DCNE

P. Christian Ondaatje

Contents

Introduction

The past decade has seen an incredible rise in digital microeconomies. Satoshi Nakamoto's 2008 whitepaper[1] and its accompanying cryptocurrency Bitcoin kicked off a revolution in digital assets. The global financial crisis was an ideal crucible for foundational innovation in finance - the world made the unpleasant discovery that the bedrock of its economy was fundamentally unstable. From this instability spring an incredible invention that has dramatically improved the technology of transactions. This creation, the "Blockchain" has implications far beyond the financial sector.

Background My first concrete run-in with digital currency was an (unsuccessful) attempt to mine Primecoin in 2013 as a relatively non-technical teenager, struggling with spotty Kyrgyz WiFi and a sluggish Linux VM. In contrast, by the end of this summer I was one of the top individual XMR miners - with over 3000 CPUs[2] across Virginia, Ohio, Northern California, Oregon, and Ireland operating as part of an automated system of price-sensitive cloud bidding and mining. Add that to nearly 300 GPUs shotgun mining ETH and SIA[3] and you have a serious operation. Through certain (unfortunately proprietary) optimizations and discoveries, I was able to increase Wolfepack's profitability by approximately 130%.

Mining as Investment By virtue of having to choose currencies to mine, I have been forced to think like an investor. Unlike purchasing cryptocurrency on an exchange, mining is long-term. The decisions one makes in hardware and the programming/automating system design to extract any given asset are difficult to reverse. Illiquidity forces miners to think very carefully about the particular cave in which they want to be picking away. To weather the ups and downs that can devastate a superficial miner, one must necessarily think long-term. *"Knowing what I know about the world and where it's going, should I buy a plot rich in oil, or one hiding a strain of gold?"* It could take years to see a return from either plot, so I should be convinced that the resource underpinning the land I purchase has a higher expectation of future value than its alternatives.

Motive That is why I wrote this paper. The process of deciding which currencies to mine has given me a strong informational advantage that would be a shame not to capitalize. Knowing what I know about where this technology is going, it would be wasteful (and even risky) not to deploy capital in the areas I will discuss below. Furthermore, it is in my own self-interest to establish a track record of successful predictions - and timestamping a hash of this document is a perfect application of the Blockchain.

While I do not expect many readers will start with any confidence in a collegiate nobody, I hope that by the end of this document you will be convinced that the assets underpinning the distributed microeconomies we will discuss are indeed worthy of investment.

Overview To do this, I will first give a thorough explanation of Blockchain technology geared towards the non-technical reader. I hope this will come as a breath of fresh air to those of you who have yet to receive a convincing explanation of what the hell cryptocurrency really *is*, and why people insist on claiming that it has intrinsic value when it seems like vapor intuitively.

---

1 `https://bitcoin.org/bitcoin.pdf`

2 Logical cores

3 Which we will discuss later

I will also dive into individual digital microeconomies, the exciting direction in which human connectivity is headed, and the concept of the Decentralized New Economy (DCNE). These ideas for the core of my research at Harvard and extend to my primary efforts at Squire.

Blockchain

Importance of Understanding For the intelligent investor to make an informed decision on digital assets, it is essential that he/she has a thorough understanding of the underlying technology. While there are those who go off trust and reputation, I am not comfortable investing in that which I do not understand - and by virtue of your uninvolvement, I expect most of you feel the same. I have yet to hear a good non-technical explanation of the Blockchain,[4] so that responsibility falls to me. With my apologies in advance, I will err on the side of over-explanation. I would be much more upset about failing those who truly want to understand a new technology than I would be about boring others who dislike excess reading.

Dynamite and Coins Imagine that you have a stick of dynamite and a bucket full of coin-shaped metal slugs [5] that you forged. If you're like me, then it is a foregone conclusion that the slugs will have to be blown up. You place each coin and the dynamite in an exact location within the bucket, taking care to record each positioning. Then, you explode the dynamite and watch the coins rocket around the room before coming to rest at specific locations. Suspending disbelief (remember that we are dealing with computers here), when you use your earlier recordings to repeat the experiment identically, the result is an identical distribution of coins across the room. Even better, if your neighbors are as enthusiastic about the scientific method as you are, they can copy your configuration of coins and reproduce your same results in their own homes. Logically, even an infinitesimal change in the position of the dynamite produces completely different and effectively random results.

Hashing Now imagine that you grow bored of pointless explosion (unlikely) and set yourself the challenge of finding a configuration that will land at least five metal coins "heads-up" in the kitchen sink (more unlikely). *This is difficult.* There is no way to start with five heads-up coins in the sink and calculate a position of dynamite that would put them there - the only way to do this successfully is to explode an incredible amount of dynamite and coins in various positions within the bucket. Once you *do* finally land 5-up however, you can enthusiastically call up your neighbors and proudly declare that you have done something really cool. Obviously, they don't believe you. Furthermore, you should shut up because it's midnight and you've been setting off explosives for three days.

Proof-of-Work This is the beautiful thing about proof-of-work algorithms though: they may take you an incredible amount of "work" to complete, but the "proof" takes comparatively little effort to verify. Since you recorded the configuration that successfully landed five coins heads-up

[4] Technical readers: feel free to skip this section and read the original Nakamoto whitepaper (bitcoin.org/bitcoin.pdf). It really is a beautifully designed system.

[5] I chose metal coins because they naturally invoke thoughts of randomness while making a tie to money/transactions as an actual component of mining/hashing. Also easier to imagine serial numbers/inscriptions on coins than dice.

in the sink, a neighbor can go back to his own kitchen (full of metal coins, naturally) and explode a bucket using the exact same alignment and dynamite positioning. Since the exact same inputs produce the exact same outputs, his experiment verifies that you have indeed discovered a way to get five coins to land heads-up in a kitchen sink. And since they know that you can't reverse-engineer the feat, you have proven to your neighbors that you put a lot of work into this discovery - you could have tried millions of times before succeeding. So the coins in the sink are your "***proof-of-work***."

