Removing Impediments to Bitcoin's Success: A Risk Management Study

Bitcoin Foundation Research Brief No. 1

Spring 2014

Removing Impediments to Bitcoin's Success: A Risk Management Study

The Bitcoin Foundation's three-part mission to "standardize, protect, and promote Bitcoin" is a pithy statement of purpose. There is much implicit in that short summary, of course. A granular assessment of the foundation's charge and the challenges it faces can help ensure that the foundation serves all its purposes well. What exactly makes Bitcoin special? What threatens Bitcoin? How can the Bitcoin Foundation protect Bitcoin against these threats?

Articulately studying these questions can help drive community-wide consensus on what makes Bitcoin an asset, what the greatest risks to Bitcoin are, and how to address them. Risk management is an essential tool for exploring these issues and for planning the activities and communications of the Bitcoin Foundation.

In addition to its role in priority-setting and organization, risk management is also a powerful driver of accountability over time. Periodically documenting the Bitcoin Foundation's thinking about its mission and work will reveal successes and failures in prioritization and action. Having set a course, the foundation's leadership and membership can know when its efforts have succeeded or failed. They can also recognize when new information and priorities or unforeseen events have required the foundation to change course.

The Bitcoin Foundation can and should be an intelligent organization that knows what it is doing and why, an organization that learns from experience. The foundation will provide the most value to its membership by subtly and smartly producing a flourishing Bitcoin ecosystem. The unattractive alternative is showily fighting fires in a weakened Bitcoin ecosystem, fires that should never have ignited.

The risk management study that follows is intended to help make the Bitcoin Foundation intelligently responsive to the risks Bitcoin faces. Though it cannot supplant real-time judgment about unfolding events, the study should permit the foundation to recognize and address challenges on the horizon rather than reacting to emergencies as they arrive.

There are complexities, but managing risks to Bitcoin involves a relatively simple series of steps:

- First, an *asset characterization* determines in detail what makes Bitcoin special and what the foundation exists to protect.

- Next, *threat assessment* captures the threats that Bitcoin faces and the likelihood and consequences of these adversities materializing. This permits the foundation to prioritize its responses.
- *Response characterization*, finally, determines in the abstract what steps the foundation should take to address the most likely and most significant threats to Bitcoin's success. This step can guide the activities of the foundation and, to the extent possible, reveal measures of progress toward the outcomes the foundation seeks.

This document follows these steps, reflecting the thinking of the Bitcoin Foundation's leadership at the end of 2013. This study should be renewed regularly with broad input from the foundation's membership. Future reassessments of the risks to Bitcoin will reveal the foundation's successes—ideally in crises and challenges averted—and show where the foundation should focus next.

The vision is a flourishing Bitcoin ecosystem. The question is: How do we remove the greatest impediments to Bitcoin's success?

Asset Characterization: What Makes Bitcoin Bitcoin?

There is no doubt that Bitcoin is special. It is chiefly recognized as a new form of money that is online and non-political, though uses of the Bitcoin protocol well beyond money and payments may develop.

A key characteristic of Bitcoin and a source of its strength is decentralization. Bitcoin's technical functioning, operation, and use should remain the domain of the Bitcoin community and not fall into the hands of any central authority. A second essential element of Bitcoin's success in the shared view of the Bitcoin Foundation's leadership is that Bitcoin should be widely adopted. A third dimension along which Bitcoin is an asset is a suite of aspirational goals, which, though not of the essence for Bitcoin, are important social and economic outcomes.

These three ideas—decentralization, widespread adoption, and laudable outcomes—together comprise the asset that the Bitcoin Foundation should work to protect. They are detailed below.

Decentralization

A strong consensus among Bitcoin Foundation leadership is that *decentralization* is a key part of Bitcoin's essence. Bitcoin is decentralized in all major respects, including:

Software Development

Though the Bitcoin protocol was famously designed by an individual or group known as Satoshi Nakamoto,[1] it was released in 2009 as open source software, to be developed and maintained by the community and no central authority, corporate or government. The Bitcoin Foundation supports a core

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf.

development team for the protocol and software, but the maintenance of both is conducted by the Bitcoin community consistent with open software development principles. The Bitcoin software must always serve the interests of the community as determined by the community.

Mining

New bitcoins are created by finding the solution to mathematical problems, increasing in difficulty over time, that create a new set of entries in the public transaction register, or "blockchain." Mining is decentralized, and anyone should be able to participate in it because of its role in validating transactions on the register. Centralized mining would allow miners to control the content of the register and use that control contrary to the interests of Bitcoin users and the Bitcoin community.

Nodes

Whether mining or not, anyone should be able to operate a node on the Bitcoin network, which is a copy of the public transaction register. Having many nodes keeps the blockchain beyond the reach of any central actor and is key to the operation of the Bitcoin protocol.

Payments

Bitcoin is available for use by anyone, allowing payments to be made, for example, by anyone with access to the Internet, a suitable computing device, and the necessary software. Use of Bitcoin should require the blessing or approval of no central authority or intermediary.

These four decentralized processes together form an essential characteristic of Bitcoin, but decentralization is not the only characteristic that will make Bitcoin successful. Having a large community of users is the second major characteristic that will make Bitcoin the greatest asset it can be.

Adoption

A premise of all visions for Bitcoin's success is widespread adoption. As a global protocol, Bitcoin will exhibit the properties described by Metcalf's Law, which states that the value of a network is proportional to the square of the number of users of the system. Increasing the use of Bitcoin will increase its value to the community, so adoption is essential to Bitcoin's success. This study identifies three factors that will help determine Bitcoin's adoption rate:

Advanced Services

The Bitcoin protocol supports a wide range of advanced services. The development of valuable utilities in the Bitcoin software will provide value to the Bitcoin user community and help drive adoption.

Bitcoin-Based Businesses

A flourishing community of Bitcoin businesses is essential to widespread adoption. Bitcoin businesses, including exchanges, payment systems, storage providers, and others, will mediate between the Bitcoin protocol/software and ordinary users worldwide.

Consumer Acceptance

An important arbiter of adoption is consumer acceptance. Based on ease of use, security, sound business practices, speed, reliability, and more, consumers will determine whether the value proposition offered by Bitcoin is superior or inferior to other infrastructures and services.

