Bitcoin is Less Secure than Most People Think

by Alex Tabarrok *January 7, 2019 at 7:25 am in* **Economics**, **Law**, **Web/Tech**

I spent part of the holidays poring over Eric Budish's important paper, The Economic Limits of Bitcoin and the BlockChain. Using a few equilibrium conditions and some simulations, Budish shows that Bitcoin is vulnerable to a double spending attack.

In a double spending attack, the attacker sells say bitcoin for dollars. The bitcoin transfer is registered on the blockchain and then, perhaps after some escrow period, the dollars are received by the attacker. As soon as the bitcoin transfer is registered in a block–call this block 1–the attacker starts to mine his own blocks which do not include the bitcoin transfer. Suppose there is no escrow period then the best case for the attacker is that they mine two blocks 1′ and 2′ before the honest nodes mine block 2. In this case, the attacker's chain–0,1′,2′–is the longest chain and so miners will add to this chain and not the 0,1… chain which becomes orphaned. The attacker's chain does not include the bitcoin transfer so the attacker still has the bitcoins and they have the dollars! Also, remember, even though it is called a *double*-spend attack it's actually an n-spend attack so the gains from attack could be very large. But what happens if the honest nodes mine a new block before the attacker mines 2′? Then the honest chain is 0,1,2 but the attacker still has block 1′ mined and after some time they will have 2′, then they have another chance. If the attacker can mine 3′ before the honest nodes mine block 3 then the new longest chain becomes 0,1′,2′,3′ and the honest nodes start mining on this chain rather than on 0,1,2. It can take time for the attacker to produce the longest chain but if the attacker has more computational power than the honest nodes, even just a little more, then with probability 1 the attacker will end up producing the longest chain.

As an example, Budish shows that if the attacker has just 5% more computational power than the honest nodes then on average it takes 26.5 blocks (a little over 4 hours) for the attacker to have the longest chain. (Most of the time it takes far fewer blocks but occasionally it takes hundreds of blocks for the attacker to produce the longest chain.) The attack will always be successful eventually, the key question is what is the cost of the attack?

The net cost of a double-spend attack is low because attackers also earn block rewards. For example, in the case above it might take 26 blocks for the attacker to substitute its longer chain for the honest chain but when it does so it earns 26 block rewards. The rewards were enough to cover the costs of the honest miners and so they are more or less enough to cover the costs of the attacker. The key point is that *attacking is the same thing as mining.* Budish assumes that attackers *add* to the computation power of the network which pushes returns down (for both the attacker and interestingly the honest nodes) but if we assume that the attacker starts out as honest–a Manchurian Candidate attack–then there is essentially zero cost to attacking.

It's often said that Bitcoin creates security with math. That's only partially true. The security behind avoiding the double spend attack is not cryptographic but economic, it's really just the cost of coordinating to achieve a majority of the computational power. Satoshi assumed 'one-CPU, one-vote' which made it plausible that it would be costly to coordinate millions of miners. In the centralized ASIC world, coordination is much less costly. Consider, for example, that the top 4 mining pools today account for nearly 50% of the total computational power of the network. An attack would simply mean that these miners agree to mine slightly different blocks than they otherwise would.

Aside from the cost of coordination, a small group of large miners might not want to run a double spending attack because if Bitcoin is destroyed it will reduce the value of their capital investments in mining equipment (Budish analyzes several scenarios in this context). Call that the Too Big to Cheat argument. Sound familiar? The Too Big to Cheat argument, however, is a poor foundation for Bitcoin as a store of value because the more common it is to hold billions in Bitcoin the greater the value of an attack. Moreover, we are in especially dangerous territory today because bitcoin's recent fall in price means that there is currently an overhang of computing power which has made some mining unprofitable, so miners may feel this a good time to get out.