Reward After their initial skepticism, your neighbors are so impressed with your achievement that they get together and conclude that you should have some kind of trophy (these are not normal neighbors). While these aren't exactly official coins, aren't they the perfect reward? If the whole neighborhood accepts your proof-of-work and decides that you deserve a reward, how about just putting your name on a few of them? You have some nice trophies, which look so shiny and have a cool enough story that some people are actually willing to buy them from you (for a couple cents).[6]

Mining Blocks Needless to say, you are pretty happy with this consensus. So happy, in fact, that you quickly start over with a new bucket of forged coins. Realizing this might get out of hand, the Homeowners' Association quickly announces a new recommendation that the community adopts; no more than 50 self-made coins may be minted per successfully discovered dynamite-and-coin-positioning. Also, verified "*dynamite-and-coin-positionings*" will now be called "***blocks***" because "*dynamite-and-coin-positioning*" is a mouthful. Furthermore, the process of "*exploding-coins-to-try-to-land-them-in-kitchen-sinks-so-that-others-may-verify-and-reward-your-achievement*" shall be called "***mining***" because...well you get the idea. These coins you are mining are worth almost nothing at the start - only your neighbors recognize them as legitimate tender, and even then nobody thinks they are worth that much. Even so, you and your close friends continue mining blocks every day because you think it's a pretty cool hobby - and maybe someday these little coins will be worth enough to buy a pizza or something.[7]

Difficulty Eventually though, a bunch of your neighbors catch wind of the operation and decide that it may be profitable to immediately sell any coins they earn, and quickly buy up some heavy explosives from the American Mining Dynamite corporation (AMD). Suddenly, the sound of explosions can be heard all around the neighborhood, and before you can discover the next successful configuration of metal and dynamite your phone rings - a neighbor has beaten you to it and landed five coins "heads-up." For the first time, the neighborhood awards 50 trophy coins to someone outside your little friend group. Soon enough, someone is discovering a successful positioning every five minutes - way too fast for you to keep up with your recordings and proof-of-work verifications. The town's combined mining power has increased to the point where something that was very improbable at an individual level is quite common in aggregate. Once again the HOA convenes as a consensus builds among neighbors that something needs to be done - the "***difficulty***" of mining has to increase. With typical HOA acuity, they originally decide that now there should be 10 coins heads-up in the sink for a block to be valid and its miner rewarded.

The miners quickly realize this will double the difficulty five times over, when they actually think that on average it makes sense for the whole neighborhood to produce one block every ten minutes.

---

[6] This is what is called a "mining reward," and is a big part of the digital economy's equivalent of monetary policy. More on that later.

[7] `bitcointalk.org/index.php?topic=137.msg1141#msg1141`

Therefore, we should all adjust the definition of a successful block to require *six* coins heads-up in the sink. Furthermore, we should commit to a continuous adjustment of difficulty; the requisite number of coins for a valid proof should increase and decrease as people join or leave the party. This way, no matter how high or low your neighborhood's total mining power, there will always be one successful configuration discovered approximately every ten minutes.

Users Now, there are those in the neighborhood who hate fun and don't care much for explosives, but have a real need for alternative methods of transaction. This is a Zimbabwean municipality, and the established fiat currency is undergoing hyperinflation. Furthermore, corruption is a real risk in the banking system - at any point your money could suddenly become someone else's money. Confidence in traditional financial institutions is low. But what about all those dynamite coins previously considered useless? Their position, size, etc. are constantly being recorded so that others can reproduce and verify successful blocks, right? Why not use a system based on those records to replace the currency that has lost the confidence of the populace? If every aspect of those coins is being recorded and distributed to the neighborhood, then there is a perfect opportunity for one of those aspects to denominate a transfer of value from one citizen to another. This can be a bit confusing, so don't worry if it doesn't make sense yet.

Distributed Ledger For this part, it is very important to understand the system that Dynamite Town is starting to use. The metal slugs being dynamited and recorded are not inherently valuable. What is important is the transfer of acknowledged wealth from one person to another - the "transaction." So the value of a "coin" comes from the whole neighborhood seeing and recording that I have declared that some of my net worth shall now belong to you. To internalize this, we can think of "coins" as simple metal slugs with inscriptions (true of real coins as well). For Dtowns purposes, that inscription is a transfer of Dynamite Coin Network Equity from one member of the system to another. So whether a coin is an original or a copy doesn't matter, the only important thing is that the inscription is recorded in the Ledger of verified configurations everyone in the neighborhood keeps. Just like a bank ledger, there is no actual physical item keeping track of your balance, but rather several institutions keeping track of your wealth. Once a miner successfully explodes my "coin," that transaction is permanently entered into that "***Distributed Ledger***" and our consensus wealth can be adjusted accordingly.

Transactions So let's say I am a non-mining neighbor, and I would like to purchase my friend Lucille's paper shredder. Knowing that the Zimbabwean dollar-denominated value of her shredder is changing by the day, Lucille is not comfortable transacting in the traditional market. Recognizing this issue, I propose a payment of 10,000 units of Dynamite Coin Network Equity (DCNE). Now, Lucille is somewhat pleased with this offer. Relative to the Zimbabwean dollar, Dynamite Coins appear somewhat stable. However, she is a bit worried about the fact that this coin could simply be a copy, and I could be buying up all the paper shredders in town with the same piece of copied metal.

Processing Transactions So Lucille says that she will only accept my payment if I send it through the miners. Since exact bucket contents are recorded as part of the verification process, if she sees my coin in the Distributed Ledger then she can be pretty sure I've paid her. In addition, if she really doesn't trust me, she can wait a few more blocks to make sure I haven't also sent someone else a copy of the same coin in a different miner bucket. Furthermore, since everyone has to record the transaction for sink-verification, she can be reasonably sure that the neighborhood

will recognize the money as hers once it is transfered - everyone saw and verified that she was the recipient of a legitimate transfer of value. The money cannot be absconded with because everyone knows that those coins are Lucille's and Lucille's only. The only way I could fool her is by owning hundreds of "mining rigs" or being in cahoots with hundreds of miners.[8] After a couple blocks, Lucille is reasonably convinced that I have indeed transfered value to her name. Happily, she hands over the paper shredder - which I promptly put to use to dispose of my old Zimbabwean dollars.

Transaction Volume In fact, this transaction was so much better than the old system that Lucille decides to start using exclusively dynamite coins for important transactions. All she has to do is call up a miner friend and give him the coin she made, which has "Lucille" in the "from" address and the recipient's name in the "to" address. As soon as a miner gets the proper amount of coins in the sink, the village inherently recognizes the transfer of value from one neighbor to another by recording and verifying all the exploded coins, their inscriptions, positions, etc. Keep in mind that due to the unpredictable force of a dynamite explosion even a change of a single letter in the inscription would create a wildly different explosion result that wouldn't land 5 coins heads-up in the sink! So fraud and forgery are easily discoverable. This system is so useful to the people of Dynamite Town that all the hobbyist miners' phones start ringing off the hook - everyone wants to send money using their dynamite buckets. One day, Lucille calls her friend Sutter to ask if she can squeeze yet another important transaction into his exploder-bucket so that it can be recorded in the Distributed Ledger.

Fees! "Enough!" protests Sutter, fed up with the calls he's been getting day and night. "I will only include your transaction for a fee. You have to write my name on 0.1 of the coin you are sending." This annoys Lucille, because transactions that used to be free now cost her a small fee, but she can see the reasoning behind it. Begrudgingly, she adds a little asterisk to the engraving on the coin/transaction declaring that 0.1 units of DCNE should also go to the miner.