Widespread adoption will make Bitcoin a greater asset. While it guards decentralization, the Bitcoin Foundation's success in fostering adoption will help produce a number of outcomes that the foundation's leaders recognize as important.

Outcomes

Though not essential or definitive of Bitcoin itself, a number of outcomes are part of the high aspirations shared by many in the Bitcoin Foundation's leadership and in the Bitcoin community.

Global Financial Inclusion and Economic Development

Bitcoin has high potential to provide billions of unbanked and underbanked individuals around the world with financial services that allow them to accumulate wealth. In April 2012, a World Bank report found that half of adults worldwide are unbanked due to barriers such as high cost, physical distance, and lack of proper documentation.[2] A 2001 study confirms what common sense predicts: Informal saving methods such as keeping physical money in the home are subject to losses—as high as 26% of the amounts saved per year.[3]

Bitcoin and Bitcoin-based financial services may help reduce barriers to financial inclusion because Bitcoin is low-cost, it is available wherever an Internet connection is available, and because transferring and holding Bitcoin requires no documentation. Bitcoin may offer underserved populations both access to more secure formal financial services and more secure informal means of holding financial assets. This holds out hope for rapid advances in wealth and well-being for the billions of capable but impoverished people around the world.

Human Liberty and Dignity

Bitcoin can help people around the world, poor and wealthy alike, realize a greater degree of autonomy, liberty, and dignity.

Deep running principles—in Western thought, at least—emphasize individuals' ownership of themselves and the things they produce: their property. In varying degrees around the world, though, governments and powerful private actors often encroach on people's right and ability to use and dispose of their

[2] Asli Demirguc-Kunt and Leora Klapper, *Measuring Financial Inclusion: The Global Findex Database* (Policy Research Working Paper #6025), The World Bank (2012) http://elibrary.worldbank.org/doi/pdf/10.1596/1813-9450-6025.

[3] Graham A.N. Wright and Leonard Mutesasira, *The Relative Risks to the Savings of Poor People*, MicroSave (2001) http://www.microfinancegateway.org/gm/document-1.9.28889/26216_file_the_relative_risks_.pdf.

property as they see fit. This makes people objects of control or victimization, denying them the dignity of being autonomous, independent, and responsible moral actors whose well-being and self-worth rise or fall based on their own decisions.

Bitcoin may expand individual autonomy, liberty, and dignity because it allows people to deploy their assets less subject to external impediments. Bitcoin can facilitate private and anonymous transactions, which are resistant to oversight and control. Bitcoin transactions can support controversial speech or causes, which governments and powerful private actors may seek to suppress using their control of conventional financial services. Bitcoin is a communications protocol, and it has the Internet virtue of being censorship-resistant.

The right to own, use, and alienate property is not unlimited, of course, and uses of Bitcoin that violate others' rights are properly subject to prevention and punishment.

Privacy

Privacy is not just a means to an end, but an end in itself. Control of information about oneself—one's relations, one's thoughts, feelings, health, and transactions—is the individual's bulwark against objectification by governments, corporations, and other individuals. Privacy is also a means to various ends, including personal security and freedom of speech and action.

Many at the Bitcoin Foundation and in the Bitcoin community are acutely aware that financial transactions in every format including physical cash are subject to some degree of surveillance. For good and bad, centralized payment systems always include overseers and potential gatekeepers. Bitcoin can facilitate more private transactions, which, when legal in the jurisdictions where they occur, are the business of nobody but the parties to them.

Privacy can mask wrongful behavior, and governments do have valid interest in information about activities they have made illegal. There are also circumstances when Bitcoin-based services will require and benefit from collection of information about users, so simple privacy enhancement is not the essence of Bitcoin. But use of the Bitcoin protocol should strengthen the hand of individual users to maintain privacy. Where privacy in financial services today is typically dictated by governments and corporations, the Bitcoin ecosystem may be more amenable to what has been called "user-defined privacy."

Stable Money Supply

A significant benefit of Bitcoin in the eyes of segments of the Bitcoin Foundation's leadership and many in the Bitcoin community is its assurance of a stable base money supply. The Bitcoin protocol provides for mining of a limited number of bitcoins, and that limit cannot be changed without the consensus of the community. The production of bitcoins will slow according to a schedule until around 2140, when the last satoshi will be mined just shy of the 21 millionth bitcoin.

The rate of new Bitcoin mining is similar to the mining rate of precious metals such as gold or silver. They have a low rate of new creation relative to the existing base, which means that added supply does not significantly debase the value of the existing stock. Like these precious metals and unlike fiat currencies, the stock of Bitcoin cannot increase rapidly, causing them to drop in value relative to other goods.

This means that Bitcoin is largely inflation proof. Time and experience may prove it to be a more stable store of value than any fiat currency, while it comes to enjoy advantages over precious metals in other respects, such as transferability, divisibility, security in transfer and storage, and so on. This makes Bitcoin a potential key to financial well-being for savers and investors worldwide.

These outcomes—global financial inclusion, increased liberty and dignity, user-defined privacy, and a stable money supply—may not all occur quickly or in equivalent measures, but they will be important products of Bitcoin's success. Widespread acceptance of Bitcoin is an essential means towards these ends. Preservation of Bitcoin's comprehensive decentralization is what will allow them to materialize. This collection of characteristics is what makes Bitcoin the asset that it is.

Knowing what makes Bitcoin special—the asset characterization above—permits detailed analysis of what most threatens Bitcoin. That is the subject to which this study now turns.

Threat Assessment: What Threatens Bitcoin?

With the dimensions of Bitcoin that make it unique and valuable in hand, we now turn to the threat environment for those characteristics. A threat is any actor or condition that may produce an unwanted outcome. Threat characterization seeks out the threats to Bitcoin that are the most likely to happen and that will have the greatest negative effects if they do. Weighing the relative likelihood and consequence of threats determines which threats to address first and with the most intensity.

Threats Assessed by Likelihood and Consequence

During the fall of 2013, a series of interviews with, and polling of, members of the Bitcoin Foundation's leadership produced a long list of threats to Bitcoin in the many dimensions that make it an asset. The process ranked those threats on a scale of 1 to 7 along two dimensions: the likelihood of the threat materializing and the consequence if the threat does materialize. This was intended to produce a general sense of the threats that are most significant, the strongest candidates for the foundation to address promptly.

