Blockchain Debunked: Why one of the most-important technological breakthroughs of all time was never suitable beyond use as a proof-of-concept prototype

Distributed Ledger Protocols, CryptoCurrencies, and why Bitcoin "investors" will be disappointed

Original © December 27, 2017 by Erik Townsend. Revision 1.01 December 31, 2017

Introduction

In my first career I was a distributed systems architect (software guy focused on network stuff). These days I manage a hedge fund and produce the ***MacroVoices*** financial podcast. Since my background seemingly makes me a natural for translating the technology lingo to finance speak, people frequently ask why I've never done a podcast episode focused on Cryptocurrencies. The short answer is because I think Bitcoin is an idiotic mania and I don't want to waste perfectly good air time on it. On the other hand, *Distributed Ledger Protocols* (pioneered by Bitcoin's *Blockchain)* represent a one of the most profound technological advancements of our time.

This paper will argue two seemingly contradicting points:

1. Blockchain, the *Distributed Ledger Protocol (DLP)* that underlies the Bitcoin cryptocurrency, represents a technological breakthrough of historic proportions. Even more profound than the biggest cryptocurrency zealots may realize.

2. Blockchain's design makes it suitable for proving possible something previously thought impossible, and for that it deserves great respect and appreciation. But that said, Blockchain is not, was not, and most likely never will be suitable for widespread use, due to fundamental design shortcomings that limit its suitability to a proof-of-concept laboratory experiment.

This paper will differentiate *Distributed Ledger Protocols* (such as Blockchain) from the *Cryptocurrencies* (such as Bitcoin) they enable. It will explain why DLPs are actually a far more important invention than the cyrptocurrencies that are currently in the public spotlight. **Perhaps most importantly, it will explain why the design of Bitcoin's Blockchain DLP is seriously flawed, not scalable, and generally only worthwhile as a proof-of-concept prototype or until something better comes along.**

I'll use one relatively recent proprietary development called *HashGraph* to illustrate that better solutions to the problem first solved by Bitcoin's Blockchain are in fact possible. I'll then go on to opine on why I believe that first-generation cryptocurrencies including Bitcoin will likely be outlawed and lose most if not all of their value. Finally, I'll describe why government-backed digital currencies based on the same underlying technologies will likely dominate the financial landscape in the future.

BlockChain is a *really* big deal! But…

How can I possibly acknowledge that Blockchain is one of the most important technological advancements of our time, but then in the very next sentence, allege that it's not suitable for prime-time use? To put this in perspective, let's consider another *major* breakthrough which to my thinking is analogous to Bitcoin's Blockchain in many ways:

The Wright Flyer changed everything. The very notion that humans could possibly fly in the air had previously been ridiculed as impossible, despite numerous prior valiant attempts. Today the *Flyer* is preserved in the *National Air and Space Museum* in Washington, DC, and is regarded as one of the most profound technological advancements in human history.

Did Blockchain really deliver a breakthrough as big as the invention of the airplane? Darned close, in my opinion. Certainly as big of a deal as the jet engine, if not the airplane itself. And by the way, the breakthrough is not in any way specific to cryptocurrencies. More on that later.

But hold on… Airlines don't use *Wright Flyers* today. In fact, there was never a compelling reason to build more of them, save for replicas built solely to honor the *Flyer*'s historical significance. So why didn't the Wright brothers build more *Flyers*? Because it was only suitable as a prototype. It didn't even have a pilot seat; the Wrights had to fly it whilst lying down on their stomachs! Thankfully, the Wright's were smart enough to recognize that their revolutionary invention wasn't ready for prime-time. They knew it needed to be refined and further developed before it would have practical value.

The same thing is true of Bitcoin's Blockchain DLP: it's a beautiful prototype that made a profound technology breakthrough, but it's not ready for prime time. Sadly, most people in the cryptocurrency world haven't figured that out yet. I'll substantiate that criticism shortly, but let's start by understanding just why this DLP stuff is such a big deal to start with.

Understanding the Breakthrough

For the entire history of the computer industry, one rule has remained in force, and was thought to be immutable prior to Blockchain: For any information to be stored in a computer system, somebody somewhere has to *own* that information, meaning they are the *central authority* over that data storage. If we're talking about bank account ledgers, the bank is the owner of the data. If we're talking about your driver license records, the state government's motor vehicle registry department is the owner of the data.

An immutable corollary was that the owner of the data always had *control* over the data. The bank could do its best to stop hackers from breaking into its systems, but the bank itself always owned and controlled its own databases. A consequence of this is that if the bank's IT staff could find a way to circumvent precautions the bank put in place to restrict their actions, a rogue programmer or system administrator might be able to over-write the ledger, committing epic financial crimes.

The same principle applies even before the advent of computers. For all of recorded history, the notion of an *account* – whether it be a bank account or otherwise, could only be implemented by designating someone (the bank, in the case of bank accounts) as the ***central authority*** in charge of maintaining the *ledger*, or record of transactions, for that account. In the early days (before computers) an account ledger was a piece of paper kept in a secure room somewhere, with handwritten transaction records recorded on it by a bank clerk.

In the modern age of programmable computers, the account ledger was moved into a computer database, on a centrally located "Mainframe" computer. With the advent of *distributed database management systems* in the late 1980s, it became possible for this database to be physically distributed across a redundant, fault-tolerant network of *server* computers. But even so, it was still necessary that *some central authority owned and controlled the database*.

The critically important aspect of this is that if someone could compromise the *central database*, (i.e. hack the server computer), they could re-write the ledger and perpetrate fraud.

For several decades, it was assumed that anyone who could gain physical access to the computer hardware could fairly easily perpetrate such a crime. That's why banks used to keep armed guards stationed outside their computer rooms.

In recent years, encryption technology and distributed database technology have turned "fairly easily" into "with considerable effort". But the point is, so long as there was a single point of control, if the security measures at that point of control could be overcome, whether by an "insider" or anyone else, the system could be hacked.

