Jimmy Song Follow
Bitcoin Educator, Developer and Entrepreneur/PGP Fingerprint: C1D7 97BE 7D10 5291 228C D70C FAA6 17E3 2679 E455
May 14 · 10 min read

Why Blockchain is Hard

The hype around blockchain is massive. To hear the blockchain hype train tell it, blockchain will now:

1. Solve income inequality
2. Make all data secure forever
3. Make everything much more efficient and trustless
4. Save dying babies

What the heck is a blockchain, anyway? And can it really do all these things? Can blockchain bring something amazing to industries as diverse as health care, finance, supply chain management and music rights?

And doesn't being for Bitcoin mean that you're pro-blockchain? How can you be for Bitcoin but say anything bad about the technology behind it?

In this article, I seek to answer a lot of these questions by looking at what a blockchain is and more importantly, what it's not.

What is a blockchain?

To examine some of these claims, we have to define what a blockchain is and herein lies a lot of the confusion. Many companies use the word "blockchain" to mean some sort of magical device by which all their data will never be wrong. Such a device, of course, does not exist, at least when the real world is involved.

WHERE SHOULD WE FOCUS THIS YEAR?
"BLOCKCHAIN"
IT WILL CHANGE EVERYTHING.
EVERYBODY IS TALKING ABOUT IT.
THE POTENTIAL APPLICATIONS ARE ENDLESS.
WE DON'T WANT TO BE LEFT BEHIND.
WHAT EXACTLY IS BLOCKCHAIN?
ALSO, "ARTIFICIAL INTELLIGENCE"
TOM FISH BURNE
© marketoonist.com

So what is a blockchain? Technically speaking, a blockchain is a linked list of blocks and a block is a group of ordered transactions. If you didn't understand the last sentence, you can think of a blockchain as a subset of a database, with a few additional properties.

The main thing distinguishing a blockchain from a normal database is that there are specific rules about how to put data into the database. That is, it cannot conflict with some other data that's already in the database (consistent), it's append-only (immutable), and the data itself is locked to an owner (ownable), it's replicable and available. Finally, everyone agrees on what the state of the things in the database are (canonical) without a central party (decentralized).

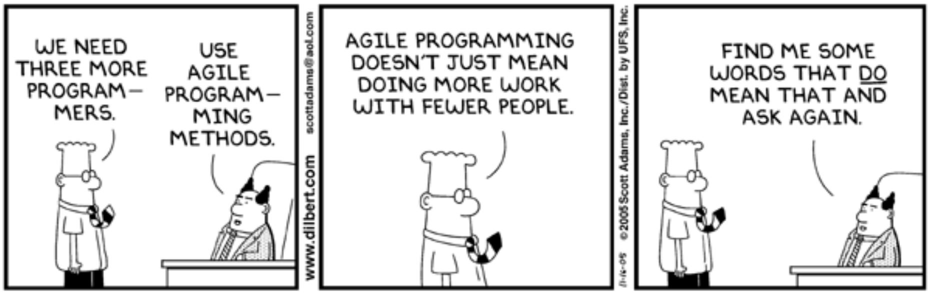
It is this last point that really is the holy grail of blockchain. Decentralization is very attractive because it implies there is *no single point of failure*. That is, no single authority will be able to take away your asset or change "history" to suit their needs. This immutable audit trail where you don't have to trust anyone is the benefit that everyone that's playing with this technology is looking for. This benefit, however, come at a great cost.

The Cost of Blockchains

The immutable audit trail uncontrolled by any single party is certainly useful, but there are many costs to create such a system. Let's examine some of the issues.

Development is stricter and slower

Creating a provably consistent system is not an easy task. A small bug could corrupt the entire database or cause some databases to be different than other ones. Of course, a corrupted or split database no longer has any consistency guarantees. Furthermore, all such systems have to be designed from the outset to be consistent. There is no "move fast and break things" in a blockchain. If you break things, you lose consistency and the blockchain becomes corrupted and worthless.