The following charts illustrate the risk profile for each of Bitcoin's major dimensions. Each threat is graphed on the chart in terms of likelihood (x-axis) and consequence (y-axis).

The charts suggest that decentralized software development, for example, is fairly secure compared to other Bitcoin dimensions, with most all threats to it lying below the "red" zone. Decentralized mining and decentralized nodes each have one or two threats on the high side.

The decentralized payments chart shows that banks' refusal to deal with Bitcoin is a prominent threat, both likely and consequential. Indeed, it is the top threat based on the simple formula of multiplying likelihood and consequence together.

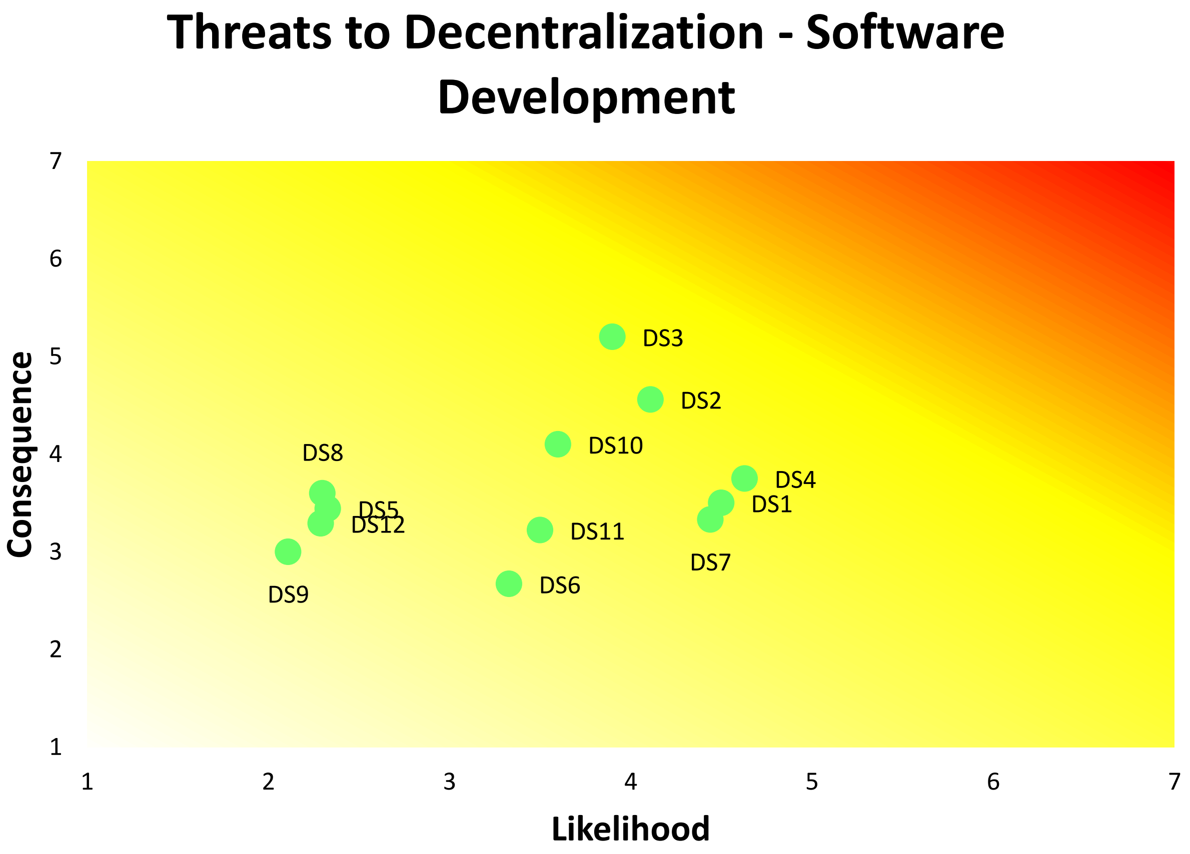
In the area of Bitcoin adoption, advanced payment services appear not seriously threatened relative to other dimensions. The threats to Bitcoin businesses range higher. Threats to consumer acceptance range higher still.

The chart of threats to global financial inclusion show that the greatest threats to Bitcoin's success in this area cluster around lack of local Bitcoin services, inability to exchange among Bitcoin and local currencies, and inability to transact in Bitcoin directly.

