Andreas Antonopoulos
"The Killer App: Engineering the Properties of Money"
Text from a speech given on May 8th, 2017 in New Zealand

So I'm going to talk a bit about Blockchain, but mostly I want to talk about money. Now, the word Blockchain is used by a lot of people to mean all of the applications of this technology beyond the financial applications. Beyond money. I'm certainly one of the people who said in the beginning that money is just the first app. A lot of people are excited about all the things you can do beyond finance; However, I'm here to remind you of two things.

One, money is the Killer App. It's the Killer App for Bitcoin and Bitcoin is the Killer App for Blockchain technology. Money is the Killer App because it is the foundational technology of all commerce and as such, it touches everything. How it works affects everything.

The second thing is, for all the applications that come after, the stuff that is beyond money, the Blockchain applications. In order to make those work in a neutral, open, and decentralized global platform, they will need to transact in a neutral, open, decentralized global currency. You can't do the commerce, the trade, the land registry, the identity, the everything else, without first having that foundation of a fundamentally new way of doing money that is open, neutral, borderless, global, censorship resistant. That is what comes out of the Killer App, which is money on a Blockchain.

One of the problems we have in this space is understanding the terms we use. Money is probably one of the most abused terms, because very few people really understand how money works, what money is. Money as such is not a definitional term. It's at best a descriptive term, really it's more of a general classifier. I'm going to talk a bit about what we mean when we say money, and how we need to understand money as things go forward, now that we have a new form of money based on the Blockchain.

This talk is inspired by a conversation on Twitter that Vitalik had with a few people just a few days ago. People were asking Vlad Zamfir, may have heard of him, one of the other Ethereum greats, about whether Ethereum is money. Vlad was saying, no Ethereum isn't money. And some other people were saying, yes Ethereum is money. Vitalik said, "How about instead of using the term money, instead we talk about MOE, SOV, and UOA." Most people didn't realize what he was talking about. That was a really insightful comment.

The three fundamental uses of money. SOV, store of value. MOE, Medium of exchange. UOA, unit of account. We use the word money to describe things that in their practical application exhibit one of the fundamental behaviors that allow us to use them for these purposes. If you just use the term money in general, you may be having a conversation across purposes with other people, because what

you define as money may be colored by your perception of what you think the most fundamental aspect or use case of money is. Ever had a conversation with a goldbug? As far as they're concerned, the most important, most fundamental use of money is as a long term durable store of value. Therefore, the New Zealand dollar is not money. The US dollar is not money, real money. Money made of gold. That's money. Right?

If you talk to many other people, gold isn't money. Because it's not very practical as a medium of exchange. While we recognize that it has proven to be a durable store of value over time, it's not very practical as a medium of exchange. Don't believe me? Take some gold go to your local bar, and say, "Do you take gold in here, matey? Arrh." Now, if it's a costume party, they'll probably appreciate that, otherwise they're going to ask you for New Zealand dollars or Visa.

Is Visa money? Visa is a medium of exchange, but it doesn't represent a unit of account, nor does it represent a store of value, in fact in many cases, it represents a form of debt. Wait, but most money is debt, except for gold, which is a store of value, and perhaps some of these new currencies on the Blockchain, which are also assets not debt instruments. So this whole conversation becomes confusing. The reason it becomes confusing is we're using a descriptive term of money to refer to these characteristics without differentiating them.

The first form of money was precious metal. The first form of broadly used money throughout the world as a singular global unit that could be recognized and used as a medium of exchange across cultural barriers. Silver, gold. Is it money? It was then, it's not today. So what are the features that make it money? What are the features that give it the capability to serve as a store of value, a medium of exchange, a unit of account. Certain characteristics. It has to be portable. There's a Polynesian tribe, Pacific Islanders, that use giant stones as money. Great store of value, poor medium of exchange. Thing ways twenty tons, you can carve it, and then it sits there because nobody is willing to move it. One of the stories that comes out of that is when during transport for payment of debt between one village and another, transport by canoe across an island channel, canoe sinks, stone goes to the bottom of the ocean, and it's still used as a medium of exchange, because both tribes agree that it's still there. Bottom of the ocean, hasn't moved. It's ownership now belongs to the tribe where it would have arrived, and they still refer to it as a medium of exchange and base value on it. It doesn't matter, it's there. It fulfills the role because it has preserved scarcity. Scarcity is a fundamental consideration when you're trying to build a store of value.