But wait! Remember how coins are copyable? The only important thing is announcing the transfer of value to the neighborhood, not the metal itself. As soon as they hear that Lucille has engraved a coin with a miner fee, every miner in the neighborhood makes a copy - it's a no-brainer. If they successfully push her transaction through, they will get an extra reward. This means that Lucille's coin is mined immediately: there was a much better chance of her transaction being processed in the next discovered block, because it was in the miners' economic self-interest to include it in their bucket explosions. When the transaction goes through, the neighborhood's Distributed Ledger records a small transfer of value to the winning miner, as well as the main transfer from Lucille to her vendor.

Suddenly, all the miners decide that it isn't worth their time to accept coins without that extra asterisk awarding a fee. Enough people are now using the system that Sutter cannot include every pending transaction coin in his bucket. Naturally, he prioritizes the coins with the highest fees attached, which establishes a general correlation between fees and transaction processing speed. Some users are understandably unhappy about this, while others get enough utility from the option for increased speed to limit their dissent to a bit of grumbling. Nonetheless, Lucille stops inviting Sutter to her Sunday night poker games.[9] Life goes on however, and the neighborhood keeps transacting under this new system. Despite the introduction of fees, everyone is still better off

[8] (51% attack - Don't worry if this doesn't make sense intuitively) `investopedia.com/terms/1/51-attack.asp`

[9] Which are legal in Zimbabwe.

than before the system came about. Miner incomes continue to increase, and the set of goods and services users are able to purchase with DCNE grows as more people start using dynamite coins to transfer value.

The Case for Chaining This continues for some time, and everyone is pretty happy. It's a relatively small neighborhood, so for the most part everyone trusts each other and the records being kept of the transactions in every block. One day though, a devious man (let's call him Mark) moves to the neighborhood. Quickly adjusting to the strange customs of Dynamite Town, he plugs away with his coins and buckets. Being the morally ambiguous man he is, Mark quickly realizes that (since everyone in the neighborhood knows and trusts each other) he can take advantage of the verification and recording system. If every successful block is treated as an independent set of transactions and verified separately, there is an opportunity for him to sneak self-rewarding transactions into the neighborhood's consensus. Remember that the actual pieces of metal aren't the important thing - it's everyone's recognition of each other's transactions received minus transactions sent that determines net worth in the neighborhood.

But things can get tricky. All these blocks are being verified, but they have no real connection to each other. Most importantly, there isn't a canonical order to them - if all the verification slips were to be shuffled, then nobody would know who had what funds at which point in time. Recognizing this, Mark takes advantage of his naive new friend Christoph. After purchasing a few shredders from Lucille, Mark's consensus wealth is somewhat diminished. However, by omitting the verification slips for the block recording his payment to Lucille, he can convince Christoph that he has enough wealth to his name to buy his (used) Lamborghini. Now, this is not the most sophisticated attack, and I'm sure there are better examples to illustrate the vulnerability of a transaction system that isn't strictly ordered and complete. However, it is hopefully sufficient to convince the reader of the glaring security holes in Dynamite Town's current system. Ever the naive optimist, Christoph promptly hands over the keys.

Chaining Soon everyone is scamming away, and the economic stability of Dynamite Town is once again at risk. Dawning their superhero capes, the HOA puts aside their hedge-trim inspection duties to come up with a solution. After sub-committee formations and requisite increases in dues, they attempt to cement the new policy with great pride - from now on all verification slips shall be timestamped.

Laughing, Mark promptly begins to forge timestamps as financial chaos continues to threaten the neighborhood. Previously underestimated, the difficulty of finding a solution to the block ordering problem is now widely acknowledged. Before the HOA can come up with another brilliant solution a bright young metalworker proposes a simple but elegant alteration to the existing protocol - why not connect the blocks like links in a chain? All the miners would have to do is use some of the coins from the result of the previous block's explosion in the next configuration, and a canonical order immune to tampering could be established.

Initially confused, the neighbors think about this for a little while and realize that it is actually quite a beautiful solution. The core issue with the HOA's timestamping proposal was the malleable nature of the verification method - anyone can say something happened in a certain order or on a certain date. Proving it is more important. With the chaining solution, block ordering is *provable*. Since any infinitesimal change in coin position, inscription, etc. produces a completely and randomly

different result that will not have five coins heads-up in the sink,[10] it is practically impossible for Mark to continue his nefarious ways. A faulty ordering can be immediately spotted in verification because the coins in the next explosion will not land properly in the sink! They will be sent in completely different directions and Mark's deceit promptly exposed. This means that Christoph, though not an expert in security, can easily double check that Mark's transfer of DCNE is legitimate, without relying on the trustworthiness of his neighbor.

And thus, the "BlockLink" was born.

Wait, that doesn't sound right ..."LinkBlock?" "Chainlink?"

"...BLOCKCHAIN!!!"

Bridge

The story of Dynamite Town is an (almost) exact metaphor for the actual structures and protocols of the Bitcoin Blockchain. At this point, you have a much better comprehension of the technology than 99.9% of the world. With this understanding under your belt, we can now jump into the exact details with much greater comfort.

Hashing Digitally, explosions are implemented using "hashing" - a buzzword that has started to be tossed around without understanding. Hashing is the digital equivalent of detonating dynamite; a pseudo-random, irreversible "explosion" that produces a concrete result (a number). I understand that it may be a stretch to imagine a tiny change in coin engraving would produce a completely different distribution of coins across the kitchen. Hopefully a concrete example of hashing is easier to digest, while preserving the intuition we cultivated over the past few pages.

Take for example the SHA-256 hashing algorithm that underpins the Bitcoin Blockchain.[11] No matter how many times you try, hashing "Ondaatje" always produces the following characters:

"`764a4879f1dbeaa39d754c2ae23722b12985e76c59724d02c9d9c0be2d1fec92`"

However, hashing "Ondatje" (with only one "a") produces a completely different string/number:[12]

[10] probabilistically speaking

[11] Developed by the NSA. Also we run it twice in Bitcoin. Probably because people think it protects against the birthday attack but it actually doesn't. `https://en.wikipedia.org/wiki/Birthday_attack`. Also important from that article - quantum computers are still exponential time (for hashing).

[12] computer numbers have letters, too - don't worry too much about it. `https://en.wikipedia.org/wiki/Hexadecimal`

"`c11c795c38a2659cfd8962a75e06ceb05ae03496c18f7b565f4a0fab52a7b14f`"

In addition to the small comfort that even computers struggle with my last name, this phenomenon is incredibly reassuring when considering the security of your finances - even the smallest tampering with the historical record of transactions will result in a glaringly unacceptable hash. Furthermore, it is *hard* to get hashes to "collide" - which is when you reproduce a given hash result with a different input. Keep in mind that when people in Computer Science say something is "*hard*," they mean that it would likely take longer than the expected date of the heat-death of the universe to successfully compute. If your computer reports a successful collision, it is literally more likely that an errant cosmic ray caused it to malfunction than it is for the collision to be valid.