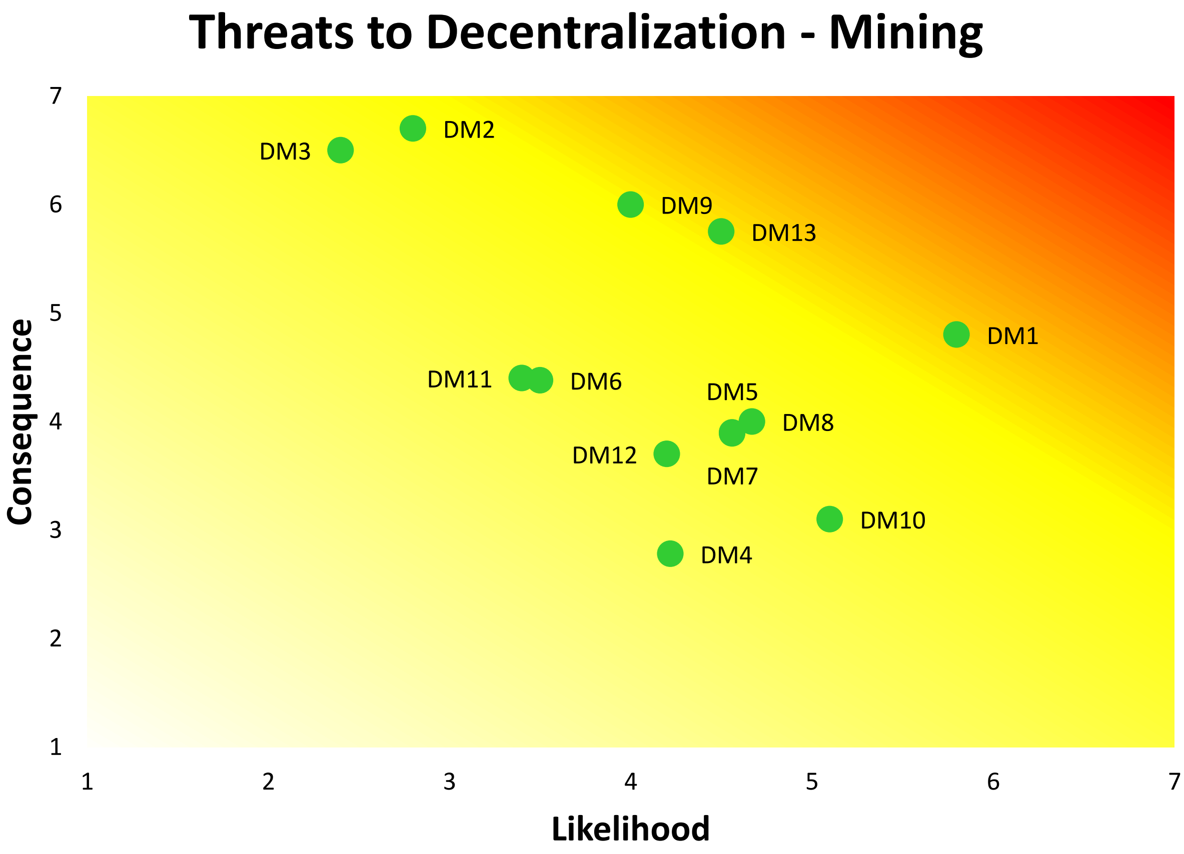
The liberty and dignity outcome goal is fairly secure relative to other Bitcoin dimensions, while the privacy outcome goal is quite besieged. The second highest threat, according to the "likelihood x consequence" multiplier, is a threat to privacy: "Governments seize data excessively using warrants and subpoenas." Revelations in 2013 about U.S. government data-gathering evidently strengthen perceptions of threat and risk in this area.

The "stable money supply" outcome goal includes a few high outliers. These show that both the reality and perception of volatility should be controlled.

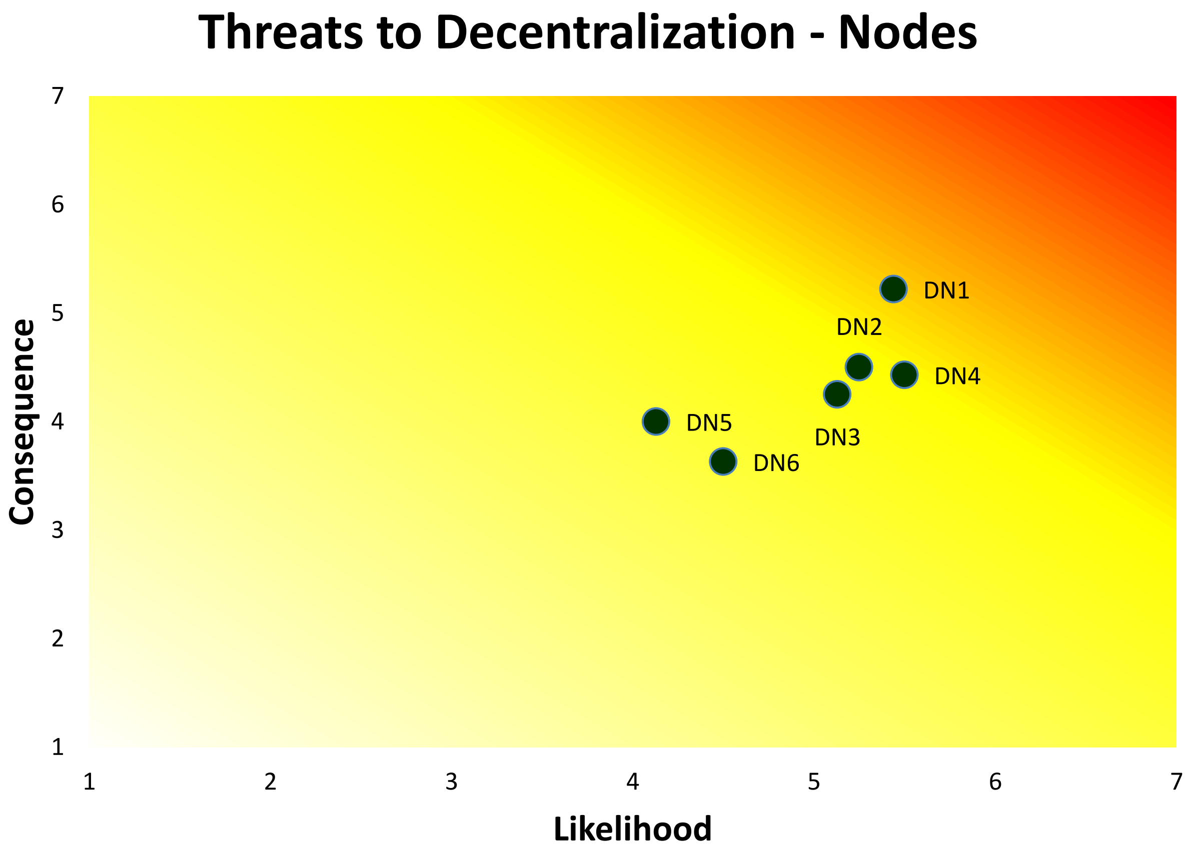
The charts below, each with a corresponding legend showing the threats under consideration, illustrate the threat profile for the important dimensions of Bitcoin. The final step of the study, which follows the charts, groups the threats rising to the top and characterizes the responses that are germane to each group.