When you stop and think about it, the very notion that the bank should be *completely in charge* of the account ledger *never* made sense except for one reason: *someone* had to be in charge of the ledger, and the bank was the logical choice. Surely, a much better solution would be if the ledger were somehow independent such that neither the bank nor anyone else *even had the ability* to "control" or "hack" its contents. ***But prior to the invention of the Bitcoin Blockchain, there was no known way to implement an account ledger that had no central point of control, and therefore, no central point of security vulnerability.***

The anonymous inventors of the Bitcoin Blockchain solved a problem that had persisted not only since the dawn of computers, but literally *forever.* They figured out how to build a distributed account ledger that is spread across a computer network in such a way that *there simply is no central authority or "owner" of the database*. Nobody has control of the database, so nobody can hack the database. Instead, the database exists in many places across a computer network, with many participants incented to continuously check to make sure every transaction is legitimate and no monkey business is going on.

Truly, Blockchain represents a brilliant breakthrough, and to my thinking, every bit as profound and important to the computer industry as the Wright *Flyer* was to the transportation industry. ***It really is that big of a deal.***

But I cannot emphasize this strongly enough: Just like the Wright *Flyer*, Bitcoin and its Blockchain made the enormous contribution of *proving a concept possible*. But just as the Wright *Flyer* was never suitable for airline service, **Bitcoin and its Blockchain are not suitable for their stated purposes either.** Just like the *Flyer*, they represent a *proof-of-concept prototype* that achieved a technological breakthrough. The Boeing 727 of DLPs and cryptocurrencies hasn't been invented yet. As soon as it is, Bitcoin and its Blockchain will find their rightful place where they truly belong – in a technology museum just like the *Flyer*.

While the Boeing 727 of DLPs is probably still a few years off, this stuff is moving much faster than aviation did. It took fully 46 years to get from the Wright Flyer to the de Havilland Comet (first jet airliner). But already hundreds of other DLP designs are already under development. I'll use one called *HashGraph* to illustrate how another approach can overcome the biggest inherent shortcomings of Blockchain. More on that later.

When it comes to Cryptocurrencies (as opposed to the DLPs that enable them), we're not that far along yet. *Ethereum* and its "smart contracts" make significant advances beyond what was pioneered by Bitcoin, but probably more akin to a Junkers F.13 than a Boeing 727 or de Havilland Comet.

Never heard of an F.13? Don't worry… In a few years, nobody will remember Ethereum either. Bitcoin will always be remembered, just like the *Flyer*, but nobody in their right mind will even think about using it to transact business. It will find its place in a museum, just like the *Flyer*.

Yes, you "can so" separate a cryptocurrency like Bitcoin from its DLP (e.g. Blockchain)!!!

A point I've tried to stress when I was interviewed on the *Chat with Traders* and *SuperInvestors* podcasts was to separate the concept of a cryptocurrency (which, for reasons we'll get to later, is of dubious longevity in its present form) from what I think is a far more profound technology breakthrough – the invention of the *secure de-centralized distributed ledger*. (Bitcoin's "Blockchain" was the first such *Distributed Ledger Protocol*, or DLP). What I tried to emphasize was that DLPs have profound importance and myriad applications well beyond enabling secure cryptocurrencies.

The historical significance of the *Flyer* wasn't about carrying one guy a few hundred yards; it was about proving that human flight is possible. Being able to securely store information (such as an account ledger) such that there is no central point of control or vulnerability is so profound an advancement that I'm challenged to fully articulate its significance. *It's a really, really big deal.* A much *bigger* deal than the Bitcoin cryptocurrency that is presently fueling what has become the biggest speculative mania in recorded history[1].

My statements motivated a huge number of people to e-mail me with admonishments alleging that I had no clue what I was talking about. The most common criticism claims that I "obviously don't understand" how Bitcoin and Blockchain work, otherwise I would not "flaunt my ignorance" by asserting that any sort of DLP

[1] Bitcon's price appreciation percentage over time first exceeded the Dutch Tulip Mania in late November, 2017

like blockchain could ever work unless integrated with a cryptocurrency like Bitcoin.

The reason these people think I've missed the point of how all of this works is because of an inherent ***design limitation*** of the Bitcoin Blockchain. My critics correctly understand that Bitcoin's blockchain only works because its network is secured by network participants known as ***miners*** whose motivation to make the network secure depends on being paid for their efforts in the form of newly minted Bitcoin cryptocurrency. My critics reason that without the cryptocurrency component to provide an incentive to for the *miners* to do this very compute-intensive work, the DLP (blockchain) could never function independently from the associated cryptocurrency.

This criticism is just as misinformed as the criticism that the *Flyer* was not historically meaningful because in its original form, it could only carry one person a very short distance. By the way, plenty of people made that exact criticism back in 1903, and dismissed the airplane generally as a novelty invention of trivial historical significance! *In reality, they were just too short-sighted to envision its eventual applications and uses*. I can't help but wonder whether it's the direct descendants of those critics of the airplane who, generations later, keep emailing me with accusations that my emphasis on separating the importance of DLPs from Cryptocurrencies somehow reveals that I don't understand the role *miners* play in the Bitcoin Blockchain DLP.

I'm fully aware of that particular shortcoming of the Bitcoin Blockchain design. But the Bitcoin Blockchain's reliance on *miners* who must be compensated with cryptocurrency is a design flaw, not an immutable law of nature that can never be overcome.

And to be sure, Bitcoin's Blockchain has numerous other shortcomings. I'll discuss them later on, but for now the point is that these flaws can and will be overcome by other DLPs that will not necessarily rely on an associated cryptocurrency to motivate network participants to keep the network secure. *HashGraph* already achieves this to some degree, and there will be others to come. More on those later, but let's focus on how this stuff actually works first.

Understanding the Blockchain DLP

We need a system where transactions cannot be written to the ledger until they are first *validated*, meaning they must be checked by an independent 3rd party to make sure they are legitimate and not fraudulent. *But validated by whom, if there is no central authority in charge of the database?*

For this to work in a distributed peer-to-peer network, it would actually be quite simple to randomly choose just one other party to validate the transaction, *if there were no nefarious actors with bad intentions*. But we have to assume there are such bad actors, and the system has to be designed such that no one bad guy or small group of bad guys can compromise security.

The solution pioneered by Bitcoin's Blockchain gets a whole bunch of network participants involved in the process – and it engages them in a creative way that prevents any one bad actor or small group of bad actors from being able to validate their own bogus transactions. The result is that *there is no central control authority whatsoever*. It's really quite brilliant!

