Blocksize

This issue comes up repeatedly, sparking many heated discussions. Some people think issues surrounding the blocksize will be the ultimate downfall of bitcoin; others think the theoretical problems are largely overstated and/or completely resolvable. Count me in that latter camp.

What is it?

The number of transactions per second that bitcoin can handle on-blockchain is directly tied to the data size of each block. Since bitcoin's inception, the size of a block has been fixed in the bitcoin code to a maximum of 1MB. Since one new block is generated on the bitcoin network every 10 minutes on average, this works out to a theoretical maximum of 7 transactions per second. Compared to the thousands of transactions per second that the Visa and Mastercard networks handle, this is not a lot.

Why is the blocksize limited?

As with many things in life, there's a tradeoff. Larger blocks would require more processing and bandwidth resources from bitcoin nodes (the global network of "volunteer" computers running the bitcoin software), which would eventually cause fewer people to be willing to run nodes. On the flipside, the network's transaction processing capacity is clearly limited by the blocksize. To be a global currency handling everything from inter-bank settlement payments to online tipping and micro-transactions, clearly 7 transactions per second is far few. The current 1MB size was chosen by bitcoin's creator, Satoshi Nakamoto, in the original codebase as a reasonable balance during bitcoin's birth and initial growth stage.

What can be done about it?

Simple – change the code to raise the blocksize limit. While this is a one-line change to the code itself, it would require most nodes to incorporate the change at about the same time. Ever prescient, Satoshi even suggested how this can be done eventually, stating on the bitcointalk forum in 2010:

It can be phased in, like:

if (blocknumber > 115000)
     maxblocksize = largerlimit

It can start being in versions way ahead, so by the time it reaches that block number and goes into effect, the older versions that don't have it are already obsolete.

*What *should* be done about it?*

This is where people differ. Some are adamant that the 1MB limit stay in place forever, in order to keep it cheap for small-time operators (individuals with laptops) to run full bitcoin nodes. Others, myself included, prefer a more market-driven/organic approach. Acknowledging that Moore's Law

continually reduces the cost of computing power and bandwidth, I think a steady or market-defined increase in the blocksize is reasonable. It could even be eliminated entirely. In theory, bitcoin miners would be incented to strike a balance between including lots of transactions to gather fees, and the costs of processing and transmitting larger blocks. Like many dynamics in bitcoin, this seems like one where a natural market-driven optimum can efficiently emerge.

Debunking "Debunking Bitcoin"

I've had the recent pleasure of lively twitter debate with Phil Carney (@carneycapital) about bitcoin. His exploratory post, "Debunking Bitcoin", is filled with the usual newbie (and gold-bug) criticisms, and I'm always more than happy to debate and debunk misguided or misunderstood ideas. I think Phil and I mostly understand each other at this point, but this is a bigger discussion than can be done 140-characters at a time.

With a background in both economics and computer-science, bitcoin is a bullseye for me intellectually. It's often difficult for those without such dual perspective to grok something as complex as bitcoin quickly. But that's why we have blogs and twitter.

Phil lays out several "problems" with bitcoin which lead him to the conclusion that it "IS another form of a fiat currency, albeit a digital one that is decentralized." His main concerns, somewhat typically boil down to: "No Intrinsic Value", "Divisibility", and "Alt Coins". I'll debunk these one at a time.

But It Has No Intrinsic Value!

This is the most basic and obvious criticism. Phil defines it as follows:

"A bitcoin has no store of wealth, no intrinsic value, just like the paper dollars printed by Central Banks around the world. Many of the Bitcoin Illuminati are peddling the fallacy that it does have a store of wealth as physical gold does. That is FALSE and MISLEADING in my opinion."

And goes on to say that

"Still you cannot melt a Bitcoin down to make Jewelry, use it in commercial products, and so it has no intrinsic value. This means it carries the same flaws the current Fiat Monetary system has."

He's right that you can't make bitcoin into jewelry (or can you?) or use it in industrial processes. But what he and many gold-bugs miss is really why things have value in the first place. It's simple: things have value because people want them. Usually valuable things are useful. They allow people

to get something done, or get something done better. In the case of dollars, gold, and bitcoin, they all allow people to exchange goods and services more easily. They solve the coincidence of wants problem. They reduce the friction of exchange. This is what money is all about.

In our internet-connected lives, we need to send money electronically. Increasingly little of our day-to-day exchange is done by handing over physical paper-cash or metal-coin. We exchange online, usually with electronic dollars administered through some third-party account (our bank, a credit-card processor, paypal, etc), with the 3rd party taking a cut somewhere in the process.

Bitcoin is exciting because it's the first thing to be able to do electronic exchange reliably without a 3rd party. It is electronic cash. No central body controls or issues it, and no 3rd party is explicitly involved when someone sends bitcoin to someone else. It also provides real transactional security, unlike easily-intercepted credit-card numbers and bank account numbers. And it is credibly scarce, with a mathematically limited supply (more on this later).

All of these properties make bitcoin very useful for our modern way of life. It is specifically useful at reducing the friction of exchange. Why? Because it requires no middleman, offers effectively instant settlement, negligible transaction cost, and it is both reliably scarce and cryptographically secure. These features add up to a near-ideal tool for facilitating online transactions. And that's what money is all about – specifically reducing the friction of exchange for however a given culture desires to exchange. In the past, it was face-to-face. Now we want to transact instantly, across oceans, at near-zero cost, with confident security. That is bitcoin's "intrinsic" value. There is no need to melt or wear it for it to have utility in our lives.