DS1	A rift among developers slows development
DS2	A rift among developers leads to a hard fork
DS3	A significant bug exists in the protocol
DS4	A significant bug exists in the code
DS5	Gavin goes missing
DS6	Other developers go missing
DS7	A forked version of the software gains ground
DS8	Satoshi Nakamoto reappears and says the project has gone wrong
DS9	There’s no more money to pay Gavin
DS10	Intellectual property claims arise against the protocol/software
DS11	Compensation of developers undercuts credibility of development process
DS12	Github/Sourceforge drop Bitcoin development



DM1	Mining becomes too expensive for anyone but a small number of specialists
DM2	Mining falls into the hands of one miner
DM3	Mining ceases
DM4	Specialized chips don’t work as advertised
DM5	A government makes mining subject to registration
DM6	Purchase of mining chips is subject to registration
DM7	A dispute about the proof-of-work arises
DM8	A dispute about the proof-of-work causes miners to drop out
DM9	Mining becomes economically infeasible
DM10	Mining is taxed
DM11	Mining is too heavily taxed
DM12	Criminal proceeds used to buy mining chips, toward the end of laundering funds
DM13	Miners execute a 51% attack



DN1 Blockchain “bloat” raises costs of running nodes

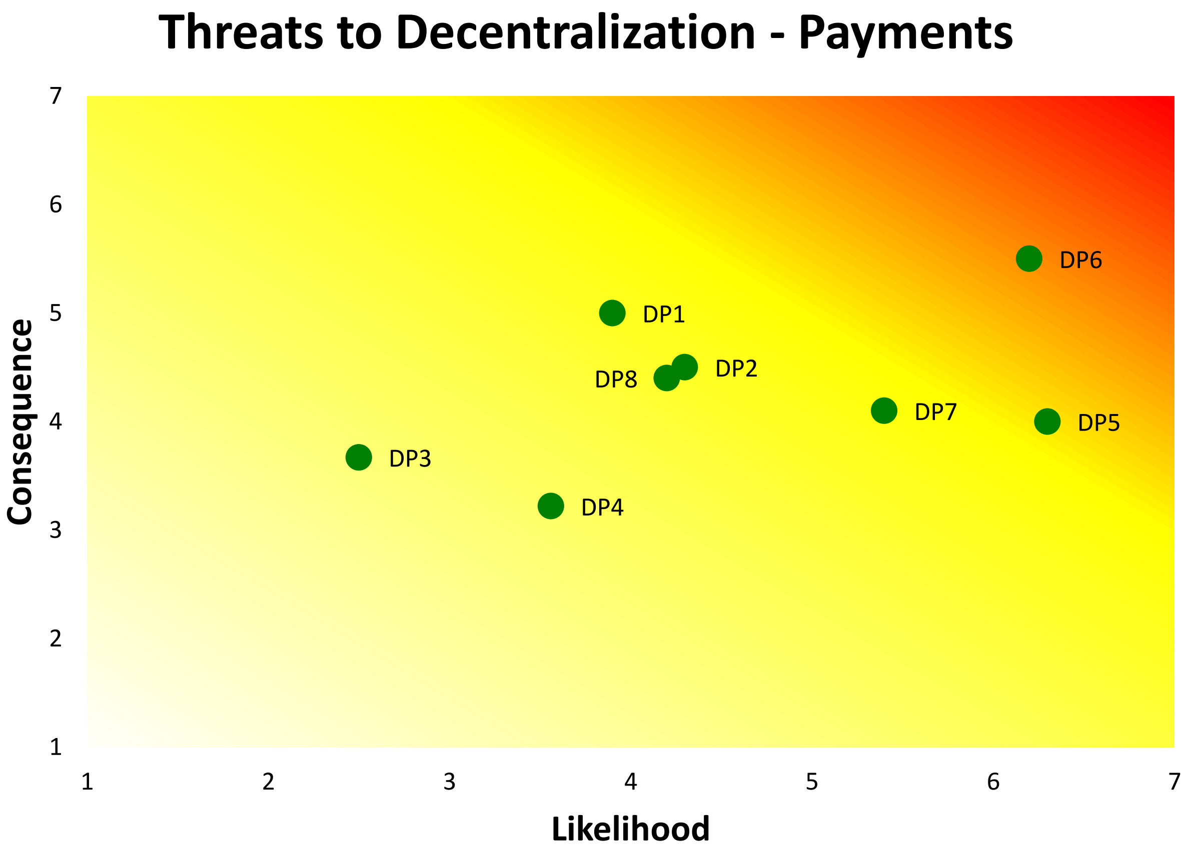
DN2 There being no benefit to running a node, the number of nodes/user shrinks

DN3 Transaction volume becomes so high that only backbone-datacenter nodes can handle it