What are the other ones? Fungibility. The ability to have units of value that are indistinguishable from each other for legal purposes. The fact that it doesn't matter that your New Zealand dollar serial number ends in a three or a five, it's still the same. It's legal tender, and you are legally prohibited from making discriminations based on that. You can not say, "In my store, I only accept New Zealand dollars that end in a six. Because I am compelled for religious regions."

Or whatever other crazy thing you want to do. You can't do that. Fungibility is a requirement under the legal tender laws. Why? Because without fungibility currency ceases to be practical as a medium of exchange, because you now have differential pricing. If you can differentiate between units, then one New Zealand dollar will be worth one New Zealand dollar, and another one that's less desirable because fewer locations will accept it, will be discounted in the market, and operated at a discounted rate, which now means you have to keep track of different values associated with different units of the same currency as they are discounted. That one was touched by a robber. That one was used by a drug dealer. That one has traces of cocaine on it. Actually all of them have traces of cocaine on them and feces. But, we still accept them at 100% value by law. Fungibility.

There are half a dozen properties that give us the characteristics that make money suitable to fulfill one of the three fundamental functions that we understand. Unit of account is less easy to understand, but the fundamental concept there is that in a barter system, prior to the invention of money, one of the fundamental problems you have is that you have to keep track of the relative value of different commodities. If I offer haircuts in exchange for pedicures, and also offer haircuts in exchange for chicken eggs, and also offer haircuts in exchange for oil changes for my car, I can have a local area functional community of barter. But, the reason that doesn't scale, is because I have to keep track of the exchange rates between haircuts, oil changes, chicken eggs, and pedicures. And so does the pedicurist, the car mechanic, and the chicken farmer. We all have to keep track. How many haircuts is it today for an oil change? How many oil changes for a chicken? How many chickens for a pedicure? Etc, etc. It gets very complicated. What if we had some magical thing, and we could say, "Let's price everything in that." That's money. That's the fundamental function of having a unit of account.

It's interesting that the first forms of money are metal. Metal isn't necessarily very good money. It has some problems. One of the problems is that if precious metal is used as money, it has some intrinsic value that is separate from the money it represents. Silver and gold can be traded independently, for aesthetic reasons, to be used in jewelry, for other purposes. If you have a silver coin, and you recognize that perhaps it's not quite worth enough as a silver coin, you melt it. And you turn it into a necklace. Add some artistic creativity to it, and it can have a value greater than it previously had as a silver coin. That destroys its fundamental function as a medium of exchange.

Or, you shave off a tiny bit off the edge. Ever notice why coins have raised bumps around the perimeter, those were introduced by the Romans when they realized people were taking roman silver coins when they used to have full silver in them, and were shaving the perimeter. Making them smaller and smaller and smaller and smaller and smaller, until you reach the point where one of the merchants went, "Hang on, there's an awful lot of coin missing in that coin. I seem to remember them being this big when I was young." They solved that problem by

gradually diluting the silver until what you got was 99% tin, and then hyperinflation destroyed the Roman Empire, but that's a story for another era. We wouldn't possibly do that nowadays.

Gold is a terrible metal to use as a medium of exchange. One of the reasons it's terrible is because it's too damn soft. It dents. It scratches. Bits of it fall off quite easily. Great for jewelry, you can hammer it very easily. Soft metal, fantastic for jewelry, not so good for a coin. One of the things you want with a coin is you want it to be able to be used a hundred thousand times in a hundred thousand pockets by a hundred thousand people touching it without it losing bits in the process because it's not durable. Durability is a fundamental requirement for a medium of exchange. Gold is too soft.

So, here's an interesting analogy, metal represented for humanity an era when we used the materials we found around us in the world and adapted them to the uses for which they fit. You don't make a spear out of gold. Not because it's too expensive, but because you can't stab anyone with it, because it's too damn soft, right? Human beings looked around them, and they said, "This is the world, we have these things in the world, what could their use be? How do we take what exists? Leather, iron, shells, bones, tusks, ivory, whatever. How do we take these materials we have and find uses that are suitable for these materials?" At this point we are adapting nature to the uses we have, but only in a peripheral way. One of the interesting things that happens in our civilization is gradually, we become more intrusive in our adaptations. We start molding nature to our needs.