The only way a *block* (a group of generally unrelated transactions) can become a validated part of the official *blockchain* is if all the transactions it contains pass validation procedures which are undertaken in parallel by a whole bunch of network participants known as *miners*.

In theory, it's always possible for the security of the network to be breached by a *really big group of bad guys*. Specifically, if more than half of the participants in the network are bad guys who are colluding with one another, they could do something shady. So the system has to be designed to make sure that no force of evil, no matter how large (not even Goldman Sachs) can ever become "big enough" to represent a *majority* of all the *miners* in the network who are responsible for validating transactions. ***The specific mechanism chosen by Blockchain to address this need (called Proof-of-Work) was a brilliant choice for a proof-of-concept prototype, but it renders Blockchain unsuitable for prime-time use due to scalability limitations.***

The role of Miners and the "Proof-of-Work" design

What if I were to tell you that the central design principle of Bitcoin's Blockchain is a giant network-wide competition to waste electricity and computing capacity, and that each time someone <u>proves</u> that he has just wasted *more electricity and more computational capacity in less time than anyone else in the contest*, he wins a prize paid in freshly-minted bitcoin? I know that sounds utterly ridiculous, and frankly it is. No sane person should ever think this is a good way to run a distributed ledger protocol that is meant to scale up to support a global payment network with tens of thousands of participants. But that's exactly the essence of Blockchain. Seriously.

In the Bitcoin Blockchain system, *miners* are the network participants who validate transactions to make sure they are not fraudulent. This determination is made possible by cryptography, and contrary to popular misconception, the process of <u>transaction verification</u> is *not necessarily overly compute-intensive unto itself*.

Let's first imagine what it would be like if the system were designed for maximum performance (it's not, for reasons I'll soon make clear). All the miner would need to do is pick up a batch of *unverified transactions* and run some checks and balances to make sure they conform to a set of straight-forward security rules and regulations. A really fast computer could probably create a full block of *verified transactions* in a fraction of a second, *and therein lies the problem!*

If a full block of transactions only took a fraction of a second for one miner to validate and compose into a block to be added to the official blockchain, then a bad actor with good financing could buy a whole bunch of super-fast computers and *before you know it, that one bad actor could become more than half of the entire network*, just by having enough computing power to pose as thousands of different independent miners. We clearly can't have that.

So they intentionally made the mining process much more compute-intensive than it actually needs to be, for the express and intentional purpose of slowing the network down dramatically. The whole idea is to make sure that *mining* <u>wastes</u> so much electricity and consumes so much computing capacity that nobody could possibly ever buy enough computers to waste more electricity and computing power than the rest of the network combined is already wasting. Seriously – that's the *design goal.* Read section 4 of the Bitcoin White Paper if you don't believe me.

Is that the *only* way to address the problem of not letting the bad guys outnumber the good guys? Of course not. Then why was it chosen? My guess is that the inventors of Bitcoin didn't foresee the present mania. Indeed, if you wanted to run a small network consisting of a few hundred accounts and perhaps at most a few dozen miners, there's really nothing wrong with a design focused entirely on everyone trying to waste more energy and resources than everyone else. The whole network is small enough that the waste is meaningless in the grand scheme of things. ***But the point is, that solution simply isn't scalable.***

The way Bitcoin's Blockchain works is that for a block of newly verified transactions to become eligible to append to the official blockchain, the miner has to do a bunch of super compute-intensive cryptographic math problems first. *A whole lot of them – specifically, enough compute-intensive work to make it nearly inconceivable that any one bad guy could ever control more than half the mining resources on the network*.

To ensure that advances in computer technology (computers getting faster over time) don't undermine security, the system is actually designed to ***dynamically adjust to make the proof-of-work process even more wasteful*** if blocks start getting created too quickly! Seriously. I swear I'm not making this up.

Bitcoin mining rigs are very expensive high-performance computer systems that consume an extraordinary amount of electricity in order to validate each block that gets added to the blockchain. This is a key point: Many people incorrectly assume that the reason these computers are so heavy-duty is that the process of verifying the actual bitcoin transactions and making them secure is somehow *necessarily* compute-intensive. That's simply not true. The whole process could be done in a small fraction of the time with a small fraction of the computing resources demanded by the Bitcoin Blockchain design. *But if it worked that way, the bad guys could afford to buy enough computers to take over the network.* So they intentionally designed it to be wasteful enough that nobody could afford enough computers to out-waste everyone else.

The most important question to ask at this point is whether there are alternative ways to keep the bad guys from outnumbering the good guys, without being so wasteful? But rather than focusing on that rather obvious question, the whole crypto community has embraced Blockchain, including this massive design shortcoming, as if it were the holy grail.

This "proof-of-work" system was a perfectly reasonable design choice if your goal was to be the Wright *Flyer* – to prove possible something that had never been done before. But it's hardly scalable to run the global economy! This is why Bitcoin's entire network can only process a few transactions per second, at extraordinary cost in terms of electricity consumed validating the blocks.

The ***sole*** *reason the performance is so poor is that they intentionally designed it to be so inefficient that bad guys would not be able to* *beat the system just by buying more computers than everyone else.*

Miner competition makes it worse!

Hang on, the story actually gets worse from there. How does the Bitcoin Blockchain design make sure that the bad guys are not somehow gaming the system so they are the ones to validate their own transactions, and letting their own fraudulent transactions pass through in the process?

The answer is that the miners *compete with one another* for who gets to add the next block to the chain, on the basis that whoever finishes the proof-of-work process (described above) first wins[2].

Once again, in a small proof-of-concept network, this is a perfectly reasonable design choice. The miners are incented to validate transactions into blocks as quickly as they can by competing with one another. The first guy to finish the very long list of math problems wins a prize, paid in Bitcoin.