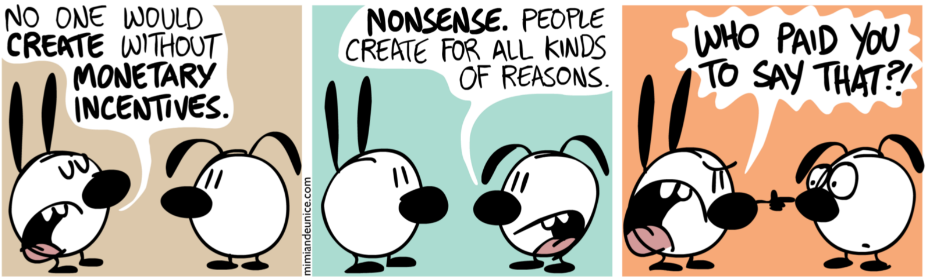

WE NEED THREE MORE PROGRAM–MERS.
USE AGILE PROGRAM–MING METHODS.
scottadams@aol.com
www.dilbert.com
AGILE PROGRAMMING DOESN'T JUST MEAN DOING MORE WORK WITH FEWER PEOPLE.
© 2005 Scott Adams, Inc./Dist. by UFS, Inc.
FIND ME SOME WORDS THAT DO MEAN THAT AND ASK AGAIN.

© Scott Adams, Inc./Dist. by UFS, Inc.

You may be thinking, why can't you just fix the database or start over and move on? That would be easy enough to do in a centralized system, but this is very difficult in a decentralized one. You need consensus, or the agreement of all players in the system, in order to change the database. The blockchain has to be a public resource that's not under the control of a single entity (decentralized, remember?), or the entire effort is a very expensive way to create a slow, centralized database.

Incentive structures are difficult to design

Adding the right incentive structures and making sure that all actors in the system cannot abuse or corrupt the database is likewise a large consideration. A blockchain may be consistent, but that's not very useful if it's got a lot of frivolous, useless data in it because the costs of putting data into it are very low. Neither is a consistent blockchain useful if it has almost no data because the costs of putting data into it are very high.


NO ONE WOULD CREATE WITHOUT MONETARY INCENTIVES.
mimiandeunice.com
NONSENSE. PEOPLE CREATE FOR ALL KINDS OF REASONS.
WHO PAID YOU TO SAY THAT?!

What gives the data finality? How can you ensure that the rewards are aligned with the network goals? Why do nodes keep or update the data and what makes them choose one piece of data over another when they are in conflict? These are all incentive questions that need good answers and they need to be aligned not just at the beginning but at all points in the future as technology and companies change, otherwise the blockchain is not useful.

Again, you may be wondering why you can't "fix" some broken incentive. Once again, this is easy in a centralized system, but in a decentralized one, you simply cannot change anything without consensus. There's no "fixing" anything unless there's agreement from *everyone*.

Maintenance is very costly

A traditional centralized database only needs to be written to once. A blockchain needs to be written to thousands of times. A traditional centralized database needs to only checks the data once. A blockchain needs to check the data thousands of times. A traditional centralized database needs to transmit the data for storage only once. A blockchain needs to transmit the data thousands of times.

The costs of maintaining a blockchain are orders of magnitude higher and the cost needs to be justified by utility. Most applications looking for some of the properties stated earlier like consistency and reliability can get such things for a whole lot cheaper utilizing integrity checks, receipts and backups.