The first level of that was the ability for human beings to interact at a molecular level with the materials they were operating. To turn wood into charcoal. To turn metal alloys into stronger metals, more durable metals, harder, more brittle, less brittle, more malleable, less malleable, of different colors, melting at different temperatures. We start manipulating the world around us using the molecules. At a very high level. That's the beginning.

Gradually, we get better and better at this until eventually we can start affecting the atomic nature. The chemical era just a century ago erupted across the world. We can now manipulate the atomic structure of things. We can create synthetic fertilizers, plastics, synthetic fabrics. We are now not waiting to find the use for a material, we are changing the material in order to create a material that fits the use we have preconceived. If you take that to its extension, we're now at the point where we can do this at a nano scale. Where we can affect a subatomic structure. We can now affect things like carbon nano tubes. We are not just manipulating the atomic structure of this, to the point of making the material behave a certain way. We are giving it physical properties: Conductivity, thermal dispersion.

Properties that we give to these materials, in scifi we talk of the diamond age. Where you can go sub particle and take any material and convert it by sheer force of will, a design pattern and sufficient energy. You could take a chair and say, a

chair has carbon, diamonds have carbon. Well here's a machine I made, you throw a chair in the back, and diamonds come out the front. What's the difference? It's just a rearrangement of the particles, right? It’s science fiction, for now. We just did something amazing to money.

Until now, we have taken money as it exists in the world and said, "This is kind of good as a medium of exchange. It kind of sucks as a store of value. But we're going to have to compromise because this is the money we have and we can not change its fundamental nature." We have precious metals, they work very well for one thing, but not for another, so we make compromises. We invent paper money, but we are still subject to the limitations of paper money. As a result, we can use it as a medium of exchange, but its control architecture means that it's going to be inflated forever by central bankers who are out of control. So we say, "Well, it's not a good store value. It's 2% inflation compounded year after year. Don't tell your children that after 30 years half of it is gone. Let's pretend that's not happening." Sucky store value. Great medium of exchange. Great unit of account. We adapt our uses to the material and not the other way around until now.

Because now, for the very first time, we can engineer money. We can engineer the fundamental properties of money. We can start tweaking whether this is more suitable as a store value or a medium of exchange or a unit of account. We start working at the fundamental structure of money by making it digital and breathing into it the exact properties we want: A monetary policy, fungibility, privacy, durability, resilience, transportability of unimaginable levels. We can whisk it across the world in seconds without sacrificing any of the properties that previously we would have to sacrifice. Instead of compromise, we engineer away the trade-off. Can we have it all? Can we have something that is simultaneously the most amazing store of value that ever existed, the most amazing medium of exchange, the most amazing unit of account? But wait, how about we invent some new characteristics of money that have never existed before.

Now, our money is also fundamentally a universal ledger of transactions. Money never did that before. We never had a form of money, that in addition to being store of value, medium of exchange, unit of account, was a universal ledger. An auditable, trackable ledger that can tell us where the money's been, how it's been used. Or not, because we tweak the privacy dial up. Say, "Guess what? Individuals should have privacy. Governments should have accountability." Let's tweak the dial. Let's reset that societal conversation and say no to surveillance. You have to tell us where you're spending our taxes. I don't have to tell you shit about where I'm spending my money, because I did nothing wrong. So, we tweak that dial. Some people are brave enough to tweak it in ways we didn't anticipate.

We are engineering money for the first time. The conversation comes up. People say, "Is this new network blockchain money really money?" Well that depends, what do you mean by money, dear sir? Are you referring to its function as a store value, a unit of exchange, a unit of account, or as a universal ledger, the thing we

just invented, or some other property that hasn't yet been invented. We don't know yet what this money is going to be good at, but I can tell you one thing, it's already better than a lot of systems of money we have, because the systems of money we have represent compromises. We have a thing, we call it money, and we take it with all of its faults and say, "That's the best we can do." We can do better now. We can engineer the properties and create forms of money that exhibit exactly what we want in their behavior. That have behaviors that surpass the physical world. That give us instantaneous settlement without third parties across the world. That can be used in payment channels for settlements of billions of transactions per second at near zero cost. We can do these things. We can do micro transactions that operate at a microsecond level on a global basis for fractions of a Satoshi. We can do these thing now. Because for the first time, we are engineering money.