The Too Big to Cheat argument suggests that coins are vulnerable to *centralized computation power easily repurposed.* The tricky part is that the efficiencies created by specialization–as for example in application-specific integrated circuits–tend to lead to centralization but by definition make repurposing more difficult. CPUs, in contrast, tend to lead to decentralization but are easily repurposed. It's hard to know where safety lies. But what we can say is that any alt-coin that uses a proof of work algorithm that can be solved using ASICs is especially vulnerable because miners could run a double spend attack on that coin and then shift over to mining bitcoin if the value of that coin is destroyed.

What can help? Ironically, traditional law and governance might help. A double spend attack would be clear in the data and at least in general terms so would the attackers. An attack involving dollars and transfers from banks would be potentially prosecutable, greatly raising the cost of an attack. Governance might help as well. Would a majority of miners (not including the attacker) be willing to fork Bitcoin to avoid the attack, much as was done with The DAO? Even the possibility of a hardfork would reduce the expected value of an attack. More generally, all of these mechanisms are a way of enforcing some stake loss or capital loss on dishonest miners. In theory, therefore, proof of stake should be less vulnerable to 51% attacks but proof of stake is much more complicated to make incentive-compatible than proof of work.

All of this is a far cry from money without the state. Trust doesn't have the solidity of math but we are learning that it is more robust.

Hat tip to Joshua Gans and especially to Eric Budish for extensive conversation on these issues.

Addendum: See here for more on the Ethereum Classic double spend attack.

88 Comments print

Comments

Rich Berger #

2019-01-07 07:56:54

Hide Replies

I was always skeptical about Bitcoin. Not news to me.

> *therussians* #
>
> *2019-01-07 12:34:36*
>
> Hide Replies
>
> so how much would a big bitcoin collapse affect the dollar?
>
> > *Jim* #
> >
> > *2019-01-07 13:44:53*
> >
> > Hide Replies

I’ve always been skeptical of the state and it’s $20T in debt. Money w/o the state is life w/o the state.

BTW Satoshi is Nick Szabo and if it wasn’t hacked at $20k it will never be hacked. He was the perfect age to blend crypto tech with old school security.

Bitcoin = Friendster. Erherium = MySpace. ? = Facebook.

El Beau #

2019-01-08 03:36:48

Hide Replies

"the state is $20T in debt".
Actually, no.
One-third of that is intergovernmental borrowing - the state owes itself.
One-third of that is treasury bills held by citizens of the state. So, the state owes its own citizens. That's not debt, that's deferred wealth transfer.
Only one third of that is actual debt.

The Anti-Gnostic #

2019-01-08 11:09:27

Hide Replies

It's all actual debt that has to be extracted from the private sector in order to be satisfied. The only thing the State can do that a company, household or business can't is print money, in which event the payments are made via inflation. TANSTAAFL.

Anton vdM #

2019-01-09 13:30:35

State liabilities represent private sector assets. The absolute level is irrelevant. What matters is the ability of the state to meet those liabilities without creating inflation. That seems pretty rock-solid to me. It takes pretty severe state collapse to create inflation, at which time inflation is the least of your concerns.

Matt Young #

2019-01-07 08:20:35

Hide Replies

The ledgers have a recall within a timeout operation. It is possible for the receiver of a bitcoin to cancel its request on the queue if the exchange does not appear within a certain time period. It should be active and used.

> *Matt Young* #
>
> *2019-01-07 08:32:37*
>
> I should explain the Spectre method. The exchange agreement is inside the processor instruction cache, it has only two finite exits, failed to register and register complete. The instruction cache, has a point where both parties call their respective trusted miners (outside the cache) to verify the exchange. Then each trusted miner can cancel within timeout for increasing fee. Thus, canceling the exchange, after the fact, will cost the parties but minimizes the fraud to a small element which can be tracked ex post. The method is independent of ledger technology, but works great with bitcoin. All the ledgers need cancel on within timeout for an increasing fee because it solves the problem of exchanging between dis-similar ledger technologies. The bug above is in that class of exchanges, crossing different ledge technologies. The cancel on timeout works because the cancellation queue is observable, users can calculate the risk, and refuse any contract not having a sufficient penalty for cancel.