But here's the problem: Only the winner of the math contest wins the prize. All the runners-up consume about the same amount of electricity in their failing efforts, only to lose the race by a tiny fraction. Once again, in a small proof-of-concept network, it's not a big deal. But if tens of thousands of miners are competing to create the same block, and only one guy wins and gets paid for it, all the others still consumed all that electricity and no good came out of it! **The severity of this problem grows *exponentially* with the size of the network.** The global bitcoin network is *already* estimated to consume more electricity than some small nations. Let that sink in. *More than entire nations.*

Conclusion: Bitcoin's Blockchain isn't ready for "Prime Time" due to scalability limitations

Making the mining process orders of magnitude harder than it really needs to be and then setting up a competition with one winner and a whole lot of electricity-wasting losers was a perfectly valid way to prove the concept, just as the Wright *Flyer* having no cabin or pilot seat or flight instrumentation, and requiring the pilot to fly from a laying-down position was perfectly valid given the task at hand. But if you want to run an airline, you need seats, seatbelts, a pressurized cabin, and some little bags of cocktail pretzels.

Distributed Ledger Protocols will change the world, no doubt about it. Bitcoin's Blockchain was the first to solve the problem, and will forever go down in history, just as the Wright *Flyer* did. But if you want to build a *scalable* cryptocurrency or use a DLP for other serious applications, you need to first overcome these limitations. One example of a DLP that takes a completely different approach to solving the same problems is *HashGraph.* More on that to come.

Bitcoin is the Wright Flyer of Cryptocurrencies

So far, this paper has focused on the shortcomings of Bitcoin's Blockchain as opposed to the shortcomings of the Bitcoin

[2] This is a slight simplification. The longest chain of blocks containing valid proof-of-work hashcodes is the actual determinant of "who wins". But the effect is to create a contest with only one winner, in which all contestants perform the same redundant proof-of-work operation. The amount of electricity and computer hardware wasted on the effort increases exponentially with the size of the network. A new contest begins with each block added to the chain.

cryptocurrency itself. Why start there? Because just as an automobile is only as good as the engine that powers it, a cryptocurrency is only as good as the DLP that enables it. Bitcoin's Blockchain was the world's ***first*** DLP and deserves accolades for being first, just as the Wright *Flyer* did.

But the Wright brothers were smart enough to understand the inherent limitations of the *Flyer*. They knew better than to try and start an airline by building more identical aircraft. Instead, they moved on to their next design.

In some regards, Bitcoin is moving ahead as well. Plans are afoot for a new "Lightning Network" (presumably named by some Apple marketing guy) that will make it faster. But at the end of the day, it's still based on proof-of-work and competition among miners for block completion. These are simply not sensible ways to design a DLP, but for whatever reason, the whole world has become absolutely infatuated with them. I predict this will change very quickly when more robust DLPs have proven themselves both scalable and commercially viable.

Being built on top of a not-ready-for-prime-time DLP (Bitcoin Blockchain) is just where Bitcoin's shortcomings *begin*. The story gets a lot worse, and I'll come back to that. But for now, I want to emphasize one key point:

Bitcoin is not special, nor is it superior, nor is it unique. It was first, and that earns it historic relevance, but nothing more.

My point is that a new cryptocurrency built on a better DLP that is scalable to thousands or hundreds of thousands of transactions per second is going to have *profound* advantages over Bitcoin. Yeah, yeah, I know… Such a crypto doesn't exist yet – the other crypos in existence at the time of this writing all basically copied Bitcoin's severely flawed blockchain design, including all its limitations and shortcomings. ***But that will change.*** When it does, Bitcoin will be relegated to its rightful place in history museums, while the other blockchain-based 1st generation cryptocurrencies are forgotten about entirely.

Just like old baseball cards, Bitcoins will always have some value just because they'll become collector's items. But the fantasies you read on the Internet about Bitcoin replacing the USD as the world reserve currency are abject nonsense, plain and simple.

Now to be clear, I think that it's not only possible but *likely* that a digital currency will eventually replace the USD as the world's reserve currency. But it won't be Bitcoin. More on that later.

Just the advent of a cryptocurrency based on a more scalable DLP should by itself make Bitcoin obsolete, and I expect that will happen within the next year or two at the very latest. But Bitcoin's problems don't end with the shortcomings of the Bitcoin Blockchain DLP.

Other Bitcoin Shortcomings

Bitcoin has a designed-in money supply hard limit of 21 million bitcoins. So-called "hard forks" which split the Bitcoin blockchain into competing products (e.g. Original Bitcoin vs. Bitcoin Cash) will overcome this limitation to some extent, but at the expense of dividing the user community and complicating commercial transactions with the need for exchange rate mechanisms.

Bitcoin buffs usually reframe the 21mm coin money supply limit as a feature, claiming that it recreates the scarcity characteristics of precious metals. This is abject nonsense. If someone else already owns most of the gold, you can't just invent your own parallel precious metal, edit the periodic table of elements as if it were a Wikipedia article, and call it just as good. But you most assuredly ***can*** copy the bitcoin design to create your own just-as-good cryptocurrency, and this is already happening now. In spades.

What's more, given Bitcoin's numerous limitations and shortcomings, it's not too much work to create something that's not only just-as-good, but rather *demonstrably better*. Right now Bitcoin is competing with new entrants that are superior in some regards, but do not command Bitcoin's market share. Time will change that.

For the moment, there is some truth to Bitcoin's claim that its market share is an important differentiator. Because of inherent design shortcomings of Bitcoin's blockchain, the blockchain with the most miners is going to be the safest and most secure. Bitcoin's blockchain legitimately holds that title right now, and Bitcoin proponents are very quick to point out that Bitcoin's blockchain is the "strongest" because it has more miners than the other fledgling cryptocurrencies have.

That all sounds good until someone introduces a new *generation* of cryptocurrency that dumps the flawed Blockchain design and its inherent shortcomings entirely, in favor of a more robust DLP that does not rely on proof-of-work or miner competition in order to securely record transactions in the distributed ledger. I predict this will happen within two years of this writing, probably much sooner.

1st Generation Private Cryptocurrencies are Zombies!

The strongest criticisms of the present generation of cryptos (including Bitcoin) have little to do with technology. Consider the principal objectives of Bitcoin, as espoused by its own designers and proponents:

- It creates a global payment network that can be completely anonymous, with irreversible payments.
- It is impossible for Governments to seize privately held Bitcoins (although they can certainly seize Bitcoins stored in exchanges or external wallets)
- It is impossible for Governments to void or claw back transactions they do not approve of.
- It is impossible for Governments to tax transactions or intercept payments intended for private parties
- It is not possible for Governments to profit from seniorage (the difference between a fiat issuer's cost of producing currency and the value it can sell or exchange that currency for)

To be clear, I personally love these Libertarian ideas, as my personal opinion is that Government already exerts too much control over our lives. But guess what? Here's a newsflash for you: *Governments don't like these ideas.* Not one bit. What's more, people who share my view that Governments *should not* have control over such matters represent only a small minority of society.