Looking at the strings above, you can see that there are 16 different possibilities for each "digit" (0-9, a-f). This means that there is a 1/16 chance the first number will be "7," for example. Now, if you are trying to break the "Ondaatje" hash, the next digit would have to be "6." That is now a 1/256 chance. By the time you get to the last digit, you have a $\frac{1}{16^{64}}$ chance of a collision. That is a 1 out of 115 quattuorvigintillion chance!

Difficulty, Probability For most blockchains, "Hashing" and "Mining" may be used almost interchangeably. While we are trying to get an adjustable number of coins to land heads-up in the kitchen sink, miners are trying to get a hash below a certain target number. This number is called the network "*difficulty*" - just like in Dynamite Town. The lower the target number, the harder it is to successfully hash below it. So while it may be practically impossible to guess an exact hash, it is much easier to guess a nonce (real-life equivalent of a specific dynamite position) that results in a hash between zero and the difficulty number. You can think of this like rolling dice - it's pretty easy to roll below a six. But if someone asks you to roll a number below 2, it might take you several tries. So if the difficulty number is the maximum possible hash value,[13] you have a 100% chance of successfully mining a block. Cut the difficulty in half, and you have a 50% chance, and mining will take you twice as long (on average). Similar to HOA policy, the difficulty adjusts automatically[14] to target 10-minute block times, so as miners come and go the transaction bandwidth of Bitcoin stays mostly the same. Since every digit in the hash is random, this is just like landing coins heads-up in the sink; probabilistically difficult, and immune to reverse-engineering.

Pooling This brings us naturally to the concept of a "***Mining Pool***." As you may have already identified, there are a set number of blocks being produced every day, and yet there may be large increases in mining power as more miners join the network. This means that the difficulty system could eventually make the payout intervals for an individual miner incredibly large. So while the averages might make sense theoretically, we humans tend to prefer steady streams of income to random (though probabilistically equivalent) chunk payments. This income smoothing is the primary motivator for a naturally occurring New Economy model. Individual miners "pool" their mining power, and in the (now less unlikely) event they discover the next block, they split the rewards proportionally to each miner's "hashrate."[15] While this model can be implemented in a

[13] 115 quattuorvigintillion, or "`ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff`" in computer numbers (hexadecimal). This is not the actual maximum difficulty in the code, but helps conceptually.

[14] every 2016 blocks, or ∼14 days if everything is going right

[15] For the curious - the way it actually works is that a mining pool will have a custom difficulty rate that is much easier that the real one. Then any successful hash beneath the pool difficulty is counted as a "share." So while

decentralized way, almost all major pools fall under the "Centralized New Economy" model, with some entity assigning work and charging a small percentage fee.

Fixed Supply One of the questions people frequently ask is how there can be a fixed amount of Bitcoin (or any digital currency) - it's not intuitive that there could be a supply limit for a digital good. This is a good place to demonstrate the "***code as law***" concept. As the name would suggest, there are a couple layers here - the first is technical, and the second is crypto-political.[16]
Simple answer to the coin limit question: there is a fixed supply of Bitcoin because it's written in the code. The function below controls the mining reward for successful blocks. Remember, this is like the HOA recommendation for the acceptable amount of self-congratulatory coins a successful sink-proof should mint.

Note: don't worry about understanding the code. But if you'd like to give it a read, it's helpful to know that the "right shift" operation (`>>`) cuts a number in half.

```
CAmount GetBlockSubsidy(int nHeight, const Consensus::Params& consensusParams)
{
    int halvings = nHeight / consensusParams.nSubsidyHalvingInterval;
    // Force block reward to zero when right shift is undefined.
    if (halvings >= 64)
        return 0;

    CAmount nSubsidy = 50 * COIN;
    // Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years.
    nSubsidy >>= halvings;
    return nSubsidy;
}
```

(from `github.com/bitcoin/bitcoin`)

These few lines of code control the global supply of Bitcoin. *That is cool.* There is no central organization controlling this reward, though there are some who have influence (like the HOA, but more on that later). It is built into the code that thousands of computers around the world are running and agreeing upon. Every 210,000 blocks (which, at ten minutes per block, comes out to around 4 years) the reward cuts in half. This has huge crypto-economic ramifications, but mathematically it just means that there can only ever be 21 million BTC.

Digital Politics Now for the more complex answer - politically, it is not set in stone that there will only ever be 21 million BTC (though it is set in code). If enough of the world were to adopt just one small change to the function shown above, further millions, billions, or even a continuous (and therefore infinite) amount of Bitcoin could be created. Such changes are the crypto equivalent of monetary policy, and even more - they are digital law. This is one of the most fascinating aspects of digital microeconomies, and I believe the political intrigue that goes into changes to the consensus

you most likely won't mine a successful block, the pool can see how many shares you contributed and get a probabilistic picture of the work you dedicated to the cause, and pay out accordingly.

[16] need a footnote? Editors lmk.

code will be the subject of history books. A unique set of influence-granting forces derived from compute power, chain wealth, and democratic mass collide to push changes into the global code in support of various (often conflicting) agenda.

These crypto-political forces are very important to understand as an investor. Sometimes, proposed changes can be so fractious that a "Hard Fork" occurs, with one group going their own way with an altered consensus, rejecting any new block that does not conform - effectively creating a new cryptocurrency. When a contested hard fork occurs, it means that there has been a revolution in a blockchain's ecosystem. Two conflicting parties have failed to come to an agreement, and will now cease all negotiations and trigger the "nuclear option." This is what forked Ethereum from Ethereum Classic, and Bitcoin Cash from Bitcoin.

Code as Law This is the process by which laws are made in cyberspace. It is not an ideological institution; the things you can and cannot do are completely determined by the consensus code that forms the Blockchain. Digital theft from an unsecured wallet, while immoral, by definition violates no code - or else the funds would have been secure. If you fail to secure your digital assets, they are not yours - in cyberspace, what you own is what you can protect. In meatspace, an individual almost always has to rely on a government to uphold her property, ownership, and other rights - this is one of the central roles of the state in political theory. This necessity is absent in cyberspace, and is part of what makes cryptocurrencies so difficult to regulate. It is also why the Blockchain appeals to so many radical cyber-anarchist types: whereas an individual cannot hope to hold land without government-enforced property rights, cryptography is such a publicly available and powerful defensive technology that an *individual* can have the digital equivalent of Fort Knox protecting his funds.