---

rayward #

2019-01-07 08:31:15

Hide Replies

The distinction between a libertarian and an anarchist is not always apparent. The adage that "a conservative is just a liberal who has been mugged" (a paraphrase of Kristol's famous quip that a neo-conservative is "a liberal who has been mugged by reality")) comes to mind. Or maybe Janis Joplin's lyric ("freedom's just another word for nothin left to lose") is more appropriate.

> *Jwilli7122* #
>
> *2019-01-07 09:40:25*
>
> That’s actually a Kris Kristofferson lyric

> *holy trinity* #
>
> *2019-01-07 21:55:15*

> Conservatives are liberals that got cuckolded.

BCR #

2019-01-07 08:58:04

Hide Replies

Isn't this why most exchanges require 3-6 block confirmations before considering the Tx valid?

> *Alex Tabarrok* #
>
> *2019-01-07 09:27:22*
>
> Hide Replies
>
> That's the escrow period I mention in the post. The upshot of the post is that the escrow period does not offer much protection.
>
> > *BCR* #
> >
> > *2019-01-07 10:48:26*
> >
> > Hide Replies
> >
> > Your argument is predicated on increasing centralization, from what you perceive as an inevitable due to a "flaw" in the hashrate algorithm whereby coordinated bad actors (not limited to mining farms) mine an increasing percentage of the blockchain.
> >
> > Yet other crypto assets already utilize alternative hashing algorithms that are not susceptible to ASIC-powered mining "cheats," leading to far better decentralization. If this "flaw" ever became a significant risk for Bitcoin blockchain integrity, it could always be forked in the future using a user-activated soft fork or a traditional hard fork if the miners thought it risky for their investments to implement an alternative (or less-power hungry ;-)) hashing mechanism.
> >
> > > *Jim* #
> > >
> > > *2019-01-07 13:56:08*
> > >
> > > Free market money baby!

AndrewL #

2019-01-07 09:53:13

Hide Replies

The economics arguments don't really make sense:

If the value stored in bitcoin increases, then mining becomes more profitable, not less. The key feature of bitcoin is that there is only a fixed number of coins the be generated -- forever, thus each coin mined would actually increase in value providing incentives for more miners to join in making the 51% attack more difficult to carry out.

> *yo* #
>
> *2019-01-07 10:57:01*
>
> Hide Replies
>
> Unless people anticipate that it's not worth the cost to be mining more. As it gets harder to get a Bitcoin by mining because new coins become rarer, the cost per Bitcoin goes up. If the value of each coin goes up less quickly, it's game over.
>
> > *AndrewL* #
> >
> > *2019-01-07 11:12:09*
> >
> > This attack requires a transaction. Each ledger block is limited to a relatively small number of transactions (by design). As the value of bitcoin increases, the value of each transaction in the ledger block has to increase, thus you will need to find someone who would be willing to take a lot of risk on a single transaction.
> >
> > thus the most obvious protection for the buyer would be to split the transaction over multiple different ledger blocks requiring the attacker to perform the attack on several blocks. You can wait and pay out in increments as you see the transactions appear on the block chain.

> *El Beau* #
>
> *2019-01-08 03:50:00*
>
> Hide Replies
>
> "If the value stored in bitcoin increases"
> Which is not guaranteed.
> " The key feature of bitcoin is that there is only a fixed number of coins the be generated -- forever, thus each coin mined would actually increase in value "
> Hahahaha, wow. Seriously? Bitcoin doesn't have *any* inherent value. The day after the

> last coin is mined it'll be worth what it is today: whatever someone will pay. There is no guarantee bitcoin won't plunge in value - like it did this year - and a limit on the supply doesn't matter when demand swings are that huge.
>
> > *John Mont*
> >
> > #
> >
> > *2019-01-12 22:49:23*
> >
> > That is true but thing have value if you believe they do, like the US Dollar, it really is just paper but people believe it has value, so it does. The price did drop, last year but over all it is way up. I recall it being $10