Look, I don’t like it either, but my prediction is that governments will soon label 1st-generation private cryptocurrencies like Bitcoin as “tools of terrorism” that nobody but a tax cheat or criminal should have any need or desire for. **And I further predict that the vast majority of the populous will be persuaded by the “logic” that cryptocurrencies are tools of terrorism that need to be outlawed.**

Don’t’ get me wrong – digital currency is not going to go away. I think it very likely that the U.S. Dollar will indeed be replaced in the role of global reserve currency by a new digital currency. But sadly, it will be a government-sponsored digital currency with nearly opposite design objectives.

So YES, digital currency definitely is the future! That part I agree with. But the dominant digital currency of the future is not going to be Bitcoin. The future dominant currency is far more likely to be a new government-backed digital currency I’ll call *The Orwell*. Here are a few of its principal characteristics:

- Every single transaction must record the *International Tax ID number* (iTIN) of both parties to the transaction. Each national government will assign its own Tax ID to each person and company resident within its national jurisdiction. That national TIN plus a country code forms the iTIN, which will be hashed using public-private key encryption.

  Every transaction must record the iTIN of each participant. Every natural person or business entity on earth must affiliate with some national government somewhere, and obtain an iTIN. No valid iTIN, no participation in the digital payment system. End of story. Alternate payment networks that don’t enforce this requirement will be illegal and subject to forfeiture and seizure of all value they contain.

- Any transaction can be voided or clawed back after-the-fact by the national government associated with the iTIN *making* the payment. That government may either seize the payment (diverting it to its own account) or reverse the transaction to credit the original payer’s account, at the government’s sole discretion.

- Any payment can be seized and/or taxed automatically by the national government associated with the iTIN *receiving* the payment.

- Any wallet or coin account anywhere on the network can at any time be viewed, seized, or directly taxed by the national government associated with the account’s registered iTIN. Accounts with no registered iTIN or a bogus iTIN can be immediately seized by government.

- Every transaction including iTIN of all parties, amount, date, time, etc. is all stored in a database that is always available to governments based on each government having visibility to its own citizens’ accounts but not to other jurisdictions.

  Ironically, technology pioneered by the inventors of Bitcoin for the intended purpose of achieving its libertarian features will be used to achieve this functionality.

The whole thing will be sold to the public as an absolutely ***necessary*** measure to combat terrorism and tax cheats, ***and the vast majority of the general public will welcome the new system with open arms.***

My prediction is that we're headed for a modern day "Space Race". It will be a race among nations to create *The Orwell* – the digital currency that will eventually be accepted by international treaty as the new global reserve currency. By the way, the People's Bank of China is already hiring Blockchain engineers to design the *Digital RMB. The PBOC "gets it". They see what's coming and they're taking the lead.* Other central banks will soon follow suit.

The future of cryptocurrency is not Bitcoin. *It's the Orwell.* I don't like it either, but that's what I'm convinced is going to happen. I sincerely hope to be proven wrong.

If there's a future for Private Cryptocurrency, it's front-running the Orwell, not enhancing Bitcoin

There's a lot to be said for the ability of private enterprise to achieve things much more quickly than government bureaucracy. So there may still be a place for a Private crypto to become *THE* standard. But sadly, my prediction is that what will actually occur when private cryptocurrency engineers recognize that government still really is in charge, will amount to "if you can't beat 'em, join 'em, and at least get paid for helping them get what *they* want".

Whether we like it or not, what governments want is the *Orwell*, not *Bitcoin.* Private companies could engineer *The Orwell* much faster and more efficiently than government itself, and this is probably the more likely path for *The Orwell* to be developed, on top of a much more robust, scalable DLP which doesn't suffer the myriad shortcomings of the Blockchain design.

I'm dumbfounded by some of the inane arguments I've read suggesting Private cryptocurrency is immune from being outlawed by government. "*They can't take it away from us! That would be unconstitutional!!!"*

Look, the U.S. Government stopped obeying its own Constitution more than a decade ago. Just about anything done in the name of "fighting terrorism", including the 2011 *National Defense Authorization Act*, which legalized the indefinite detention of U.S. Citizens without probable cause, goes forward without challenge by the Supreme Court. Do you really, seriously think they can't take away your cryptocurrency system which was *designed* to make it impossible for governments to seize or control payments that could be used to finance terrorism? I suggest you think again.

While it would be difficult to impossible for governments to prevent the continued existence of a *network* like Bitcoin, they can and will outlaw the exchange of Bitcoin for fiat currency, and they can and will enact laws allowing anyone caught trading Bitcoin for monetary value to have their Bitcoin confiscated on the spot.

When they do these things, it won't completely defeat the Bitcoin network, but at that point Bitcoin really will become what governments previously alleged it was – the exclusive playground of criminals. The people caught trading Bitcoin for fiat after that won't be treated nicely.

Moving on from Cryptocurrencies, let’s return to a subject that’s actually worthwhile: The next generation of DLPs.

The first generation of cryptocurrencies (Bitcoin, LiteCoin, Ethereum, etc) are all (to the best of my admittedly limited knowledge) based on one variant or another of the original *Blockchain* design pioneered by Bitcoin. See earlier discussion for the myriad shortcomings of Blockchain.

I’ll describe how *HashGraph* fits into this story in just a moment, but first I want to be really emphatic on this point: I have no clue what the “gold standard of DLPs” will be. Nobody does. We’re way too early in this story to know. The Wright brothers were smart enough to recognize the *Flyer* had pretty much served its purpose once the first flights were made. They knew it didn’t have much practical application beyond that, and so they immediately moved on to the next design.

Sadly, it seems the Bitcoin crowd isn’t as able to see the obvious as the Wright brothers, so they’re babbling about how the *Flyer* (Bitcoin) is going to revolutionize the world and replace the USD as global reserve currency. I have no idea how long this hysteria will continue. It’s already surpassed the *Dutch Tulip Mania* on a percentage price appreciation over time basis, so who knows how much farther it can go from here.

