Nicholas Weaver

▶ **Peter G. Neumann,** Column Editor

Inside Risks
Risks of Cryptocurrencies

Considering the inherent risks of cryptocurrency ecosystems.

RYPTOCURRENCIES, ALTHOUGH a seemingly interesting idea, are simply not fit for purpose. They do not work as currencies, they are grossly inefficient, and they are not meaningfully distributed in terms of trust. Risks involving cryptocurrencies occur in four major areas: technical risks to participants, economic risks to participants, systemic risks to the cryptocurrency ecosystem, and societal risks. Fortunately, for all but the last case, there is little risk to anyone not directly participating; (see the article "Privacy in Decentralized Cryptocurrencies" on page XX in this issue).

Cryptocurrencies are tradeable cryptographic tokens, with Bitcoin as the most famous example. Bitcoin, developed by a pseudonymous creator, Satoshi Nakamoto, consists of a distributed public ledger system showing all balances associated with public keys. To spend Bitcoin, someone with the corresponding private key signs a message indicating the particular balances should be transferred to a set of destinations and then broadcasts this message

> **The primary notion behind Bitcoin's design is to enable a censorship-resistant and irreversible payment system.**

through a peer-to-peer network.

This peer-to-peer (P2P) network then validates the transaction as valid in the public ledger and commits it to another block in the ledger containing at most 1MB of data. In order to prevent the block from being tampered, the Bitcoin system uses "proof of work"[1] to protect its hash chain. Each block contains a pointer to the previous block (creating the "blockchain"), and every miner attempts to create a new valid block by computing partial hash colli-

sions, hoping to find a value less than a dynamically tuned difficulty factor by taking a potential block and modifying various mutable fields until the miner discovers a partial collision that meets the difficulty requirement.

Once a miner discovers a new block, it broadcasts this block over the peer-to-peer network; all other miners then validate the new block and start mining the next block. As a consequence, changing the last n blocks in the ledger requires approximately the same number of hash calculations as creating those n blocks. Each block also contains a transaction that pays a fixed reward to the winning miner, as well as all transaction fees sent in the block. In order to implement a fixed monetary policy, the difficulty factor self-adjusts on regular intervals to limit the block creation rate to one block approximately every 10 minutes, and the block reward halves approximately every four years.

This naturally creates a "Red Queen's Race," which currently causes the Bitcoin network to consume more power than Ireland. When there is potential profit, more miners are in-

centivized to join the process until the point where nobody makes a profit anymore. For example, a 10x reduction in power consumption per hash for Bitcoin mining would have little real effect on Bitcoin's power consumption. Instead, there would just be 10x as many hash computations needed to produce a block.

A good rule of thumb is that when prices are stable, approximately one-third to one-half of the block reward is sold by miners to pay power bills. This implies that when prices are high, Bitcoin consumes an outrageous amount of power. Any system based on proof-of-work will suffer this fate: If there is profit in mining, the miners will keep using more and more power until there is no more excess profit available. The only way Bitcoin could reduce its power consumption is through a massive collapse in price.

The fixed block size also limits transaction throughput to a trivially small global rate that is approximately three transactions per second. Although transaction fees start low, they can quickly increase when the transaction rate exceeds the global limit—as only those willing to pay increasing auction-based fees see their transactions confirmed. This is what caused the recent spike in Bitcoin transaction costs to a median price of over $30 a transaction. These global volume limits make Bitcoin clearly unsuitable as a public ledger. Nevertheless, a comparable cryptocurrency that supported 300 inexpensive transactions per second could see its global state grow at an untenable 14GB/day of additional storage for every participating node in the network, storage that also needs to be searched to validate transactions.

Since the original deployment of Bitcoin, a host of other cryptocurrencies has arisen, often by simply modifying the Bitcoin source code and changing a few parameters. These have taken many forms, including faster-committing blocks with a catchy slogan (Litecoin: "Litecoin is silver to Bitcoin's gold."), explicit jokes (Dogecoin), forks that maintain the same history until the date of the fork (Bitcoin Cash), and some notable ideas including an attempt to create a stable reserve of value by reinventing 18th-century banking (Tether) and "programmable money" to create smart contracts (Ethereum).

Cryptocurrencies for Payments: Not Fit For Purpose

The primary notion behind Bitcoin's design is to enable a censorship-resistant and irreversible payment system. It is intended that there should be no central authority that can say "thou shalt not" or "thou shouldn't have." The only other analogue in the real world is cash, which is bulky and requires physical presence.