Bob

#

2019-01-07 09:59:58

Hide Replies

Alex, every second of your time dedicated to the byzantine details of specific cryptocurrencies is a second you should be use on something else. It's a solution in search for a problem. As currency replacements, they are only better than the very worst available: They lack basic characteristics of good medium of exchange, or units of account. Keeping a cryptographic wallet safe and usable at the same time is beyond what any individual can, and should, handle: In industry we only rely on something like this to defend secrets in environments where 5+ people are part of a protection scheme, and even then, breaches happen. If I lived in Venezuela, I'd rather just use smuggled dollars/euros.

Technological innovations that actually go anywhere get adopted faster than ever before. And yet, the satoshi paper is over 10 years old, and the entire blockchain "ecosystem" has produced very little, if any, value, unless you consider value finding a variety of ways to run scams on potential customers and investors. It's only slightly newer than the iphone, and smart phones are hardware, and therefore should develop more slowly and be harder to adopt. We've moved further forward in quantum computing than blockchains of any sort. If 10 years of venture capital thrown at a problem leads us to where we are now. It's a colossal waste of resources: A deadly mental trap, a mix of string theory and Herbalife.

Save yourself Alex.

> *Some One*
>
> #
>
> *2019-01-08 11:48:08*

> Hide Replies
>
> Every second it took you to write this answer is a second you should be use on something else.
>
> > *The Anti-Gnostic* #
> >
> > *2019-01-08 14:58:41*
> >
> > It's, "you should done be use."
> >
> > Like how we used to say "asked" instead of "axt."

> *Wodie* #
>
> *2019-01-13 16:50:57*
>
> The internal combustion engine was a solution searching for a problem. Vapor-compression refrigeration is too. Same for packet switching protocols, permaculture, and solar panels. If we let the knuckle draggers of the world dictate where we should allocate our intellectual and experimental capital, we'd all still be bashing rocks together to light kindling on fire. There's an old saying "If the Queen had balls, she'd be King." Your fiat still spends fine, so you have no barometer.

Li #

2019-01-07 10:21:37

Hide Replies

Headline may be true. But isn't it also true that "most people" know very very little about financial and technical and scientific and medical and political and economic (and on and on) matters as well? "Most people" seems to be one of those vague meaningless phrases which are extraordinarily popular to writers. Even if you quantify it, does it have any real significance? Most people are intellectually lazy and avoid learning which doesn't directly and immediately improve their lives. This is not news.

> *byomtov* #
>
> *2019-01-07 14:48:57*
>
> I don't think the headline is true at all. I think "most people," of whom I am one, are very skeptical about the security of bitcoin and would hardly be surprised to learn that there are possible scams available.

> Only true believers are surprised.

Nicholas #

2019-01-07 11:06:49

Hide Replies

By definition, if you have more compute power than all honest miners, aren't you just executing a standard 51% attack? Wait, are some people just learning about 51% attacks now? There was a whole Silicon Valley episode about this, I can't recommend that show enough. Very educational for people outside of tech.

> *Analyst* #
>
> *2019-01-07 13:33:24*
>
> Yes this is a textbook 51% attack.

---

albatross #

2019-01-07 11:33:06

Hide Replies

It seems like there's another incentive/economics defense against this class of attack: Bitcoin miners have a large investment in single-purpose hardware (ASICs designed only for Bitcoin mining). A single entity or pool that has 51% of mining capacity has some huge number of dollars invested in that mining hardware, which is worthless in a world where this particular function isn't being used for Bitcoin mining.

Running large-scale double-spending attacks is possible for this attacker. But doing so will inevitably become public--in a couple days, everyone in the world will know that there are large-scale double-spending attacks going on and people are losing money from them. At that point, it seems like Bitcoin's value drops very quickly, and the value of that existing investment in mining equipment likewise goes to zero.