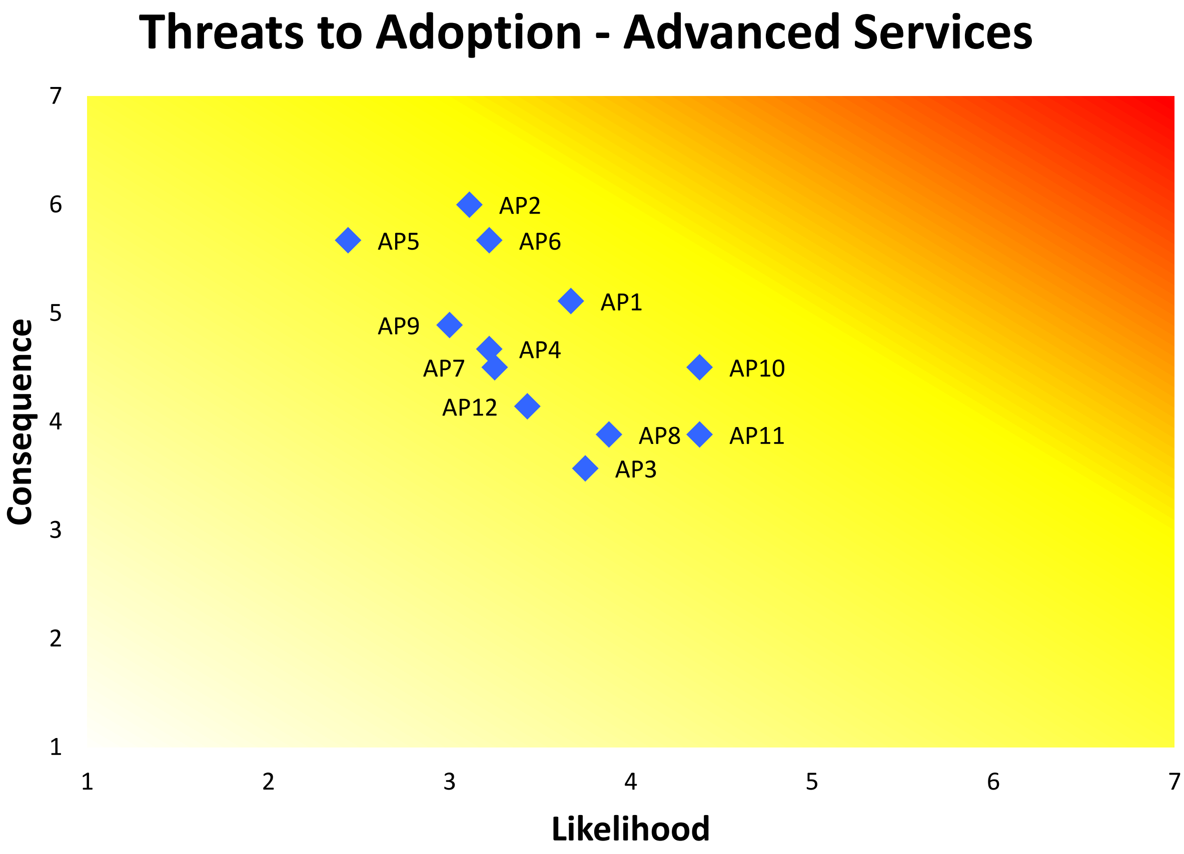
DN4 DDoS attacks

DN5 ISPs block the DNS seed nodes

DN6 A country or countries block Bitcoin traffic

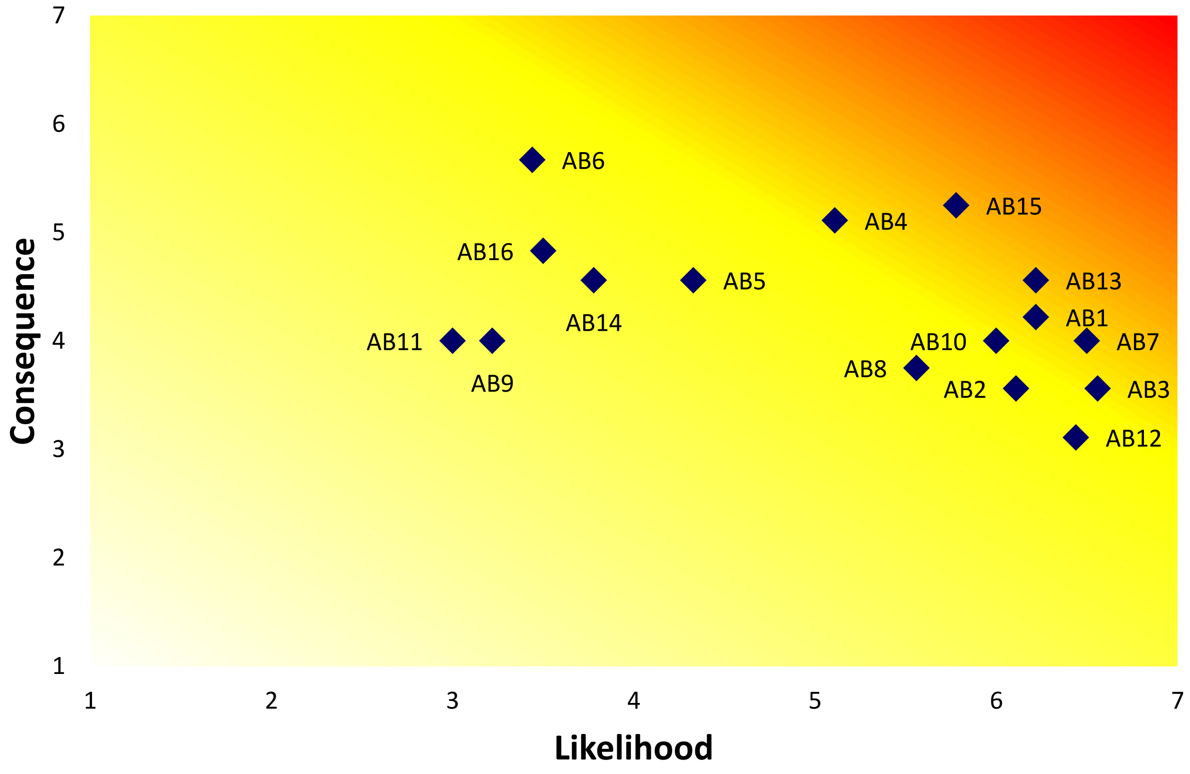


DP1	Governments outlaw Bitcoin payments
DP2	Regulation requires Bitcoin-receiving businesses to register
DP3	An electro-magnetic pulse attack cripples power systems in a big chunk of the world
DP4	Connectivity between major population centers is interrupted for more than a few hours
DP5	A government produces its own digital currency
DP6	No explicit outlawing, but banks decide any Bitcoin activity is too risky to deal with and they close accounts of users
DP7	Revenue agencies require reporting of payments
DP8	Revenue agencies require too onerous reporting of payments

