure mode

6.1 Hashing is nothing like other arms races

> *I'm in a knife fight here, and I'm holding a dildo made of American cheese.*
>
> – Gil, *HBO's Succession*

Imagine two rival nations, side-by-side. Nation A develops swords and spears, then Nation B must develop these in order to protect themselves. Nation A develops guns and cannons, so also Nation B must develop guns and cannons in order to protect themselves. Nation A develops airplanes and missiles, Nation B builds up an air-force and a missile facility. Nation A stacks up on Bitcoin, Nation B *bans Bitcoin.* Now years go by, Nation A has $2 Trillion in Bitcoin, Nation B does not. What's the difference, who has the tactical advantage? It might seem relatively little, but suppose tensions escalate without coming to nuclear war. Nation B can conscript local fabs to build an arsenal of miners, perhaps $10 Billion worth. With these miners, they begin to attack Bitcoin, throwing the $2 Trillion store of value into question. Whales in Nation A are furious, and not wanting to see their wealth evaporate, they demand their leaders make concessions to nation B that will deescalate the conflict. This is a clear W for Nation B.

If your nation's economy depends on Bitcoin and mine does not, you have a vulnerability that I do not have.

6.2 Permissioned bypass

> *It is easier for a camel to go through the eye of a needle, then for the rich to enter the kingdom of heaven*
>
> – Jesus

Now Nation A is scrambling, as trillions of dollars of wealth is under attack. If they are bound to proof of work, they have no choice but to fight back against Nation B with proof of work. This could be a war of attrition, this could cripple Nation A if they have not prepared for it.

OR.

Nation A could simply send out a software patch to everyone using Bitcoin, which invalidates all blocks that are not mined by a Nation A approved set of miners. Nation B is spending billions of dollars mining blocks. Nation A ignores these, and continues following a proof of work protocol that only allows approved miners in Nation A. That's fine - these corporations Unrest, 10K, Philistine etc have been mining for years and have the public trust, and none of these have more than 15% of the hashrate. Home miners are temporarily excluded, but they can be added to the approved list if they fill out a few forms saying they aren't from Nation B and will be getting their blocks slashed if they get up to any shenanigans. EVERYTHING IS FINE.

This is called a permissioned bypass.

6.3 What happens if someone wins?

> *What? I didn't break it. I was just testing its durability*
>
> – Happy, *Happy Gilmore*

If Oceania wins a hashwar, EastAsia and NearAsia softfork their own chain or chains. This is a better alternative to watching supply chains brick and watching massive civil unrest. Bitcoin forks. Life continues in EastAsia, Oceania and NearAsia, just on separate blockchains.

6.4 Permissioned bypass is a cheap takeover.

Waste is a terrible thing to mind.

– Dan Quayle

Suppose Bitcoin gets really super bullish, and everyone is holding Bitcoin and transacting in Bitcoin, including all the major financial institutions, central banks, and everybody. Transaction fees are huge, and the security budget is $300 billion per year. Double spends don't happen, because most of the parties ponying up $10,000 to pay the transaction fees are wealthy corporations and individuals, people who have 'family offices', and not clandestine transactions happening in a Walmart parking lot. So what's the point of security? This $300 billion is a ton of money that's coming directly out of the economy. It's not protecting against double-spends, it's protecting against a single miner coming in and taking over the network. This is a lot of money to be spent on decentralization.

Now suppose in this super bullish scenario, next year, at Davos, the bankers get together and say "look, there's $300 billion of fat we can trim, this is money we're paying to settle transactions with each other, but we all know each other. We're disruptors, we can solve this." They also own stock in all the mining corporations, or are the mining corporations themselves. They then issue a statement that as of next November 1, Bitcoin will be only mined by a list of permissioned miners, chosen by the good folks at Davos.

There's nothing the economic minority can do, at this point the financial institutions are majors players in Bitcoin, and if anyone tries to carry on the legacy Bitcoin, they get left out of the major gains that are happening every year as fiat continues to print to ∞ . They could sell, but to whom? So they stick with the Davos Bitcoin. Meanwhile the miners come to an arms agreement about hashrate reduction, slowly winding costs down so that costs become minimal and profits are huge.

If major corporations own and mine Bitcoin, then they are both the miners and "the nodes" (in the meaningful economic sense) and cannot be resisted.

This is not a fantastical situation, it's the most likely one if Bitcoin were to usurp the place of gold and US Treasurys. It's hard to imagine that all the

masters of the universe would abandon the legacy financial system so they can take a back seat on the pleb bus. They would only abandon legacy finance if they see an opportunity to take it over. **This is the fallacy of thinking that just getting the financial institution to FOMO into Bitcoin will change the financial institutions and not Bitcoin. If the value becomes dependent on the financial institutions, the financial institutions control Bitcoin.** If you invite all of the cool kids to your party, promising lots of good booze, they might show up and drink your booze, but they're not going to sit around listening to your rare vintage Vashti Bunyan record collection, they're going to get a hold of the bluetooth and play their top 40.

7

Bitcoin is not the Basilisk

Let us weigh the gain and the loss in wagering that God is. Let us estimate these two chances. If you gain, you gain all; if you lose, you lose nothing. Wager, then, without hesitation that He is."

– Blaise Pascal

Bitcoin is voluntary. Bitcoin is opt-in. It provides an option for people who are not best served by other available options for storing or transferring value.