All other electronic payment systems have the potential for censorship. There are third parties involved in the payment process that, under government pressure, can and do seek to ban or reverse disallowed payments. This includes blocking a wide assortment of criminal activity, such as drug payments, ransom and extortion payments, and money laundering. It can also be used to implement currency controls (limiting the ability of residents to exchange local currency for dollars or euros) and conduct fi-

CREDIT TK

AD TK

nancial blockades, such as how U.S. credit cards cannot be used for online gambling, could not be used to buy ads on Backpage (when this now-admitted criminal enterprise was first blocked from accepting credit cards due to local pressure), or transfer money directly to WikiLeaks.

However, unless censorship resistance in an electronic transaction is a requirement (such as for drug deals, ransom payments, money launderers, and those seeking to evade currency control), irreversibility combined with the volatile price means Bitcoin is significantly inferior to alternatives such as credit cards or PayPal.

Most sensible recipients of a Bitcoin payment immediately convert their payment into dollars, to avoid the substantial risk that currency swings may prove costly. Thus, most legal sites that accept Bitcoin payments are not actually taking Bitcoin, but instead using a service that both adjusts the Bitcoin price dynamically (so the merchant is actually pricing in U.S. dollars) and immediately sells the Bitcoin.

This also means that unless the buyer is a believer in Bitcoin, the buyer ought to buy Bitcoin only immediately before they initiate the transaction, to avoid volatility (and will have had to mine or buy the Bitcoin in any case). This is the point where Bitcoin's irreversibility results in substantial costs.

The Bitcoin exchange either effectively has to take cash only, must wait several days after a bank transfer completes before allowing the customer to buy Bitcoin, or is implicitly extending credit to the customer. Any exchange that does not follow these rules faces the fate of Tradehill, a Bitcoin exchange that went defunct when faced with chargebacks on Dwolla-based bank transfers. Steve Wozniak recently ex-

> **Most sensible recipients of a Bitcoin payment immediately convert their payment into dollars.**

perienced the same fate when he sold $75,000 in Bitcoin to an individual who paid with a credit card, only to find the transaction canceled since the thief used a stolen credit card (see https://cnb.cx/2EUxVY6).

Bitcoin payments are thus significantly more expensive for legal purposes when including the mandatory two currency conversion steps, the first one of which must be either slow, involve cash, or an implicit extension of credit. Even eliminating the irreversibility (which goes contrary to a fundamental explicit Bitcoin design goal stated by Nakamoto) would still result in two currency conversion steps. It is impossible to eliminate these two steps from a volatile cryptocurrency.

Yet, for those who do believe in Bitcoin it still is not usable as a currency. The monetary policy for Bitcoin is fixed with a limited and prescheduled creation rate designed to be deflationary. The only rational behavior for someone holding a deflationary currency is to never actually spend it. Otherwise the person risks eternal regret for buying a 10,000 BTC pizza (in 2010) and later realizing the pizza's payment is now worth a notional $100M.

Individual Technical Risks
Since cryptocurrencies are controlled by private keys, anyone who gains access to the private key can move the currency. This makes cryptocurrencies incredibly vulnerable to theft. If someone holds their cryptocurrency using a third-party service, they run the continual risk that the service gets robbed—an almost routine occurrence throughout the short history of Bitcoin. Thus, users instead need to store their money on their own systems.

But even this is difficult. During early research into Bitcoin when attackers installed Bitcoin miners on compromised systems, we hypothesized that malcode might also start to include Bitcoin theft amongst the automatic functionality. So we created a small Bitcoin wallet, placed it on images in our honeyfarm, and set up monitoring routines to check for theft. Two months later our monitor program triggered when someone stole our coins.

This was not because our Bitcoin was stolen from a honeypot, rather the graduate student who created the wallet

maintained a copy and his account was compromised. If security experts can't safely keep cryptocurrencies on an Internet-connected computer, nobody can. If Bitcoin is the "Internet of money," what does it say that it cannot be safely stored on an Internet connected computer?

Bugs can also naturally cause significant damage to cryptocurrency holdings. Although this potentially can affect any cryptocurrency, the biggest danger for bugs arises when cryptocurrencies are combined with "smart contracts"—programs that are generally immutable once deployed and that automatically execute upon the transfer of currency. The most successful platform for these is Ethereum, a cryptocurrency that allows writing programs in a language called Solidity.

Bugs in these smart contracts can be catastrophic. The first big smart contract, the DAO or Decentralized Autonomous Organization, sought to create a democratic mutual fund where investors could invest their Ethereum and then vote on possible investments. Approximately 10% of all Ethereum ended up in the DAO before someone discovered a reentrancy bug that enabled the attacker to effectively steal all the Ethereum. The only reason this bug and theft did not result in global losses is that Ethereum developers released a new version of the system that effectively undid the theft by altering the supposedly immutable blockchain.