Until now, when choosing the form of money we had, we are making a choice that lasts. A choice that is difficult to get out of. If I hold New Zealand dollars, but I really want it to have gold because it's a better store of value, that's not an easy conversion. I can't simply lift a finger, press a button, and convert my New Zealand dollars into gold. I can convert a spreadsheet representation of New Zealand dollars into a spreadsheet representation of gold. Then .. I don't actually have either of them, the bank has it. Let's hope Greece doesn't happen again. Surely that couldn't happen here. That's not really a conversion. If I really wanted to convert the product of my labor into gold, I have to go through some pretty incredible hoops to do that and take physical possession of the gold, which then becomes very difficult to transport because it's heavy. Then if I wanted to spend it, I have to sell it, which is another whole rigmarole of problems.

Trade-offs, compromises, what if we could do something different? Instead of trade-offs we can trade. Trading becomes the better solution. Now, if I have a fully digital owned asset that is a perfect store value, and I want a fully digital owned asset, not under account or party custodial account, I own this, I control this, with my own keys. I want to convert from the very very slow conservative robust super secure store of value currency, to the very very nimble, micro payment, instantaneous, buy a damn cup of coffee right now, across the world currency, now I can do that with a click. In a cross chain atomic swap, with no counterparty risk.

I don't do trade-offs anymore. I trade. Then I don't trade, my wallet does on demand, intelligently, as I need. If I need to buy a cup of coffee, my wallet converts a sufficient amount of stored value into coffee. Then the remainder goes back into stored value in milliseconds. No trade-offs. I can disaggregate the fundamental functions of money. Get the best store value, the best medium of exchange, the best unit of account, and some new properties I didn't have before like a universal ledger, because we are engineering the very molecular nature of money by making it digital, by making it decentralized, by opening it up to engineering innovation, by making it completely borderless, outside of the

controls of banks and governments and third parties by making it a pure digital technology. Money is technology. It's a value language. It's a system of symbols that allows us to communicate value to each other.

Until now, we've had just poor substitutes of this. Paper and precious metals and cards that give us access to debt in somebody else's spreadsheet, if they will give it to us, if they're still solvent. All of these inferior forces of money, all of these inferior forms of money, will now have to compete. They will have to compete against this new form of Blockchain based, network based decentralized money that is engineered to deliver exactly the principles and features that we want. They're not going to compete very well. They don't get it. Right now, this seems like a glorious experiment. "Hey the banks will do blockchain too, we'll optimize the bottom line, we'll recentralize the decentralized. We'll co-opt it. Give it a haircut, put it in a suit, present it up to the board, and we will park it in our innovation lab." Where innovation goes to die. If it's innovative enough, and disruptive enough, everyone in that management chain will get seriously uncomfortable. That's what innovation does.

This morning someone said, "Disrupt yourself." Bullshit. Disruption isn't comfortable, it's not easy, it's not nice. Disruption means losing your job. Disruption means cannibalizing your profit center, it means destroying your fundamental business. You don't do that to yourself. No. You resist stubbornly until the very last moments. Until you can no longer resist. You go the way of Kodak. You invent digital photography in 1987, bury it under the rug, pretend no one sees it, and say, "Hey, we got a good thing going on here with film. Who could ever beat us?" Who? Nokia. Shipped a billion cameras and they're not even a camera company. You can't see that coming. You can't protect from that. You can't co-opt and adjust to that level of disruption.

Engineered currency, designed by a ragtag group of anarchists, cyberpunk, misfits who don't give a shit about your business plan, about your innovation lab, about whether you like it, whether the regulators will legitimize and add credibility and accept, because they are doing now for eight years in Bitcoin. In three years in Ethereum. Laying down on the ground unassailable facts faster than anyone can keep up. By the time the regulators figure out how to regulate 2009 Bitcoin, Z-Cash comes along and slaps them in the face. Who knows what's coming next. Lightening network, payment channels, raiden, smart contracts, 17 ICOs in the last 15 minutes. There are people at the SEC right now with their hair on fire going, "What the hell just happened? I thought you said we were in charge?" No one asked for permission. Guess what? That's what permission-less means.

Permission-less doesn't mean present a business plan and hope someone funds you. Permission-less means, write code, launch code, change the world, ask for forgiveness later, maybe. Do not ask for permission. Engineered money just happened. It is a new form of digital money. This is the Killer App. This will change everything, and eventually, amazing applications will be built on top of this incredible platform for global trust. This new organization model for a decentralized society that scales to fit the global needs of a global society will be built, but first we've got some amazing things to do to money. And they won't even see us coming. Thank you.