Now, if this were an attack that anyone with 5% of the mining power could carry out, we'd be screwed--there'd be an incentive for each miner to run the attack before the others did. But a 51% attacker is by definition unique--he decides right now whether to run the double-spending attack (and once it's discovered, to forgo all future mining rewards) or to continue mining. And he also has the largest stake in the world in the continued value of mining hardware.

> *albatross* #
>
> *2019-01-07 11:34:39*
>
> Hide Replies
>
> Sorry, I just realized the OP addressed this.
>
> However, I think that current bitcoin mining rigs are absolutely *not* repurposable.
>
> > *BCR* #
> >
> > *2019-01-07 11:44:38*
> >
> > Hide Replies
> >
> > They are repurposable for mining other blockchains.
> >
> > > *David J* #
> > >
> > > *2019-01-07 13:31:27*
> > >
> > > Hide Replies
> > >
> > > They can only be repurposed to mine other chains that use SHA256 hashes for mining. There are many that do not, and blockchains that currently use it could be forked to switch the algorithm if an attacker with sufficient SHA256 resources surfaces. At that point, their investment in SHA256 ASICs would be about as useful as a bunch of really expensive space heaters.
> > >
> > > > *albatross* #
> > > >
> > > > *2019-01-08 21:18:19*
> > > >
> > > > Hide Replies
> > > >
> > > > However, changing the proof of work algorithm also makes all the existing miners' investments useless.
> > > >
> > > > > *David J* #
> > > > >
> > > > > *2019-01-09 11:39:52*
> > > > >
> > > > > That's a good point. If more than half of the mining power is controlled by a malicious entity, it is an existential threat to the network. I would expect the value of Bitcoin to then trend to zero. I'm not sure how quickly it would happen, but

> > > > things do move very fast in cryptocurrency markets. I would imagine that those miners' investments in hardware would be essentially worthless no matter which path the network takes (either changing PoW algorithm or not).

> *OldCurmudgeon*
>
> *2019-01-07 12:01:42*
>
> Hide Replies
>
> Eventually maybe... but "in a couple days" seems wildly optimistic, particularly when the attack individual/consortium has total control of the ledger.
>
> It's worth noting that there is no guarantee the top named miners are independent currently. They can side agreements among themselves, "enforced" using the transparency of the blockchain.
>
> > *yo*
> >
> > *2019-01-08 03:11:57*
> >
> > You are relying too much on incentives for the 51% miner. Given enough time, someone at that 51% place may want to destroy it or self-destruct it or something. By then, the damage to the block chain is done and it may never recover.

Andrew Hofer

2019-01-07 13:07:15

Hide Replies

(This is a relayed comment from a security expert who audits Ethereum code)

Not news. They're describing what is colloquially called a 51% attack, and it is noted explicitly in the white paper. The security of the system depends upon there not being a majority miner. Also, in practice miners tend to have lots of Bitcoin, and a credible double-spend threat would tank the value of Bitcoin (presumably?), so there's also some extrinsic disincentive to attack the chain. (Miners have their mining reward locked by the chain for a while.)

It's reasonable for economists to disagree with the technical decision that the security of the chain depends on a plurality of miners, but it is not news.

> *James*

> *2019-01-07 15:37:11*
>
> The attack isn't new what is new and surprising is the cost calculations--showing the cost of such an attack is well below plausible benefits.

---

george m weinberg #

2019-01-07 13:13:01

Everyone who knows anything at all about Bitcoin knows that an attacker with more than 50% of the total mining capacity can multi-spend.