Since then there have been other catastrophic bugs in these smart contracts, the biggest one in the Parity Ethereum wallet software (see https://bit.ly/2Fm7je4). The first bug enabled the mass theft from "multisignature" wallets, which supposedly required multiple independent cryptographic signatures on transfers as a way to prevent theft. Fortunately, that bug caused limited damage because a good thief stole most of the money and then returned it to the victims. Yet, the good news was limited as a subsequent bug rendered all of the new multisignature wallets permanently inaccessible, effectively destroying some $150M in notional value. This buggy code was largely written by Gavin Wood, the creator of the Solidity programming language and one of the founders of Ethereum. Again, we have a situation where even an expert's efforts fell short.

The entire cryptocurrency environment also faces systemic risks.

Individual Economic Risks

Everything about the cryptocurrency space is full of bubbles. Since all volatile cryptocurrencies are actually substantially inferior for legal purposes, this implies that the actual value as currency is effectively $0, so the only store of value is in other utility for a distributed trustless public append-only ledger.

Yet the Bitcoin blockchain, due to consolidation of mining into a few mining pools, does not actually distribute trust. Instead the system is effectively controlled by less than 10 entities self-selected by their willingness to consume power and anyone using Bitcoin implicitly trusts a majority of these few entities. Every proof of work blockchain seems to experience similar consolidation as the more efficient miners inevitably drive out less efficient ones. Given the almost trivial cost of building a three-transactions-per-second distributed system with identified and trusted entities using cryptographic signatures instead of proof of work this suggests the utility value for these cryptocurrencies is also effectively $0. This means everyone participating in the cryptocurrency market is basing the value only on the price that somebody else will pay—no different from tulip bulbs or beanie babies—and are all vulnerable to substantial and sudden collapse.

But further magnifying the problem is a large number of scams. There is a current trend in "Initial Coin Offerings," mostly consisting of cryptographic tokens implemented on top of an existing cryptocurrencies such as Bitcoin or Ethereum. Although claiming to be crowd-sold tokens for purchase of future services, the tradeable nature of these tokens has resulted in their acting as unregistered securities in a bubble market. There are also or-

ganized groups conducting pump-and-dump schemes, complete with fancy websites, animated advertisements, and even placing paper advertisements in BART commuter trains in San Francisco, CA. This market developed largely in absence of regulation, although regulators like the U.S. Securities and Exchange Commission are finally starting to pay attention.

Likewise, not only is a bubble often a natural Ponzi scheme, there are many explicit or likely Ponzi schemes. In the early days of Bitcoin approximately 10% of all Bitcoin were invested in Bitcoin Savings and Trust, a Ponzi scheme run by a pseudonymous individual known to the community only as PirateAt40. The editor of *Bitcoin Magazine* at the time so much believed it was not a Ponzi scheme that he made side bets that it was not, using Bitcoin that he did not have, just before the scheme collapsed.

Even explicitly advertised Ponzi schemes see significant activity, such as the "Proof of Weak Hands', a Ponzi scheme implemented as an Ethereum smart contract. More than $1 million in notional value flowed into the scheme in the space of a few hours before the flow stabilized. Two days later, one bug froze the scheme (making withdraws impossible) before a second bug enabled a thief to take all the value.

Systemic Risks

The entire cryptocurrency environment also faces systemic risks including worms, exchanges, central authorities, and government intervention.

Peer-to-peer systems, and especially those written in unsafe languages such as C and C++, are particularly vulnerable to worms. A worm that can exploit a P2P node and then spread to all connected nodes takes approximately the same time to spread worldwide as a broadcast message in the same network. For cryptocurrencies that minimize the time required to send transactions, this would enable a worm to spread globally in a matter of seconds.

The ease of theft and the common practice of speculators using multiple cryptocurrencies create an incentive for thieves to deploy worms, because a worm could spread through one cryptocurrency's network and then steal all other cryptocurrencies accessible on the victim computers. For example,

Dogecoin (coded in C++) has effectively received no updates in two years, yet this explicit joke still has a notional value (at time of writing) of over $550M and is the 27th-largest cryptocurrency. The odds of a wormable vulnerability in the P2P software are significant, especially when combined with the observation that Dogecoin is a fork of Luckycoin's source, which was itself a fork of Litecoin, itself a fork of Bitcoin. Security patches in any of the upstream cryptocurrencies can act as a guide for discovering exploits.