At no point in the future will this change, despite claims made by perma-bull olympians. These arguments often claim that Bitcoin will become so valuable that it will consume everything, anyone who chooses not to use it will be left destitute.

First it should be noted there's a thing called Gresham's law: soft money circulates faster and thus gets used. Hard money gets less used, so hard money doesn't become the currency for everything. Somehow along the way a few people have decided Gresham's law is the opposite of Gresham's law (there's a name for this, Thier's law) but Gresham's law is more famous because it's more likely to be a dominant principle.

Also, some argue that societies who use Bitcoin will thrive and brutally destroy everyone who doesn't. But it's hard to imagine a situation in which the nation that sits around and stares at their money invades and destroys the nation that uses their money for economic activity. A productive economy is not about what is held, it's about what is done. But members Bitcoin's Most Bullish club claim that Bitcoin is so obviously useful that eventual everybody will see the infinite bullishness and succumb.

This is the Basilisk Theory of Bitcoin. It's a circular reasoning that starts with the observation that Bitcoin will conquer the world, and then using back-

wards induction, once everyone sees that Bitcoin is conquering the world, all are going to want to buy Bitcoin, so as to not be left out. Bitcoin will mercilessly crush everyone who does not get on board, if it does take over, so everyone alive will make Pascal's wager, realizing that everyone else is also about to make the same wager. Obviously, the powerful and rich people who see their power slipping if they don't buy Bitcoin, will buy Bitcoin, and Bitcoin takes over the world. Therefore Bitcoin takes over the world. Some versed in logic and situated outside of this particular loop may point out that this is perhaps a circular reasoning, which it is. In order to get in the loop you need some sort of leap of faith, some statements like "the hardest money ever created" or "forever, Laura"

7.1 Most people aren't in the forever loop

What's this? Broken. Huh? Sorry about that, sport.

– Dad, *The Polar Express*

Bitcoin is useful for some people. It can be a lifesaver for people in authoritarian regimes. But it's not for everybody. Bitcoin is clearly not for billionaires like Warren Buffett or Bill Gates. They've made their opinions clear.

We should not conflate the usefulness of Bitcoin for some people with the universal usefulness of Bitcoin for everybody

The idea that one day not only will Bitcoin be a global currency and but will be *the* global currency that every person must use is a concept called *coercive hyperbitcoinization*. Coercitive hyperbitcoinization is an attractive conclusion for someone who has come late to Bitcoin and wants to build the most bullish bull market case ever.

Coercive hyperbitcoinization is nonsensical and unfeasible: it would require a mass formation psychosis in which everybody, suddenly, after years of resisting FOMO, commits in a tarantistic mania. It's not going to happen. Don't worry, there are less insane forms of hyperbitcoinization that could still occur.

Coercive hyperbitcoinization is completely undesirable and fundamentally against Bitcoin's core principles of optionality and free market competition.

8

The map is not the territory

It's snowing on the goddamn map, not the territory, you dick!
– Infinite Jest, Eschaton Episode

Bitcoin has existed for a decade and half, proving the viability of a decentralized currency. At the center of this, proof of work has functioned as a decentralized arbitrator determining who gets to write the next block. But the value of Bitcoin is created by the demand for a decentralized currency - there is no demand for proofs of works themselves. Controlling an abundance of hashrate to overwhelm the security mechanism could lead to devastating results for Bitcoin.

Besides the small amount of profits made in the mining industry, nobody cares how many hashes one can produce. In the 21st century, leaders of major nations will not revert to animalistic contests of thumping the ground and bestial howling in order to establish dominance. Not that our leaders do not engage in theatrics of ground-thumping during high-level games of poker, but this alone does not confer victory. These games are embarked upon with the insights of John von Neumann and Thomas Schelling. World leaders do play high stakes games, and while we may over-estimate their prowess by suggesting they are playing chess on Calabi-Yau manifolds, their intelligence exceeds that of prehistoric skull-clubbers. To think they would abandon all the complexities of poker for artless chest-beating is laughable.

Buying Bitcoin today is not a hedge against future security issues: Security if a flow unit, Bitcoin is a stock unit, and you need centralized players to try to convert between the two. If Bitcoin's value goes up, you can buy more security for whatever requires it. If the value goes down, you will be able to buy less. Buying Bitcoin will not protect your Bitcoin. **There is absolutely no basis**

for the claim that insufficient Bitcoin reserves on the US (or any nations) government's behalf could threaten national security.

Cryptography will remain useful, but cryptography does not need Bitcoin to exist. The security of good password standards and hygiene is many orders of magnitude stronger than proof of work. **The proof of work barrier was intended to be surmounted by somebody with no credentials.** Cryptography is designed to never be breached, and if used correctly, is practically impossible to overcome.

Begging for the powerful financial players and central banks to buy into Bitcoin indicates a willingness to let Bitcoin be controlled by these people, in exchange for Number Go Up.

> *Many orthodox people speak as though it were the business of sceptics to disprove received dogmas rather than of dogmatists to prove them. This is, of course, a mistake. If I were to suggest that between the Earth and Mars there is a china teapot revolving about the sun in an elliptical orbit, nobody would be able to disprove my assertion provided I were careful to add that the teapot is too small to be revealed even by our most powerful telescopes. But if I were to go on to say that, since my assertion cannot be disproved, it is intolerable presumption on the part of human reason to doubt it, I should rightly be thought to be talking nonsense.*
>
> – *Bertrand Russell*