Control as Ownership In this sense, "ownership" is a more primal concept on the Blockchain. I "own" a significant amount of cryptocurrency in that I am the only one with the keys to a publicly viewable safe, inside of which all the participants of the Blockchain acknowledge there exists a specific amount of wealth (remember, your net worth in Dynamite town comes from the amount of wealth everyone knows you have received, not from the metal coins themselves). This is a complicated and dense bundle of concepts, but it illustrates the altered concept of ownership in a "lawless" ecosystem. Nobody "owns" cryptocurrency - they control it. For all intents and purposes, these are the same externally. As long as you are the only one with the keys, and can send some of your wealth to someone else, you control (and therefore own) the asset.

Security This is why you hear about cryptocurrency "hacks" and theft so frequently. Many non-technical or inexperienced users fail to properly secure their funds, or fall victim to scams. Even well-regarded programmers have exposed incredible amounts of wealth to theft, and paid the price. The most important thing to note, however, is that (aside from a few specific cases) every one of these "hacks" is due to human error. The underlying security of the Blockchain is astoundingly robust - and completely dominant in comparison to any other financial system.

Bitcoin's Shortcomings

While I hope you have come to share my reverence for blockchain systems as a technology, the topics we've discussed most recently bring us naturally to some of the shortcomings with Bitcoin specifically. Through further examination, we can start to explore some of the reasons why Blockchains other than the original have taken over most of crypto wealth transacted. Furthermore, it is important to show that (while generational) the basic blockchain technology I've illustrated above is unfortunately outdated technology at this point.

FPGAs/ASICs In late 2011, miners started using devices called "FPGAs" (Field-Programmable Gate Arrays). These are cool. Basically, whereas a programmer can usually only write code to make software-level changes and is stuck with the hardware configuration she starts with, FPGAs let you change the actual structure of the hardware on which you operate. This means you can customize the device to do something specific incredibly well - like mining Bitcoin. Pretty soon the FPGA was replaced by a device called an "ASIC" (Application-Specific Integrated Circuit). These took the advances made with FPGAs and set them in stone, with super-fast single-purpose hardware. You can think of a regular computer as similar to a Swiss Army knife - it can do a lot of different things pretty well. An ASIC is like a longsword - it can't do most of the stuff a swiss army knife can do, but goddamn can it cut things up. Crypto ASICs *live* to mine coins.

ASIC Difficulty Bomb As a consequence however, the fundamental structure of the Bitcoin microeconomy changed dramatically. Because of the mining difficulty concept we discussed earlier (where it becomes harder to successfully mine a block the more compute power there is in the network), there was a dramatic reduction in the relative hashing power of personal computers. When ASICs came online, they immediately dominated all other forms of mining and made the odds of successfully discovering a block nearly zero for the average person. For example, if I had been hashing in 2011 (prior to the ASIC invasion) I would be earning approximately 0.59 BTC every day (∼$50/mo at historical prices). By comparison, that same level of non-ASIC mining power in fall of 2017 would only net me ∼0.0000007 BTC - just about 8 cents a month at $4000 USD/BTC. Calculating in the cost of powering a mining computer, that's actually a significant financial loss every month. An example of how ridiculous the relative probabilities are now: if you played the lottery as frequently as you hashed, you could expect to win the (1 out of 175 million) powerball 100 times before successfully landing enough proverbial coins heads-up in the sink with a personal computer.[17]

CNE There are a few key issues with this blockchain state (though opinions on the matter are diverse and divisive). First, though pooled mining has certainly centralized the hashing power of most popular cryptocurrencies, it is important to note that it does not centralize the rewards. Mining pools are ***Centralized New-Economic systems***. It is not through brute force effort in hiring that the Über fleet grew to over one million drivers, but the simple incentives of the system that led drivers to sign up. There are more Über drivers than active duty servicemen and women in the US Military. Consider that the Department of Defense has an annual budget exceeding half a trillion dollars,[18] and the efficiency of these economic systems as compared to traditional models

[17] Stats from March 2018: `https://goo.gl/K6AjRs`

[18] Of course it's not a perfect comparison (Über spends much less on cruise missiles), but you get the point. Regardless, DoD military personnel costs are in the hundreds of billions: `https://en.wikipedia.org/wiki/`

becomes clear. Some other examples of the central-distributed model: AirBnB, Net Metering, the Tesla Autofleet, and my own company - Squire. Including Mining Pools, centrally-distributed systems represent (in my opinion) the most elegant business models out there. I say "centralized" because while the work done is thoroughly distributed, at the core there is some singular entity in charge of the incentives.[19]

DCNE Pure mining, on the other hand, is a ***Decentralized New-Economic System***. There is no controlling entity, and the movements of the microeconomy as a whole have more similarities to weather patterns than traditional market trends. Imagine if there was no Über corporation - only the app. Payments go directly to drivers from riders, with no middleman. Driver behavior and ride pricing would be driven purely by market forces. This model is almost exclusive to the cryptocurrency world, so unfortunately I do not have a perfect explanatory analogy to explain the DCNE - only a very long paper. If you are trying to think through whether a system is a DCNE, consider the incentives. Is there a central authority in control of the system's incentives? If so, it is not a Decentralized New Economy. Decentralization gets back to the core of economics - global commerce, while somewhat regulated by international coalitions, is naturally decentralized. Barter and trade-based economies are as well. DCNEs are not new - they are the most natural economic phenomenon. DCNEs, when combined with hybrid ecosystems (CNEs), form what I like to call the ***New Economy.***

BTC Mining as Old Economy In contrast, ASIC mining much more closely resembles the old economy - simple, brute force revenue generation. Modern Bitcoin miners have tremendous overhead and the field has serious barriers to entry. It may be profitable, but the core model is inelegant and scale is difficult. This has centralized Bitcoin mining *rewards*, which is very different from centralizing mining *power* (with pools). Compared to currencies that are still profitable for the individual miner, Bitcoin's political landscape is more subject to the whim of individuals at the head of large mining entities. These individuals may in turn be accountable to governments - in fact most Bitcoin mining takes place in China, whose government could almost certainly influence the currency.

Centralization For this reason, I will claim that ASICs have not improved Bitcoin's overall security in practice. Theoretically, since the majority of SHA256 hashing power in the world comes from Bitcoin ASICs, the network is more secure than one which could be taken over by a mass of compute power (such as ASIC-resistant blockchains). If all the relevant compute power is already dedicated to Bitcoin, then it should be safe. However, the 51% attack (where a mass of compute power attempts to take over a blockchain) is more of an interesting theoretical risk than the very real danger of centralization. This improvement in *theoretical* security has come with a great sacrifice of *practical* security. If the abstract worry is that some central authority or government could take over half of all mining, the current situation (with nearly all mining centralized in China) is completely unacceptable.[20] Centralization has caused an incredible amount of political turmoil within the Bitcoin ecosystem, with Chinese-based mining companies holding an incredible amount of power over the protocol. Changes to the code are debated with intensity, and for good reason -

`Military_budget_of_the_United_States`

[19] `https://blog.ycombinator.com/read-this-before-you-build-uber-for-x/`

[20] Luckily China has never fiddled with currencies.

mis-steps can be devastating to millions of users, incredible quantities of personal wealth, and an entire growing mining industry.