David J #

2019-01-07 13:27:43

The leading Bitcoin Cash implementation, Bitcoin ABC, has added default, rolling 10-block checkpoints: https://twitter.com/Bitcoin_ABC/status/1065041060101935104

That means that if you complete a transaction and wait for it to be confirmed and for 9 additional blocks to be processed that built off the initial block including your transaction, you are safe and the transaction is truly irreversible, at least according to the majority of nodes running the Bitcoin Cash network (note: this is still a vulnerability on Bitcoin [BTC]).

Also, if an entity controls more than half of the network and they are dishonest, then the whole network will collapse unless or until they implement a mining algorithm change.

A #

2019-01-07 13:30:53

poring over the paper :)

The older ‘one-CPU, one-vote’ thinking doesn't hold up anymore, you're right.

Doug #

2019-01-07 16:24:15

Hide Replies

This argument's making some pretty erroneous or ill-informed assumptions.

> The rewards were enough to cover the costs of the honest miners and so they are more or less enough to cover the costs of the attacker.

No, because in the state of the world where a large-scale 51% attack is successful the value of those block rewards will be substantially less than in the state of the world where the honest miners win. In fact we can say they'd be essentially zero, because bitcoin will no longer have any trusted value.

Moreover the second leg of the double-spend would basically be worthless. Yes, the attacker could spend BTC once for dollars (or some other asset). But the other leg would be the BTC he still holds on the alternative fradulent chain. Again the market value of that BTC will fall to near-zero, so he'll basically end up with hardly any more asset value relative to his initial bitcoin investment. Remember double-spend is not a mis-spend attack (which is secured by DSA encryption, not blockchain consensus). Any BTC that he wants to double-spend, he has to buy in the first place.

Also remember, he can't sell his BTC on the fraudulent chain, since he'd have to publish it. Say he tries to confirm one transaction on the honest chain to Alice and one on the fraudulent chain to Bob. That means he has to publicly broadcast his fraudulent chain, which announces to the world that a 51% attack is occurring. No counter-party will confirm a transaction while the is taking place.

The current block reward is 12.5 BTC, or $7.2 million a day. Assume half of that is electricity, and a mining hardware depreciation rate of 30% a month. The value of all mining hardware would be $324 million.

Therefore a 51% attacker would need to invest $162 million in hardware, who's value will drop to basically zero once a large-scale double-spend is carried out. Because once BTC has zero value, the future block rewards from that mining hardware also has zero value.

So the attacker would need to make a transaction larger than $162 million. In fact much larger, because as we've established above the possible returns to the initial bitcoin investment are far less than 100%.

If a large-scale double spend dropped the market value of BTC to 10% of its pre-spend (which it would at a bare minimum), then attacker would need to make an initial bitcoin investment of $1.6 billion, and find enough liquidity in the markets to sell that position quickly. If BTC fell to 1% of its pre-attack value, he'd have to make an initial bitcoin investment of $16 billion.

Needless to say these are insanely high numbers for an insanely risky speculative gamble. Outside a few mega-rich billionaires or well-funded state actors, nobody is capable of even potentially pulling off a profitable 51% attack.

> *A B* #
>
> *2019-01-07 17:09:25*
>
> Hide Replies
>
> This ^^^ in spades. This issue was detailed in the original paper launching Bitcoin in 2009. The answers and defenses are also in the original paper. Just about everyone who works in bitcoin is completely aware of this. You can go to crypto.app right now to see the expected cost of a double spend attack per hour on any number of currencies.
>
> > *Jim* #
> >
> > *2019-01-07 19:20:24*
> >
> > Hide Replies
> >
> > Those issues are explicitly mentioned in the post and the paper.
> >
> > > *A B* #
> > >
> > > *2019-01-07 20:35:57*
> > >
> > > The issue is the claim 'Bitcoin is less secure than you think,' with the issues of 51% attack and double spend presented as problems that aren't addressed naturally. They are.