In sharp-contrast to a gold-bug's sensibilities, it is bitcoin's non-physical nature that allows all these benefits. In modern times, tangibility is a bug, not a feature.

Ok, Bitcoin is useful, but there are a gazillion units! It's not scarce!

Phil's next problem with bitcoin is that they can be divided into a hundred million pieces. He equates this with violating the notion that bitcoin is scarce money with a hard-cap of 21 million bitcoins. He elaborates:

"…there may be 21,000,000 total Bitcoins, there are, however, a massive 2,100,000,000,000,000 or 2.1 quintillion [sic] tradable bits that will be available when all the coins are mined. This figure also needs to be multiplied by the dollar value assigned to each 0.00000001 or "satoshi" highlighting the fact that its finite status is at best one hell of a stretch"

Phil and others who make this argument are missing several points:

1) Anyone who controls one bitcoin, will always control all divisions thereof. It's like owning an ounce of gold. The owner can split it down to gazillions of individual gold atoms, but he still just has one single ounce of gold. No more gold has been created. Gold is no more scarce because each ounce can be divided into 10×10^27 individual gold atoms.

2) Perfect divisibility is a strength. It allows further precision in economic transactions, and that reduces friction. If I want to sell something for 1.23456789 bitcoin, I can do that trivially, with perfect precision. Try dividing an ounce of gold to a one-hundred-millionth of an ounce…without a

state-of-the-art chemical lab. While this may seem academic, it will likely prove a major benefit in allowing bitcoin to flower into an underlying protocol layer doing the heavy-lifting for additional services requiring very detailed asset-registers (see Naval Ravikant's excellent The Internet of Money for starters).

Divisibility is a feature, not a bug.

But anyone can create new crypto-currencies!

This is the most interesting concern that Phil and other critics raise. Phil states:

"Put simply, as time evolves, as more crypto currencies enter the virtual currency space, the Bitcoin phenomenon and hysteria may be eroded. Whilst it has dominated the virtual currency space, Bitcoins 2.1 quintillion [sic] bit supply may be finite to Bitcoin itself, the space for new virtual crypto currencies is growing.

Bitcoin is not special or unique.Bitcoin will be to the virtual Crypto world what the Euro, the Yen or The US Dollar are to the central bank world… FIAT MONEY WITH NO STORE OF WEALTH."

Phil is right that anyone can create a new crypto-currency (go make your own here. See how well it catches on…). But he ignores the question of why anyone would use it. Why did humanity use gold as our primary monetary instrument and not silver? Or copper? The answer boils down to concepts familiar to those studying tech adoption or social sciences: network effects and first mover advantages.

When some convention or technology (or monetarily-appropriate metal) is adopted by enough people, it's advantageous for everyone if the next person in line also adopts that convention. The new guy gets the benefit of exposure to the rest of the network, and the network itself expands, enhancing the value proposition for all existing participants as well as the next entrant. As long as no vastly superior new convention appears, new entrants are highly incentivized to use the existing status-quo. Like core internet protocols (IPv4, TCP, HTTP, SMTP), bitcoin is demonstrating strong and likely unstoppable network effects.

UPDATE: Erik Voorhees eloquently addresses these points as well, in his open-letter follow-up to his appearance on Peter Schiff's radio show.

So what *if* something better comes along? Well, we can look to adoption of previous technological protocols, specifically internet/networking protocols. New ideas appear continuously – just look at the list of internet RFCs – yet the internet essentially functions the same way as it did 30 years ago; ie, on the same core protocols. Generally speaking, new services are built atop the core, with core protocols evolving and incorporating new features as needed. This dynamic is already emerging in bitcoin, with Bitcoin Improvement Proposals serving as bitcoin's RFC equivalent. By far the overwhelming tendency on the internet has been for the protocols to be evolved as needed, and it will likely be the same with bitcoin. For open systems on which infrastructure is built by diverse sets of individuals and companies, all spending their own energy on engineering, education, and process, it makes far more sense to evolve than to switch.

Part of the critique of this aspect of bitcoin, most typically from gold-bugs, stems from a fundamental

lack of appreciation for how flexible and malleable technology can be. Bitcoin is not MySpace. It is far more fundamental, like the core packet-switching ideas that have underpinned computer networks since inception. In the past 30 years, the basics of packet-switching have been rapidly extended, patched, evolved, and layered on top of extensively. Bitcoin is equally fundamental, open, and extensible.

As with gold, malleability is a feature, not a bug.

Phil's arguments are reasonable and fairly typical of non-tech gold-bugs. They fail to appreciate the dynamics and flexibility of technology; both how "real" and "hard" it can effectively be, as well as how beautifully malleable. Much of human interaction is moving to digital realms due to the friction-reduction and efficiency that it offers. The same is now happening with money, courtesy of bitcoin.

- If you liked my article, you may leave a bitcoin tip!

- If you wish to leave a tip in gold, I guess we can meet-up in person?

- I do not accept tips in dollars, Euro, Yen, or any other fiat currency.