Case Study: Scaling Debate That dynamic came to a head in the recent scaling debate, and subsequent fracture of the Bitcoin Blockchain. Basically, Bitcoin's slowness was limiting day-to-day use and possibly contributing to a massive decline in market cap relative to the rest of the cryptocurrency ecosystem. Because of it's 10-minute block time (as explained in Dtown) and a limit on the number of transactions that could make up each block (a hard-coded maximum number of coins per bucket), Bitcoin couldn't process that many transactions per second relative to price-independent demand. This meant that as more and more people started using Cryptocurrencies, the Bitcoin network "clogged," and dollar-denominated transaction fees skyrocketed. In the Dtown analogy, there were so many neighbors trying to get into Sutter's next block that his bucket couldn't fit any more transaction coins - so he had to keep raising the fees he charged until demand met supply. What used to cost a few cents now cost several dollars - making Bitcoin impractical for certain types of transactions.[21]

BCH Hard Fork This problem is what led to Bitcoin's divisive "scaling debate," and ultimately to the Bitcoin Cash hard fork. Rifts within the community grew as factions formed along lines of ideology and economic self-interest. Without getting into the digital politics, which would take pages to discuss, let's just say that it was not the Bitcoin community's finest moment.[22] In fact, it showed quite clearly that major changes to the code are not likely to be settled peacefully, even with vast majority consensus. To be fair, that's not necessarily a bad thing. If Bitcoin is to become "digital gold" rather than easy-to-use digital currency, the argument can be made that changes to the code should spill digital blood.

Digital Gold The Bitcoin Cash hard fork is just one instance of a larger movement away from Bitcoin as anything but a store of value. While this is a very real use-case for the digital currency, it comes at the price of market dominance. There is so much else that blockchains can do, and following this path makes Bitcoin's value purely societal - like gold, we appear to have all decided that Bitcoin is worth something. Nobody can really say why. Gold is quite useless, and like Bitcoin it has little to no *intrinsic* value - though both have enormous socially-assigned value. While this value is very real, it tickles my spidey senses. I would much rather invest in oil or electricity than gold, because "a lot of other people say it's valuable" is not a convincing proposition.[23]

Altcoins The fact remains that in the time it took for the scaling debate to resolve, Bitcoin's market capitalization fell from 99% to less than half of all crypto wealth.[24] Hundreds of alternative currencies ("Altcoins") sprung up to fix the issues Bitcoin's community couldn't/wouldn't address. While there are advantages to whim-resistance in code that is supposed to be digital gold, the Bitcoin community's inability to effect meaningful change without scandal is a real risk to the

[21] Very important to note - this made it very expensive to "anonymize" on the Bitcoin chain, which led to the rise of private blockchains like Monero.

[22] It was *fascinating*, though. Here's a summary: `https://hackernoon.com/the-great-bitcoin-scaling-debate-a-timeline-6108081dbada`

[23] Yes, it is the most stable element. But come on - when the grid goes down and society falls apart would you rather have gold or oil?

[24] `https://cryptolization.com/`

currency. As an example, the ECSDA signatures underlying BTC ownership are vulnerable to quantum computers. If Bitcoin can't adapt when quantum computers come online, all that value will be open to alternative locations of storage - like a thief's wallet. That would make the Bitcoin largely worthless. In the Ethereum community, there is tons of chatter about "*the flippening*" - an event where the top crypto would "flip" from Bitcoin to Ether. In reality, the flippening has already happened. Whereas crypto used to be Bitcoin and some others, logically the market is now mainly Altcoins and a bit of Bitcoin.

Ethereum

Ethereum/Ether is the leader of the Altcoins, and represents a significant leap forward in blockchain technology.[25] Hopefully the concepts underpinning the technology will be easier to understand now that we've covered the fundamentals, and gotten a decent overview of the crypto ecosystem.

World Computer To put it bluntly, Ethereum is the real deal. The concept at its core is an absolutely generational technology, and has opened up a field to which I intend to dedicate my career - economically distributed general computation. This is the "***World Computer***" aspect of Ethereum. Surprisingly, it often goes unmentioned in explanatory articles and is definitely not at the forefront of public perception - perhaps because it isn't an intuitive concept. It is important to understand however, because this concept is earth-shatteringly valuable. While I don't expect the reader to fully understand it yet, the basic intuition is that Ethereum is actually a big, decentralized computer. Instead of running programs on your laptop for example, the system runs them across thousands and thousands of computers connected to the network - all agreeing on the results. One such result can be the answer to "how much money do I have?" - so Ethereum can do digital currency, but it can also do everything else.

Ethereum, Ether To understand Ethereum, it will be helpful to get a clear picture of the ways in which it differs from Bitcoin. While the underlying system is very similar, there are a few key improvements - especially in the areas Bitcoin falls short (as explained above). First, a clear distinction must be made between Ethereum and Ether. Ethereum is software. Ether is a cryptocurrency/token built into that software. A "***token***" is just like a plastic coin at a kid's arcade or a poker chip at a grownup arcade; a unit of value to be used within a specific ecosystem. While Ether speculation is what has made (and lost) a lot of people comical amounts of wealth, its inherent value comes from a monopoly on operating the World Computer. In the Ethereum ecosystem, Ether is code-legal tender.

ASIC-Resistance The first big difference is that Ether has inherent value, as contrasted to Bitcoin's socially-assigned value. Whoever answers the question of whether the market is pricing that value correctly will be a rich person. Another big difference comes from Ethereum's apparently ASIC-resistant hashing algorithm (the importance of which we discussed in the previous section). Without getting into too many specifics, "***Dagger Hashimoto***" has memory-heavy properties that nullify the relative advantages of custom hardware. Furthermore, the fact that the community

[25] While Altcoins now encompass most of the value of cryptocurrency, and therefore deserve a less inherently dismissive title than "Altcoins," there unfortunately is no good substitute at this time and changing the name for ideology's sake would be churlish.

(led by the Ethereum Foundation) appears to be cohesive and opposed ASIC takeover means that the *reward centralization* we discussed earlier is improbable. This means that Ether will hopefully continue to be widely mined until Proof-of-Stake takes over and mining stops with the hard-coded Difficulty Bomb. More on that later.