> *Fred* #
>
> *2019-01-07 17:15:13*
>
> Yes, but: here's what appears to be a real double-spend attack happening right now in ETC.
> https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de

> *Sure* #
>
> *2019-01-07 20:38:09*

> I would think that an assured drop of Bitcoin by 90% would be worth far more than the double sale. Bitcoin has a market cap of what $70 billion? Is there some reason a nefarious billionaire would not be able to short a billion or two (e.g. sell futures contracts, place puts, or some fun margin trade for dollars) and then use about a quarter of that to tank the currency via hardware purchases?
>
> Assuring that price drops appreciably close to zero seems like a very good way to make a lot more money at a much higher rate of return. Now maybe Bitcoin does not have the typical amount of derivative opportunities available, but that would seem to limit its ability to be used as a currency in the modern economy.

> *yo* #
>
> *2019-01-08 03:18:32*
>
> Again, a rogue employee at the 51% company may want to trash it all.

Gabe Harris #

2019-01-07 16:26:26

This is an argument to diversify some of your crypto portfolio into Monero. No-coiners...just keep betting on governments and see how it works during the next FOMO run.

Jon M #

2019-01-07 16:26:54

Hide Replies

Surely the real concern is that the integrity of bitcoin relies on just a handful of computers not being hacked. The economic benefits of a 51% attack are very clear for a criminal who didn’t have to invest in the hardware. The security of bitcoin is now only as good as the security of a single digit number of computer systems.

> *IVV* #
>
> *2019-01-07 17:08:07*
>
> ...Which we're expected to... what's the word? Oh yeah, trust.

> *asfd* #

> *2019-01-07 18:29:32*
> Hide Replies
>
> This is a fundamental misunderstanding of how hash functions work and the nature of distributed systems. The integrity of Bitcoin is not based on a "handful of computers".
>
> > *Jon M* #
> >
> > *2019-01-08 09:23:57*
> >
> > The calculations are distributed, but four mining pools control 51% of the power and I assume there is some way for their owners to control those somewhat centrally. If so, you just need to compromise those four pools or a subset of them plus some other source of computing power.

---

athEIst #

2019-01-07 17:07:24

No reflection on Alex, but every time I read an article on Bitcoin/blockchain I know less than before which wasn't much. And then there's.........mining.........?!?

---

athEIst #

2019-01-07 17:10:25

OT

Where is Ray Lopez? Was there a typhoon in the PH, volcano?

---

asdf #

2019-01-07 18:27:59

Alex, I emailed you my thoughts. I blogged about this recently and this is a viable attack vector -- especially with the advent Bitcoin futures and ETF markets. It will be interesting to see how this plays out, but I don't think government & law will be what makes Bitcoin or any (non-sovereign) digital money ultimately possible. Cryptography enables us to avoid walled gardens. Lets try to achieve that.

Jim Birch

2019-01-07 18:34:59 #

Bitcoin fork! I'd like to see that. Honey, we solved the wrong Sudokus.

TXX #

2019-01-07 18:59:22

Hide Replies

This is a thoroughly devastating takedown of Bitcoin by Alex. There is no way cryptos will survive. No way.

> *Bit Coinerson* #
>
> *2019-01-08 13:12:36*
>
> Hide Replies
>
> This isn't a devastating takedown, it's an explanation of something called a 51% attack, which is Bitcoin 101. I can understand how people who don't know Bitcoin would read this as a "shocking discovery" or something, but it has been understood and discussed from day one.
>
> The attacker would destroy the value of their own coins, so right there you've got a bulwark against most actors who would do this. And accumulating the amount of computing power to pull this off in the first place is a much bigger task than you may realize.
>
> > *ricardo* #
> >
> > *2019-01-08 15:44:45*
> >
> > Hide Replies
> >
> > No way TXX recovers from this.
> >
> > > *Alex Tabarrok* #
> > >
> > > *2019-01-08 16:29:55*
> > >
> > > Hide Replies
> > >
> > > The attack is well know the fact that the cost of the attack is so low is not well known.
> > >
> > > > *But Coinerson* #
> > > >
> > > > *2019-01-08 16:44:42*

> The cost of a 51% attack is currently estimated at $70.64 Billion. There is no way someone could cash out anywhere near that amount for USD before the attack was detected. You’d have to be willing to lose virtually all of that money.