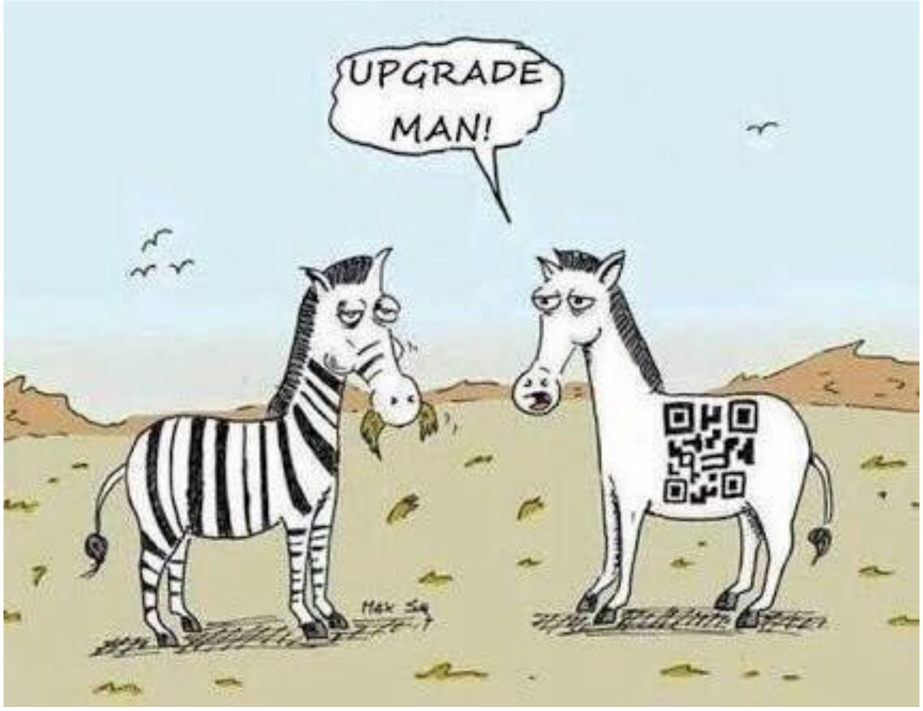
Users are sovereign

This can be really good as companies don't like the liability of having user data in the first place. This can be bad, however, if the user is "misbehaving". There's no way to kick out the user that's spamming your blockchain with frivolous data or has figured out a way to profit in some fashion that causes other users lots of inconvenience. This is related to the above observation that incentive structures have to be designed really, really well in that a user that figures out an exploit is not likely to give that up, especially if there's profit for the user.

You may be thinking that you can simply refuse service to malicious users, which would be very easy to do in a centralized service. However, unlike a centralized service, refusing service is difficult because no single entity has the authority to kick anyone out. The blockchain has to be impartial and enforce the rules defined by the software. If the rules are insufficient to deter bad behavior, you're out of luck. There is no "spirit" of the law here. You simply have to deal with malicious or misbehaving actors, possibly for a very long time.

All upgrades are voluntary

A forced upgrade is not an option. The other players on the network have no obligation to change to your software. If they did, such a system would be much easier, faster and cheaper to build as a centralized system. The point of a blockchain is that it's not under the control of a single entity and this is violated with a forced upgrade.



Instead, all upgrades have to be backwards-compatible. This is obviously quite difficult, especially if you want to add new features and even harder when thinking from a testing perspective. Each version of the software adds a lot to the test matrix and lengthens the time to release.

Again, if this were a centralized system, this would be very easy to correct by no longer servicing older systems. You cannot do this, however in a decentralized system as you cannot force anyone to do anything.

Scaling is really hard

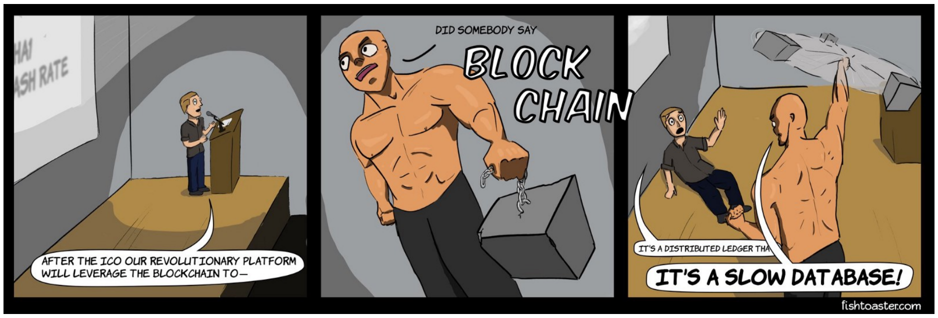
Finally, scaling is at least several orders of magnitude harder than in a traditional centralized system. The reason is obvious. The same data has to live in hundreds or thousands of places than in a single place. The overhead of transmission, verification and storage is enormous as every single copy of the database must pay them instead of those costs being paid just once in a traditional, centralized database.

You can, of course, reduce the burden by reducing the number of nodes. But then at that point, why do you need a decentralized system at all?

Why not just make a centralized database if scaling costs are the main concern?

Centralization is a lot easier

If you notice a theme, it's that decentralized systems are very difficult to work with, expensive to maintain, hard to upgrade and a pain to scale. A centralized database is much faster, less expensive, easier to maintain and easier to upgrade than a blockchain. So why do people keep using the word blockchain as if it's some panacea for all their problems?


HA!
ASH RATE
AFTER THE ICO OUR REVOLUTIONARY PLATFORM WILL LEVERAGE THE BLOCKCHAIN TO—
DID SOMEBODY SAY
BLOCK CHAIN
IT'S A DISTRIBUTED LEDGER THA
IT'S A SLOW DATABASE!
fishtoaster.com

First, a lot of these industries that are being sold on blockchain are really overdue for IT infrastructure upgrades. Health care has notoriously terrible software. Financial settlement is still running on software from the 70's. Supply chain management software is both difficult to use and hard to install. Most companies in these industries resist upgrading because of the risk involved. There are lots of infrastructure upgrades that cost hundreds of millions and end up being rolled back anyway. Blockchain is a way to sell these IT infrastructure upgrades and make them a bit more appetizing.