Complex vs. Simple Blockchains Another difference between Bitcoin and Ethereum is in the relative complexity of their Blockchains. While you will probably groan at the declaration, I will classify Bitcoin and it's siblings "***Simple Blockchains***." From a technical perspective, the hashing and consensus systems are actually quite elegantly simple. Ethereum, while still elegant, employs what I call a ***Complex Blockchain***. While there are an incredible amount of technological improvements over Bitcoin, the one change that makes Ethereum's chain "complex" is the implementation of a Turing-complete programming language inside the blockchain. "Turing-complete" basically just means that it can theoretically compute anything. This may be a bit of a stretch for the Dynamite Town analogy, and if disbelief is a flying car I've probably trashed its suspension. But imagine for a minute that instead of coins with to/from engravings in the exploding buckets, every coin was inscribed with code. The same basic process is going on in Sutter's kitchen, but now you can pay him to immortalize your code on the blockchain as well.

Gas and the EVM The aggregation of these little bits of code form what's called the "***Ethereum Virtual Machine***." A virtual machine is just a simulated computer, but that doesn't sound as cool. To activate a program you've put on the chain, you fuel it with some amount of Ether - paid as "***Gas***." Adding two numbers, for example, costs three(?) gas. Much like gas in real life, the price of computer fuel goes up and down with supply and demand - so while you know how many gallons it takes for your car to drive across the country (or for the EVM to add two plus two), the price of that drive could change dramatically depending on what the Saudis (or cryptokitties) are up to.[26]

In fact, under the hood Ether is just implemented as a number in the world computer's memory. The contents of that virtual memory is called the EVM's "***state***." So when you send someone Ether, you are actually executing a bit of blockchain code to update the EVM's state; "decrease my number, increase his." This is freaking cool. The permutations of useful things you can do with little coin computers is infinite, and not in a hyperbolic way. *There are actually infinite uses for Ether.* This is what people are talking about when they throw the phrase "***smart contracts***" around. I think that term gives a poor intuition for what is actually going on inside the Ethereum blockchain. Contracts (in the colloquial sense) are such a small subset of all possible things that can be coded that it would be like calling the entirety of the internet "*smart telegraphs*" - technically accurate, but comically understated.

Digital Oil This is why Ether has inherent value. Whereas BitCoin is commonly referred to as "Digital Gold," I believe Ether is most properly characterized as "***Digital Oil***." Outside of certain applications in electrical circuits, gold is actually quite useless. There is little to no value *inherent* to gold - just like the US Dollar or any other fiat currency. [27] Oil, on the other hand, is bloody

[26] True story. `hackernoon.com/how-crypto-kitties-disrupted-the-ethereum-network-845c22aa1e6e`

[27] Crypto evangelists love to ~~shove down your throat~~ propose politely that the dollar hasn't had inherent since Nixon un-pegged it from the gold standard. They are right, but you still get to tell your annoying nephew he's dumb - it didn't have any inherent value before 1998, when The Undertaker threw Mankind off Hell In A Cell, and plummeted 16 ft through an announcer's table.

useful. Yes - Ether can be transacted. But more importantly, it can be *burned*.

There is no script for this - there has never been an inherently valuable currency. Consider the implications of the same concept in meatspace - you could put dollar bills in your gas tank. Entire stadiums could be illuminated - not by paying the power company, but by converting a dollar bill into pure energy; raw compute in the digital world. The entire economy of complex blockchains is fueled by a crystallization of *raw computer power* - the world has already started to transact in FLOP. This is the coolest science-fictiony reality of the Decentralized New Economy. It is one of the few aspects of our society that I think we wouldn't be embarrassed to share with visiting aliens. "That semi-sentient colony of meats was pretty dumb, but how cool is it that the entire transaction infrastructure is built on trading raw compute power?"

Proof-of-Stake As the technology improves, the amount of computation 1 ETH can purchase improves.[28] One such hopeful improvement is a transition away from Proof-of-Work (traditional Dtown mining) to ***Proof-of-Stake***. Proof-of-Stake is basically mining without the computers. Instead of investing tons of money in mining hardware, you "stake" some Ethereum and subject it to confiscation if you misbehave. There is a hard-coded "difficulty bomb" in the Ethereum blockchain that will essentially make mining Ether impossible - intentionally. The idea is for Proof-of-Stake to have been implemented by then. Nobody knows yet what the crypto-economic impact of Proof-of-Stake will be, but it will bring about some interesting incentive changes. First, those with the greatest potential to damage Ethereum the most will have a financial disincentive to do so - your staked ETH will be burned. Second, the entities that support the network will not have an implicit need to sell Ether - unlike miners, who must cash out at least some of their earnings to pay for operating costs. This may eliminate a downward price pressure on the currency.

Vitalik Buterin I will state clearly that I am not yet convinced that Ethereum should switch to Proof-of-Stake. Almost everything I've based my work on comes from the abstract economic model of distributed computation that the Proof-of-Work system created. That being said, I'm also betting my future on the hybrid model being ideal for raw compute, so we don't necessarily have a contradiction. Ethereum is not built to be like Squire, with all the nodes in the network forming a Distributed Supercomputer. The EVM is supposed to be one slow (but *very* secure) computer, and PoS does preserve/improve that. In addition, I recognize that I am completely outclassed here - some of the top crypto-economic minds are working on this. I have found that the most profitable default is often to first assume that the experts are dumb, and then go about finding proof. In this case however, I make an exception to my ~~blatant arrogance~~ prescient skepticism. Vitalik's eccentricity and comically stereotypical nerdiness lead to a throw-away "boy coder genius" label. Computer genies are a dime a dozen though, and that lazy stereotype obscures what I believe to be the greatest economic mind of our generation. So when Vitalik Buterin says we should do Proof-of-Stake, I suspend my disbelief and start trying to figure out why he's likely right.[29]

In Conclusion Ethereum is pretty cool. It is the most advanced computer that has ever been created, and the cryptocurrency that fuels it is probably super valuable - inherently. If Bitcoin is digital gold, then Ether is digital oil. Furthermore, Ethereum is vastly superior to any preceding

[28] Holding price constant, which is an assumption so hilariously stupid I hesitate to use it even in a hypothetical.

[29] And why I'm likely a POS.

Satoshi systems - featuring centralization-averse ASIC-resistance, improved algorithmic security,[30] a responsive and somewhat cohesive community/developer base,[31] and a creator who could win a Nobel prize in economics on top of his Turing award.

XMR

XMR, or "Monero" [32] is the most promising mathematically anonymous blockchain. I will get into what that means in a second, but the basic gist is that transactions in XMR are untraceable. Naturally, this brings us to another of Bitcoin's shortcomings.