The exchanges themselves also create systemic risks. Almost all exchanges seek to avoid regulation, which means they implode with almost seeming regularity—usually due to a combination of theft and fraud. These exchanges may even participate in active market manipulation.

A previous Bitcoin bubble appears to have resulted from deliberate price manipulation on the MtGox Bitcoin exchange; the current bubble may be due to the Bitfinex exchange creating Tethers and then using them to buy cryptocurrencies. There are also credible allegations of exchanges enabling wash trading, spoofing, insider trading, and other market manipulations.

Finally, cryptocurrencies are actually vulnerable to intervention by central authorities. Although cryptocurrency advocates claim there is no central authority that can censor transactions, the common collectivization of mining into a few entities, combined with official distributions, means small groups can arbitrarily change the rules, and have done so in cases such as a bug-related hardfork in Bitcoin and the Ethereum rollback of the supposedly immutable DAO contract in response to the DAO theft. Both showed that central authorities exist for even the biggest cryptocurrencies and that these authorities can act arbitrarily to rewrite the rules. Such interventions have generally been benign; however, that such interventions are even possible negates the basic thesis that these currencies lack central authorities.

Governments can also intervene to effectively kill cryptocurrencies, should that be desired. The most effective mechanism is simply regulation. Cryptocurrencies have value only when they can be converted back to local currency. By effectively strangling the exchange process, governments can make cryptocurrencies unworkable. Already most exchanges are now cut off from banking, limiting the conversion opportunities. Similar face-to-face individual exchanges (such as those felicitated on LocalBitcoins) are inevitably running afoul of local money-service laws. Enforcing these laws could further limit convertibility.

Governments (or others with a substantial budget) can also attempt technical disruptions. The limited transaction capability can be exploited by a government purchasing a quantity of Bitcoin, and then creating useless transactions. The goal of such a spam campaign would not be simply to clog the network, but also to generate responding spam filters. As the spam campaign continues, the goal becomes to tune the spam so that the filters cause false positives. How can a cryptocurrency work if a non-trivial fraction of legitimate transactions are blocked by spam filters?

Risks to Society

The aforementioned risks are all limited to market participants, and result in various failures. But the greatest risk to society may come not from failures, but from success. Beyond the obvious externalities imposed by cryptocurrency mining (a stable doubling in Bitcoin's price will further double its power consumption), it is primarily criminals who regularly benefit from censorship-resistant payments.

In many cases the bandwidth limit for crime is not the crime itself, but the money laundering. For criminals, cash is censorship-resistant but requires proximity and mass with $1M U.S. weighing approximately 10kg. Euros are more compact, requiring only 1.7kg in 500€ notes for the same value, leading the European Central Bank to begin phasing out the 500€ note. Additionally, it is deliberately difficult to move significant quantities of cash into the rest of the banking system, as deposits over $10,000 or other features generate suspicious activity reports.

If cryptocurrencies succeed, we can expect a great increase in criminal bandwidth. The only reason why the online drug markets remained small (approximately $1M a day in sales despite existing for half a decade) is that Bitcoin and the other cryptocurrencies are like the classic corrupt poker game; yes, it's rigged, but it's the only game in town. A cryptocurrency that actually offered both real anonymity and acted as a store of value (eliminating the need to constantly shift between dollars) would see an explosion in this market.

But such uses would not be limited to criminal-to-criminal transactions but would also act as a vehicle for extortion. The first ransomware epidemic a few years ago offered a choice to victims, either Green Dot or Bitcoin, with almost every victim using the much easier Green Dot, where the victim could purchase a MoneyPak from a convenience store and provide the numbers to the extortionist. It was the U.S. Treasury pressure on Green Dot (to break up a money-laundering flow) that disrupted that epidemic. How much greater would the current ransomware epidemic be if it was easy for victims to pay? How much other criminal extortion would target ordinary citizens?

Conclusion

The risks in the cryptocurrency world are multifaceted and diverse, but fortunately most are limited to those who participate. This leads to a natural conclusion. As the philosopher WOPR said in the movie *WarGames*, "The only winning move is not to play." Ⓒ

> **If cryptocurrencies succeed, we can expect a great increase in criminal bandwidth.**

Reference
1. Jakobsson, M. and Juels, A. Proofs of work and bread pudding protocols (extended abstract). In B. Preneel, Ed., *Secure Information Networks*. IFIP, The International Federation for Information Processing, vol. 23. Springer, Boston, MA, 1999.

Nicholas Weaver (nweaver@icsi.berkeley.edu) is a researcher at the International Computer Science Institute and a lecturer in the CS department at UC Berkeley. He wishes to thank Steve Bellovin for his constructive shepherding of this column.