Second, blockchain is a way to look like you're on the leading edge of technology. Like it or not, the word "blockchain" has taken on a life of its own. Very few people actually understand what it is, but want to appear hip so use these words as a way to sound more intelligent. Just like "cloud" means someone else's computer and "AI" means a tweaked algorithm, "blockchain" in this context means a slow, expensive database.

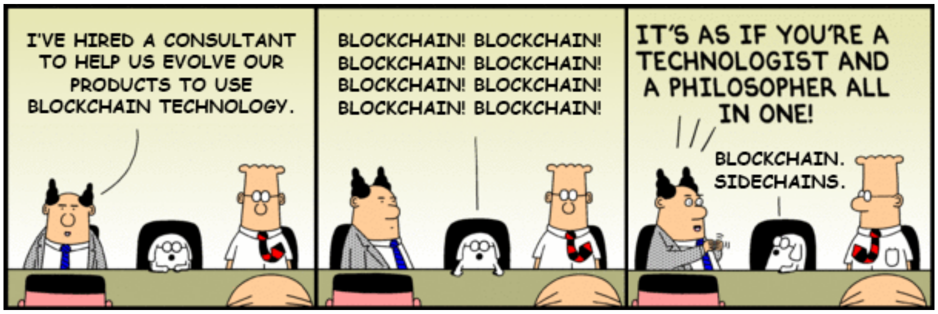
Third, people really don't like government control of certain industries and want a different adjudication mechanism than the legal framework which is often slow and expensive. To them, "blockchain" is really just a way to get rid of the heavy apparatus of government regulation. This is overselling what blockchain can do. Blockchain doesn't magically take away human conflict.

The result is a lot of people that are hyped up on the promises without actually understanding the abilities or costs. What's worse, the actual technical details and costs are abstracted away from a lot of VCs and executives in such a way as to obscure what a blockchain can and can't do. Everyone under them become afraid to say that the emperor has no clothes and we have the situation that we have now.

So what is blockchain good for?

We've already established that a blockchain is very expensive relative to centralized databases. So the only reason you should be using a blockchain is to decentralize. That is, remove the single point of failure or control.

This naturally means that the software or database must not change things around often, if at all. There should be little upside to upgrading and much downside to screwing up or changing the rules.


I'VE HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO USE BLOCKCHAIN TECHNOLOGY.
BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN!
IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!
BLOCKCHAIN. SIDECHAINS.

Most industries are not like this. Most industries require new features or upgrades and the freedom to change and expand as necessary. Given that blockchains are hard to upgrade, hard to change and hard to scale, most industries don't have much use for a blockchain.

The one exception we've found is money. Unlike most industrial use cases, money is better if it doesn't change. Immutability and difficulty in changing the rules is a positive for money and not a detriment. This is why blockchain is the right tool for the job when it comes to Bitcoin.

What's clear is that a lot of companies looking to use the blockchain are not really wanting a blockchain at all, but rather IT upgrades to their particular industry. This is all well and good, but using the word "blockchain" to get there is dishonest and overselling its capability.

Conclusion

Blockchain is a popular term these days and unfortunately, this "blockchain not Bitcoin" meme won't die. If you are a centralized service, a blockchain doesn't get you anything that you can't do a thousand times cheaper with a centralized database. If you are a decentralized service, then you're probably fooling yourself and not thinking about the single points of failure that exist in your system. There wouldn't be a "you" at all in a truly decentralized service.

Biggest joke in this entire article

Back in the early 2000's, there was a push by a lot of executives in the tech industry to use Java and XML. Despite these two things being *tools* and not actual products, many executives insisted on their use, no matter how poor the fit was to what their engineers were trying to achieve. Blockchain is very much like that. Focus on the problems you're solving and the tools will make themselves readily apparent. Focus on tools that you want to use and you'll end up making Rube Goldberg machines that don't do anything particularly well.

In a sense, current conceptions of blockchain are trying to do the impossible. They want the security of a decentralized system with the control of a centralized one. The desire is the best of both worlds, but what they end up getting is the worst of both worlds. You get the costs and difficulty of a decentralized system with the failure modes of a centralized one.

Blockchain is used way too much as a buzzword to sell a lot of useless snake oil. The faster we get rid of the hype, the better off long-term we'll all be.