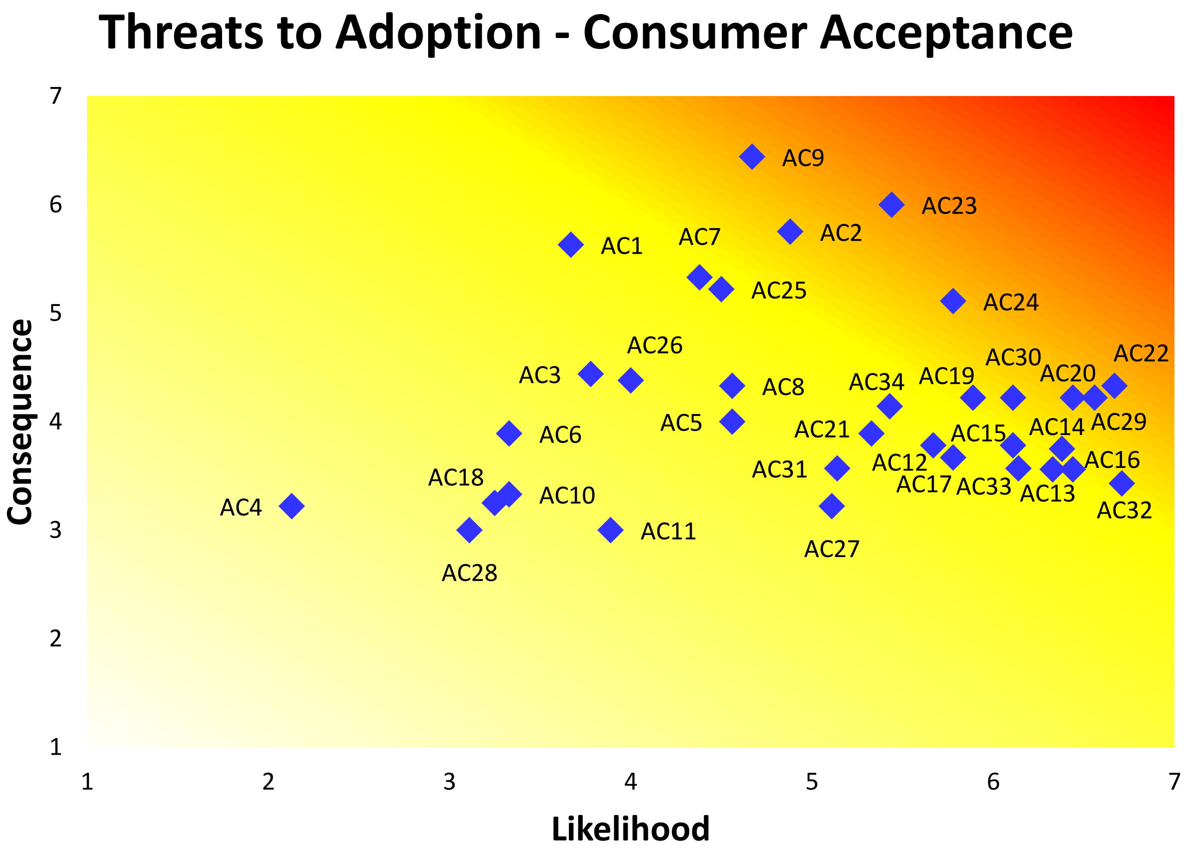


AP1	Wallet/storage/banking services see few legitimate entrants
AP2	Wallet/storage/banking services remain obscure and complex to average users
AP3	Payment protocol under X.509 CA architecture fails to gain acceptance
AP4	Microtransaction services do not materialize or take hold
AP5	Exchange services do not take off
AP6	Merchant services fail to see adoption
AP7	Protocol-level escrow services fail to see adoption
AP8	Escrow/intermediary businesses fail to see adoption
AP9	The Bitcoin “killer app” doesn’t materialize
AP10	A software bug collapses a Bitcoin service
AP11	The NSA undercuts encryption standards
AP12	Someone cracks an encryption standard

Threats to Adoption - Bitcoin Businesses



AB1	Government regulations of Bitcoin exchanges raise costs
AB2	A government seizes a Bitcoin business’s assets
AB3	Government regulations raise barriers to entry
AB4	Bad reputation of Bitcoin causes customers to shy away
AB5	A government outlaws exchanging Bitcoin and fiat currency
AB6	The Bitcoin “killer app” doesn’t materialize
AB7	A Bitcoin business suffers DDOS attacks
AB8	A mismanaged Bitcoin business casts doubt on Bitcoin
AB9	It’s hard to find quality employees
AB10	Potential investors in Bitcoin businesses hear bad things about Bitcoin
AB11	A government bars investment in Bitcoin businesses
AB12	A government subpoenas investors in Bitcoin businesses
AB13	Speculators manipulate the price of Bitcoin
AB14	States/central banks manipulate the price of Bitcoin
AB15	Revenue agencies produce unwieldy rules re: digital currency transactions
AB16	DDOS protection services fail or decline to serve Bitcoin businesses



AC1 People come to believe Bitcoin is only for drugs and terrorist financing

AC2 Compromise of Bitcoin wallets produce widespread theft

AC3 A government bars individuals from using Bitcoin

AC4 Satoshi Nakamoto reveals himself and criticizes current implementation of Bitcoin

AC5 A government bars Bitcoin remittances

AC6 Use of Bitcoin not “cool”