Danger of Public Chains Every Bitcoin (and even Ethereum) transaction you make is public, and immortalized permanently on the blockchain. This is an inherent part of the technology's security - if there were no permanence and you couldn't verify transactions/ownership, you couldn't have cryptocurrency. But there are serious drawbacks to having your entire financial history open for the world to see. [33]

Value of Cryptocurrency This brings us to a conversation about the true value of cryptocurrencies that do not have inherent worth. As we discussed earlier, Ethereum has *inherent* value, because it can be "burned" to produce consensus computation. The value of cryptocurrency that do not have this built-in combustibility is a little harder to pin down. There is obviously some value there - as evidenced by market pricing. But it does not come from online payments or any of that junk - which have been around in a much more practical and efficient incarnation for ages. This is why I find it silly when people emphasize the importance of transactions-per-second over decentralization, usually citing how fast traditional payment systems like PayPal or Visa are.

These are faulty comparisons. The core value in this class of crypto comes from financial freedom. While speculation drives price in the short term, the long-term value of cryptocurrency comes from its ability to implement transactional and stored wealth beyond the reach of the state. So if a political dissident in China is afraid of having his wealth erased from his bank account with the click of a button, it makes a ton of sense to look for safe alternatives to the party's financial system. Likewise, if you are at risk of falling to civil forfeiture in the United States (where authorities can seize your assets without a charge or presumption of innocence), then the bank is the *least* safe place for your money. Or if you are a professional online poker player - your livelihood could be taken from you in an instant.

What is Monero? This should hopefully make the dangers of public blockchains clear - when you have your money in dollars or within the reach of the government, it isn't truly yours. The bank, the state, whoever - they can take it from you at any moment (directly or through coercion) and there's not much you can do about it. For most of us that's not a huge deal, and the benefits

[30] Achieved through a structure that would make it's underlying model more accurately described as a Block-Tree, actually. This means that technically, money *does* grow on trees.
I wrote the whole paper so I could make that joke.

[31] Let's not get into the DAO?

[32] Not my favorite name, which is why I tend to use it's abbreviation: "XMR"

[33] there are some attempts at financial privacy in Bitcoin and other public chains, but they are not robust - relying on obscurity or obfuscation rather than hard science and mathematics.

of state-controlled wealth outweigh the costs. But there is a large and growing portion of the world for whom financial independence and privacy are *everything*.

Monero is a *mathematically anonymous* blockchain. The inner workings of that math are way beyond the scope of this paper, and there isn't a great Dynamite Town analogy. Suffice it to say, however, that the science underpinning XMR is sophisticated - but *bloody cool*.[34]

Value, Part 2 There is, of course, a dark side to this mathematical freedom. It is almost a foregone conclusion that Monero will be used for nefarious purposes. A large subset of those people "for whom financial independence and privacy are *everything*" transact or make their living in markets that are not state-sanctioned: "black markets." Drug dealers, money launderers, assassins, etc. will all doubtless be using anonymous blockchains the future. Their economy represents anywhere between 2% and 22.67% of Global GDP [35] - a significant portion of all human productivity is dedicated to creating value that governments do not like. I won't get too far into this - for more on the black market (specifically illicit drugs) and Monero, please read my "*Illicit Drugs and Financial Privacy*" paper here: `http://financial-privacy.condaatje.me`

Morality I am not here to make a judgment about whether this is good or bad. I am here to make a judgment on whether it is *valuable* - and it is obviously valuable in the literal sense. But I think something needs to be said at this point about the morality of investing in Monero. That's what the decision comes down to - investing. Regardless of whether you decide to invest in Monero, these things will happen. Decentralization and natural economic incentives for non state-sanctioned wealth will ensure they do. So all we can do is decide whether or not to invest in the currency. Doing so will not have any effect on outcomes - only personal wealth.

So, is it wrong to profit off the drug trade? Personally, I do not think so. Imagine that I have a friend (let's call him Ross) who is so morally opposed to the drug trade that he believes it is his duty to put his money where his morals are and bet against it. Your (maybe now somewhat less) beloved author on the other hand, tries to make investment decisions objectively - not ideologically. Ross comes to me with a bet: "I bet you 100 dollars that the drug market in ten years will be much smaller than it is today." Seeing a clear trend in the market and no reason for it to slow down, I gladly accept. This bet clearly has no impact on the outcome, but it is factually accurate to say that I will profit on the rise of illicit drugs.

I claim that this is not immoral, and therefore I am comfortable investing in Monero. That being said, I also recognize that it is in my own self interest not to see this decision as immoral, so I am not to be trusted. To that end, I would ask the reader to carefully consider his or her own moral code and see whether XMR fits in it. For me, however, this is the easiest investment decision I've ever made.

[34] `getmonero.org/resources/research-lab`

[35] `unodc.org/unodc/en/money-laundering/globalization.html`
`freakonomics.com/2012/06/25/how-big-is-the-world-black-market`
`voxeu.org/article/shadow-economies-around-world-model-based-estimates`

Digital Commodities

The previous two sections covered Complex and Encrypted Blockchains. As the leading cryptocurrencies in their respective ecosystems, I consider BTC, ETH, and XMR "blue chip" items. There are however, some (even) more speculative cryptocurrencies in the digital commodities space that deserve close attention. If you are familiar with my work on this topic with Squire, the value proposition for tokens like Golem/Dfiniti/Zilliqa (raw compute), Siacoin/Storj/Filecoin (storage) is likely pretty straightforward. If not, please take a look at the full, in-depth exploration of the concept of "*Digital Commodities*" at `http://digital-commodities.condaatje.me`

Summary I will lean on that paper to provide the bulk of my argument for digital commodities, but the basic concept is that everyone has some spare storage on their drive, and isn't using their CPU/GPU 100% of the time. Rather than throwing away 90% of your computer's spare resources every day, the distributed digital commodities ecosystem promises to monetize that extra computation and storage. Now, each of the cryptocurrencies listed above has its flaws, as do the many others in the space that I haven't mentioned. The underlying techonomics, though, are incredibly promising. Put simply, this is the way things should be done - distributed, economically incentivized, efficient.

Conclusion

I'd like to think we covered some important topics in this paper. We first took a look at the inner workings of the blockchain through the story of Dynamite Town. Then, we tied the story into the very real code, economics, and crypto-politics of the digital currency ecosystem. While Bitcoin was the first of its kind, there is a real case to be made for alternative blockchains like Ethereum and Monero. Ethereum has the potential to take the abstract idea of global consensus and make it computationally real. Monero demonstrates the raw power of cryptography, and promises to create financial freedom - regardless of the consequences. And finally, the digital commodity ecosystem will dramatically increase the world's accessible compute power and storage. All these blockchains are the start of a monumental shift in the global economy. For those paying attention, it would be foolish and reductive to call this a new asset class - it is much bigger than that. Cryptocurrency is the Decentralized New Economy.