Rob Viglione #

2019-01-07 20:47:53

A big mistake i see in academic research on bitcoin is that most often the system(s) is considered static--what you see now is what you'll get indefinitely. Bitcoin and its offspring are constantly evolving and already we have projects (like my own, Horizen (ZEN)) that have adopted modified Nakamoto consensus to prevent 51% attacks. Horizen was attacked last June and within three months we had a double check in consensus that effectively ended this threat. These systems really are antifragile :)

joselin #

2019-01-07 21:56:10

the best of this year for those people who are interested in the world of Cryptoprophecy, we bring you this new package bit.ly/2TC6dT8

joselin #

2019-01-07 21:58:46

The best application to buy bitcoins.https://www.coinbase.com/join/5bfdb3b2632c6c0af823dac0

doctorwes #

2019-01-08 01:12:32

Not bitcoin, but:

"On 1/5/2019, Coinbase detected a deep chain reorganization of the Ethereum Classic blockchain that included a double spend. In order to protect customer funds, we immediately paused movements of these funds on the ETC blockchain. Subsequent to this event, we detected 8 additional reorganizations that included double spends, totaling 88,500 ETC (~$460,000)."

https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de

https://arstechnica.com/information-technology/2019/01/almost-500000-in-ethereum-coin-stolen-by-forking-its-blockchain/

KT #

2019-01-12 20:06:58

If you can get enough CPU power to manage a double-spend attack, you still need to find something to spend it on. Will anyone sell you a billion dollars worth of gold for bitcoin?

There are two sides of the scam: the real world side, and the crypto-world side.

In other words, for this to work, you need to find a powerful person to rip off, who is too weak to find you after you stole from him.

Satoshi Nakamoto himself offered the solution of using an escrow service.

Steve #

2019-01-12 20:10:33

When I found out how Bitcoin and other blockchain currencies operate, I knew that I would never put my money in them. There may be some future cyber currency that will be sound, but it will not be blockchain based.

---

remi #

2019-01-12 20:16:00

You do realize billions of dollars worth of BTC trade hands every day right? If what you're saying were true it'd be constantly being exploited. Pools are also comprised of many separate miners, who would take their hash off the pool if they suspected anything like this were being planned. You make it sound as though 4 entities control 50% of Bitcoin's network, that is false. Sorry, I think you need to rethink this theory.

---

magnus #

2019-01-12 20:39:27

Bitcoin a very unstable with zero value and no safety net

---

mats #

2019-01-12 20:44:06

"Consider, for example, that the top 4 mining pools today account for nearly 50% of the total computational power of the network. An attack would simply mean that these miners agree to mine slightly different blocks than they otherwise would."

I see this conflation of *pools* with *miners* all the time. You do realize that in any one large pool there are, conservatively, many thousands of unrelated miners (individuals, not machines), right? And that for said miners it takes very little time to switch all their machines to another pool, right?

I'm not saying it wouldn't be possible for an individual to accumulate hashing power equal to 51% of the network. I'm just saying this habit of pointing to the size of several pools taken together as though they are a monolith when in fact they are a loose, temporary and non-binding group of individual miners is lazy and dumb.

That said, miners, spread the hell out.

Toger #

2019-01-12 22:36:57

Hide Replies

I can’t believe people don’t see what nonsense this article is. Yes it’s possible to have a double spend but only after a 51% attack controlling 51% of the mining... this writer must be taking far too much LSD to come up with this story... wow. I like it, only scares the gullible away from it so it drops lower so I can buy more

> *John mont* #
>
> *2019-01-12 22:58:07*
>
> That is the point of the article, scare people away

Jamie Buffet #

2019-01-13 00:20:52

Good luck with that one.

Comments for this post are closed