So let’s focus on where DLP technology *needs to go*, not where it’s presently stuck due to irrational human behavior. We need to advance this DLP concept so that we can have a secure distributed ledger that does <u>not</u> require use of a proof-of-work algorithm, and which does <u>not</u> require miners to compete with one another, wasting exponentially larger amounts of electricity as the size of the network increases. Ideally, we should find a way to do this that eliminates the need for “miners” entirely.

The MAIN POINT of this paper…

Reviewers of the first draft thought it read as if I were saying Blockchain is not the right long-term solution but *HashGraph* is. Nothing could be farther from my intent. So let me clarify before introducing *HashGraph:*

- The important point is that the *Proof-of-Work* and *Miner Competition* aspects of Bitcoin’s BlockChain are not the ONLY way to solve the problem of preventing bad guys from taking over the network.

- I’m introducing *HashGraph* solely to illustrate how another DLP took another approach. Whether *HashGraph will rise to become the gold standard of DLPs is something I have no opinion on because I’ve not evaluated its dozens if not hundreds of competitors.*

- ***The point is, regardless of whether it’s HashGraph or something else, somebody is going to invent a better mousetrap that doesn’t involve a network-wide contest to see who can waste the most electricity and computing resource the fastest! When a leader emerges, Bitcoin’s Blockchain will be relegated to museum duty soon thereafter.***

Enter *HashGraph*

Look, I have no idea whether *HashGraph* really has the potential to become the de Havilland Comet (first commercial jet airliner) of DLPs, or if it's more akin to the Lockheed Electra (the earlier propeller-driven passenger plane aviatrix Amelia Earhart famously disappeared in). I also want to be clear that I only know a tiny bit about *HashGraph* – after watching a couple of videos featuring its inventor, Leemon Baird. **I really have no idea how HashGraph compares to its many competitors. The sole reason I'm introducing it now is to show that other DLP designs are possible, which do not rely on integration with a cryptocurrency, Proof-of-Work, or Miners.** So let's briefly review *HashGraph's* strengths and weaknesses.

For starters, *HashGraph* is another *Distributed Ledger Protocol (DLP)*, which means it has the same basic purpose as Bitcoin's Blockchain: to provide a secure distributed ledger that has no central point of control, and therefore, no central point of vulnerability. Just like Bitcoin's Blockchain, the idea is that transactions are verified as legitimate and non-fraudulent before they can be added to the permanent, shared ledger. So functionally, it's pretty much the same thing as blockchain. But the similarities end there. Key differences include:

- There are no blocks, and therefore, no block *chain*. Transactions are added to a shared distributed ledger called the *HashGraph*.

- Unlike Bitcoin's Blockchain, "miners" are not needed to verify and validate transactions. Therefore, it becomes possible to support applications that have nothing to do with any cryptocurrency. Contrast with Bitcoin's Blockchain, where you need to have the Bitcoin cryptocurrency because small awards of Bitcoin are needed to motivate *miners* to compete with one another to see who can waste the most electricity fastest while validating blocks and adding them to the blockchain.

- *HashGraph* does not rely on a proof-of-work algorithm nor does it rely on competition between miners to verify transactions. As a direct result, it is orders of magnitude faster and more efficient than Bitcoin's Blockchain, and does not require the presence of a cryptocurrency to reward "miners", because there are no miners in the HashGraph design.

- *HashGraph* still has to contend with the same challenges that Bitcoin's Blockchain solved with the *proof-of-work* algorithm and the *miner* system, but it solves those challenges in completely different ways, instead relying on two principal new innovations called *gossip about gossip* and *virtual voting.* More on those later.

- Unlike Bitcoin's Blockchain, *HashGraph* was ***not*** designed as part of an integral DLP-cryptocurrency. Rather, *HashGraph* is a generic DLP which can work with or without a cryptocurrency. Swirlds (the company behind *HashGraph)* doesn't presently plan to offer a cryptocurrency of their own; they are focused on being the best DLP they can be, and they leave it to others to build one or more cryptocurrencies on top of their DLP platform.

Is there a catch? How is this possible?

Are you questioning how it could even be possible for *HashGraph* to achieve everything that Bitcoin's BlockChain achieves, without the need for miners or having to incentivize them with cryptocurrency payments? And it achieves several orders of magnitude of performance improvement at the same time?

Well if you're not wondering that, you should be. Things that seem too good to be true often turn out not to be true, and there are a lot of really phenomenal claims being made in the sales pitch for *HashGraph*. I've never tested or evaluated this software myself, so I'm going only by what little I know from Swirlds.com, which should clearly be treated with caution since the information comes from people who have a product to sell. But from what little I can tell, their story seems reasonably credible.

I'll come back to how *HashGraph* actually works, but first, let's start with some more fundamental concepts.

The Proof is in the Proofs!

If there's one thing I can tell you authoritatively based on my own career in this field many years ago, it's this: When you're talking about whether or not a distributed system is truly secure, you need to be able to prove it with solid math.

Mathematical proofs are the buzzword here. All it means is that there are solid mathematical equations that prove whatever claims are being made about security beyond any shadow of doubt. The next thing I can tell you is that these *mathematical proofs* are only as good as the extent to which they've been scrutinized by experts who really know their stuff. That part is beyond my pay grade, I'm afraid.

The first thing that impressed me watching Leemon Baird's videos was his frequent references to mathematical proofs. This guy clearly "gets it" in the sense he understands the proofs are what's important.

But the second part is even more important – to what extent have Mr. Baird's mathematical proofs been scrutinized by cryptography experts who really know their stuff? I have no idea, but I can assure you that's the most important question to ask here. My guess would be that because *HashGraph* is new and relatively unknown, the math behind it has probably not yet been subjected to nearly the same degree of mathematical scrutiny that the Bitcoin system has received over the past 8 years since its inception.

Bitcoin is Open Source

One serious caveat about *HashGraph* is that it's a proprietary system, whereas Bitcoin's Blockchain is open source. Let me explain what that means.

The software programs that run the Bitcoin/blockchain network are published in the public domain. Ok, so what? The relevant point here is that every hacker on the planet knows that the ultimate claim to hacker fame would be to be the first guy who figured out how to crack the Bitcoin/Blockchain network and find a way to get away with fraudulent Bitcoin transactions.

All over the world, right this instant, there are literally thousands of computer programmers poring over the Bitcoin/Blockchain source code, looking for even just the smallest mistake that could somehow be exploited to create a security breach. And that's really not an exaggeration – literally thousands of computer programming experts are constantly reading and re-reading the Bitcoin/Blockchain source code. Some of them are bad guys hoping to find a way to cheat the system. The rest are good guys who want to find and correct problems before the bad guys find them, because uncovering such flaws leads to something akin to rock star status in hacker circles.

At the end of the day, the point is simply that a LOT of smart people are trying every day to find something wrong with the Bitcoin/Blockchain programming. That's a pretty impressive safety valve – if Bitcoin had a security hole in it, somebody almost certainly would have found it by now.

A proprietary system like *HashGraph* certainly gets scrutinized by its prospective customers, but not to the extent that is possible with an open-source system.

How *HashGraph* works…

With those disclaimers firmly in place, I'm quite impressed by Mr. Baird based on what I've seen of his work so far. He's working with two very well-known, solid ideas – *gossip protocol* and *voting protocol*, both of which are old news in distributed computing. They're both very solid ideas, but in their original form they just don't scale to meet the need. Baird has enhanced them with two new innovations, *Gossip about Gossip*, and *Virtual Voting*, and he may have made a breakthrough of his own in the process.

HashGraph seeks to solve the same problem as Bitcoin's Blockchain, but without needing (or having to pay) "miners" to validate transactions in a proof-of-work architecture. Instead the idea is that the participants in the network share transactions with one another so that everyone gets a chance to double-check the validity of each transaction. Remember, with no "proof of work" algorithm, they don't have massively tedious math problems that require numerous dedicated GPUs to solve. So checking all the transactions isn't that much overhead for the other guys in the network to take on.

HashGraph gets the word out about new transactions using a very old and well-known approach called a *gossip protocol*. It's really simple; think about what happens when a friend tells you a really funny joke. You tell everyone you know. Then they tell everyone they know. And so on. Very quickly, the whole town has heard the joke.

A *gossip protocol* is exactly the same thing. All it means is that when each participant in the network learns of a new transaction (hears the joke), they pass it on to their friends. Very quickly almost everyone on the network has the message. *It's possible that a few never get it, but that doesn't matter*. The point is, enough people got the message that if anything is wrong with the transaction not meeting credibility standards, enough people are paying attention that somebody will notice and call foul.

So now, thanks to the *gossip protocol*, most participants on the network know about all the unverified transactions. *So how should the system decide whether to validate each transaction?*

A *voting protocol* is exactly what it sounds like. All the participants on the network could make their own assessment of whether the transaction passes muster. Then they all vote on each transaction, passing their votes to one another through the network. This works, and could in theory achieve a workable DLP solution.

But just like Bitcoin's Blockchain, a DLP based solely on *gossip and voting protocols* might be suitable for a proof-of-concept prototype, but definitely not ready for prime time. The reason is the inefficiency of the voting protocol. It just takes too long to conduct a vote over a large distributed network in order to approve every single transaction. It would be just as bad as Bitcoin Blockchain's proof-of-work architecture, if not worse!

Gossip about Gossip and *Virtual Voting*

The essence of *HashGraph* is Leemon Baird's idea that in any system with defined rules for how each participant *should* vote, the outcome of a vote is *predictable* if one knows what information has been provided to each voting participant in the network.

Gossip about Gossip simply means extending the time-tested *Gossip protocol* to make it possible for any participant in the network to know what information each of the other participants has about a given transaction, including when they got that information and who they got it from.

Virtual Voting eliminates the need for an actual vote, by relying on information derived from *Gossip about Gossip* to predict how other network participants *should* vote without the need for a network message to ask them to express that vote directly.

Watching Baird's videos on the subject led me to as many new questions as answers… How do I know the information I have about how others *should* vote was not tampered with by a nefarious participant in the *gossip about gossip* network? Without a proof-of-work model, what stops well-heeled bad guys from taking over the network by becoming more than half of its participants? The questions only begin there…

Does all this *gossip about gossip* and *virtual voting* stuff really work? *Is the math solid?* Is it really secure enough to conduct financial transactions with? I don't know. Baird says it works, and he seems like a credible guy, but I've not done any due diligence research whatsoever on *HashGraph*.

The way these things get sorted out in world of science and engineering is that a guy like Baird prepares *mathematical proofs* to support his claims, then announces that he's invented something revolutionary and *invites anyone to find fault with his mathematical proofs*. Those words *"find fault with my mathematical proofs"* are basically the computer-geek equivalent to Client Eastwood's famous line, "*Go ahead, Punk. Make my day".*

If the invention being claimed is significant, which Baird's *HashGraph* certainly is, a small army of mathematicians and cryptography experts will try their best to "*make his day"* by proving him wrong, publicly. Again, the only way we really know with certainty that something like *HashGraph* really is bulletproof is when it gains enough attention that the smartest math and crypto geeks in the world feel motivated to try their best to break it, but then fail in doing so. We're not there yet.

Baird is doing exactly the right thing with his videos: He's basically waving a flag at the math and crypto community, effectively saying "Hey guys, I invented something really cool. *Go ahead punks, make my day*! Try to find fault with my proofs. *I dare you!".* There's no doubt in my mind he's doing this consciously and intentionally, because he knows that the one thing that will make his invention immensely valuable is when the very best minds in the field try and then fail to find fault in his work. The *mathematical proofs* are the key to all of this.

CONCLUSIONS

Bitcoin and its Blockchain DLP are the Wright *Flyer*s of DLPs and digital currencies. The importance of this new DLP invention could arguably be as important as the invention of the airplane. The Bitcoin cryptocurrency is only one small, relatively unimportant example of what DLPs can be used for.

Both Bitcoin and its Blockchain are proof-of-concept quality at best. They have profound importance to *history* but little practical viability, despite the present mania surrounding them. They will eventually both be replaced by much more robust solutions that eliminate the serious shortcomings of Blockchain's reliance on miners to validate transactions and the proof-of-work architecture that serves only to slow down the network and make it painfully inefficient and wasteful of electricity and other resources.

Will Leemon Baird's *HashGraph* be the next big advancement in this field, or will it be a soon-forgotten relic after someone comes along and finds fatal flaws in Baird's math? *I have no idea*. But I'm confident that regardless of whether Leemon Baird has *already* invented a DLP that doesn't need Bitcoin Blockchain's miners and proof-of work architecture, someone somewhere will invent one, sooner or later. And that won't be the last advancement in this nascent field.

Just as airplanes evolved from the *Flyer* to single-engine piston-engine propeller planes to multi-engine planes and eventually pressurized jets, this field is still in its infancy. We're only just at the stage of waiting to see what comes next after the Wright Flyer (Bitcoin and its Blockchain). There will be several evolutionary generations to come.

If I were able to prescribe an improvement for this whole process, it would be this: The crypto community needs to stop treating the Wright Flyer (Bitcoin/Blockchain) as if it were the holy grail, and instead refocus on moving ahead with the much more important task of advancing the field toward the eventual introduction of the Boeing 727. The prototype has already served its purpose. We need to standardize around a DLP that doesn't depend on miners or Proof-of-Work, and which can operate with or without an associated cryptocurrency.

To put in context just how "big" all of this is, I'm reminded of the introduction of the IBM Personal Computer in 1980. The best visionaries of the day were quick to say the PC would change everything. But when challenged to describe *exactly how* PCs would actually be used, they generally couldn't come up with many credible examples. Believe it or not, the most common answer given at the time (yes, I'm old enough to remember) was that you might use your PC to balance your checkbook. Even the most forward-thinking visionaries could seldom come up with better examples, *because they didn't know yet. Nobody did.*

What those visionaries *did* know was that suddenly, it was possible to put approximately the same computational capacity of the multi-million dollar "mini-computers" of only a few years earlier in a package that a normal person could afford to own for personal use. The visionaries looked back on how the mini-computer, when first introduced, was thought to primarily be useful only in science and engineering applications, such as calculating rocket flight paths for NASA. That was analogous to the checkbook balancing application envisioned for the PC.

Nobody predicted that police officers would soon be able to call in a driver license number over a 2-way radio, and have a dispatcher logged into a mini-computer tell them whether the driver had a criminal record. Nobody predicted that hospitals would use mini-computers to organize and store medical records, delivering new efficiencies that would directly result in saved lives. Nobody predicted that extremely inefficient manual processes for things like air traffic control would be automated with mini-computers.

So the visionaries who correctly predicted that the PC would change the world had no idea what the PC would eventually be used for. They just knew how much had been accomplished when the exact same amount of technology had only a few years earlier been made available for "only" a few million dollars. And now it was being made available for only a few thousand. They knew it would lead to innovation on a scale that could never be fully anticipated in advance, and that's exactly what happened.

The analogy here is that for the entire life of the computer industry, there always had to be a central point of ownership and control for any stored information. ***Always***. It has ***never*** before been possible to have an account ledger with no owner, where *nobody* (including the bank itself) has the ability to cheat. Now all of that has changed. This literally changes everything. ***It will take a long time for the Information Technology field to even get their heads around the significance of this development.***

Why can't I cite better examples to illustrate just how big a deal DLPs are going to be? For the exact same reason that the best example the visionaries in 1980 could come up with was the "balance your checkbook" application for the PC. *Because the ultimate answer depends on profound degrees of innovation that have now been enabled by the invention of DLP, but the innovation itself has yet to occur.*

Bitcoin's Blockchain was the Wright *Flyer* of DLPs, and it's a pity that the Bitcoin crowd has yet to recognize just how seriously flawed its design truly is. If they could see the picture clearly, they would realize that Bitcoin is a flash-in-the-pan cryptocurrency that belongs in a museum.

Don't get me wrong – digital currencies are definitely going to be the thing of the future. But like it or not, issuance of legal tender has always been the province of government. The only reason Bitcoin has been allowed to come as far as it has is because governments are notoriously slow and inefficient, and are only just now beginning to realize how seriously cryptocurrencies threaten to undermine the power of central banks.

Bitcoin and the other blockchain-based cryptocurrencies will be forgotten soon after the emergence of a viable digital currency based on a more robust, scalable DLP. It remains to be seen what technology will emerge as the preeminent de-facto gold standard of DLPs. *HashGraph* is but one of many contenders. But sooner or later, someone will figure out how to build a digital currency that doesn't suffer the serious limitations and drawbacks of Bitcoin's deeply flawed blockchain architecture.

Government's degree of response and involvement will be critical. While I'm the first to predict that governments' participation will probably do more harm than good, that doesn't mean it won't happen. Governments can and will outlaw digital currencies that threaten the government's power. And despite its myriad technical shortcomings, Bitcoin already poses such a threat, even if governments have been slow to recognize it.

Technology will advance far more quickly than government will be able to regulate it. But eventually, governments themselves will want in on the game, and will decree that only they have the authority to issue digital currency.

To be sure, there will be a black market for cryptocurrencies. It's next to impossible for governments to stop a network like *Bitcoin* from *existing*. What they can do quite effectively is to outlaw their use for financial transactions, and impose rules allowing law enforcement officials to seize cryptocurrency. That, in turn, will lead to new innovations to prevent such government seizures. So I envision both a legal and a black market evolving for cryptocurrencies. Sadly, the ones that share Bitcoin's values for preventing government from unduly interfering in the financial affairs of the people will be deemed illegal, and relegated to the crypto black market.

One things's sure: We live in interesting times, and this whole thing has just barely begun. DLP (not cryptocurrency) is the most important innovation here, and its potential is unlimited. Digital currencies will also be very important, but unfortunately their future is likely to be determined more by actions of government than advances in technology.

Revision History

1.01 31-Dec-17: Reviewers said the first draft read as if I were suggesting that *HashGraph* is the clear solution and was likely to become the preeminent DLP. I've edited to make it clearer that *HashGraph* is cited merely as *one example*, and was included only to illustrate that it clearly is possible to design a DLP without reliance on Blockchain's Proof-of-Work and Miner concepts. Also fixed several typos and spelling errors.