AC7 Users regard Bitcoin as insecure

AC8 A government outlaws exchanging Bitcoin and fiat currency

AC9 Users decline to adopt Bitcoin

AC10 Power outages show Bitcoin less useful for transactions than physical cash

AC11 Environmental concerns arise around computing power used for mining

AC12 A mismanaged Bitcoin business casts doubt on Bitcoin

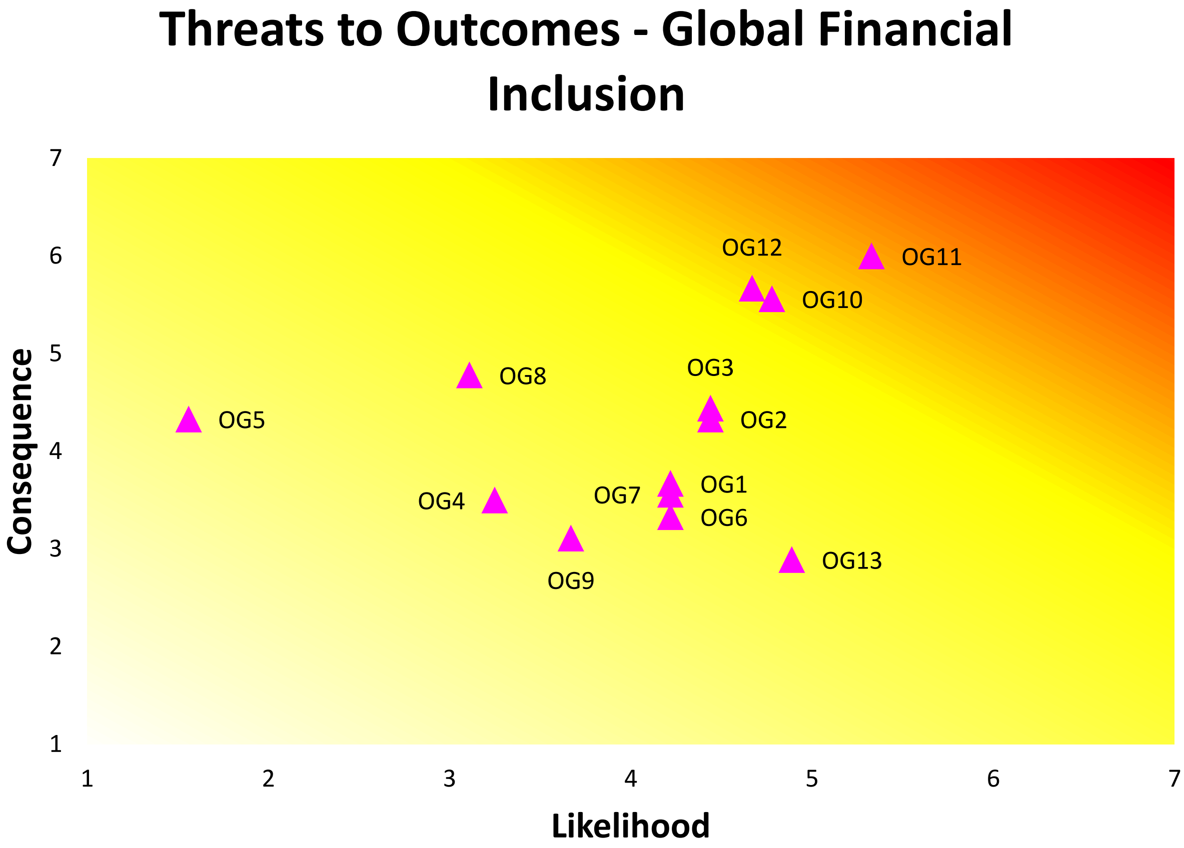
AC13 A Bitcoin business is hacked and Bitcoins are stolen

AC14 A Bitcoin business suffers DDOS attacks

AC15 Terrorists use Bitcoin

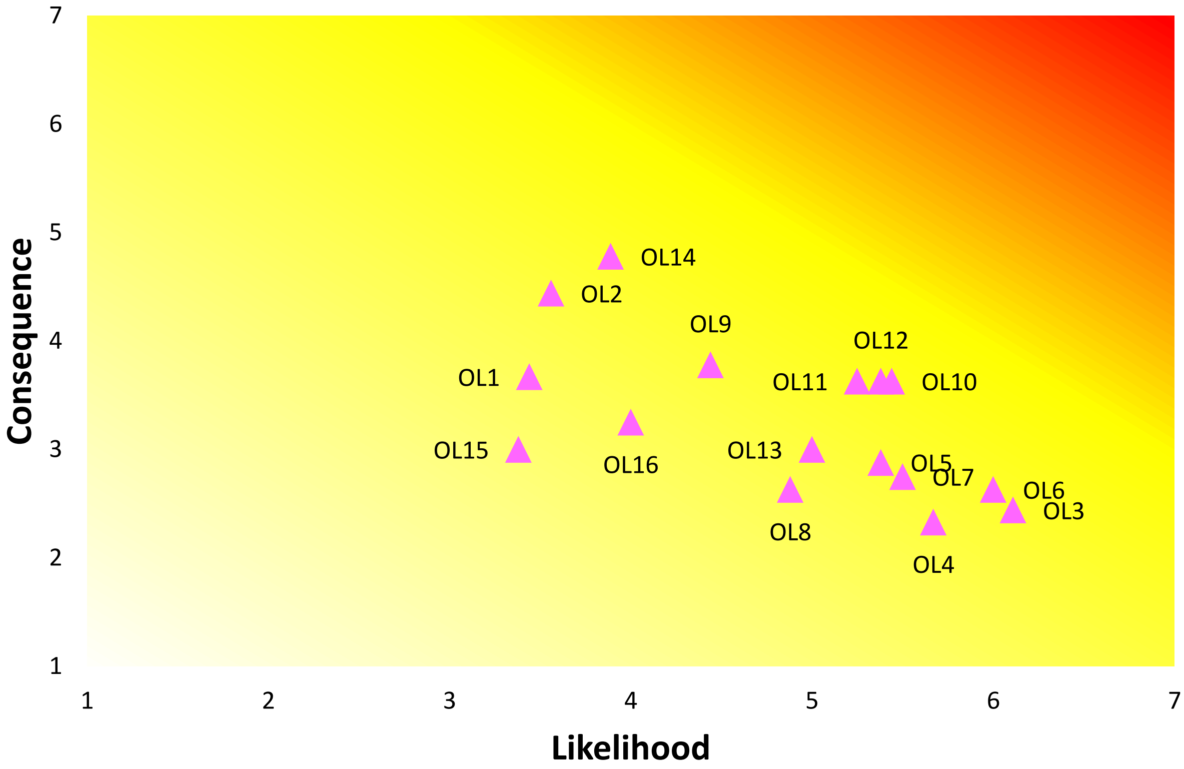
AC16 Drug dealers use Bitcoin

AC17 Drug cartels use Bitcoin
AC18 Bitcoin kidnappings become common
AC19 People use Bitcoin to buy and sell child porn
AC20 Politicians talk about Bitcoin being used to support “narcoterrorism”
AC21 People don’t understand fractions of Bitcoin beyond hundredths
AC22 Consumers have a hard time dealing with long strings as addresses
AC23 People can’t find retailers that accept Bitcoin
AC24 Manipulations of the price of Bitcoin create the appearance of volatility, unreliability
AC25 Revenue agencies produce unwieldy rules re: digital currency transactions
AC26 Alternative protocol with centralised dependency gains acceptance
AC27 Non-reversability draws criticism to Bitcoin vis a vis other payment systems
AC28 Bitcoin-based lenders are seen as predatory
AC29 Politicians and regulators talk about Bitcoin being used to buy drugs
AC30 Politicians and regulators talk about Bitcoin being used to buy child porn
AC31 Consumers are confused by multiple competing digital currencies
AC32 Bitcoin is used for gambling
AC33 Politicians and regulators talk about Bitcoin being used for gambling
AC34 Politicians and regulators seek to thwart use of Bitcoin for gambling

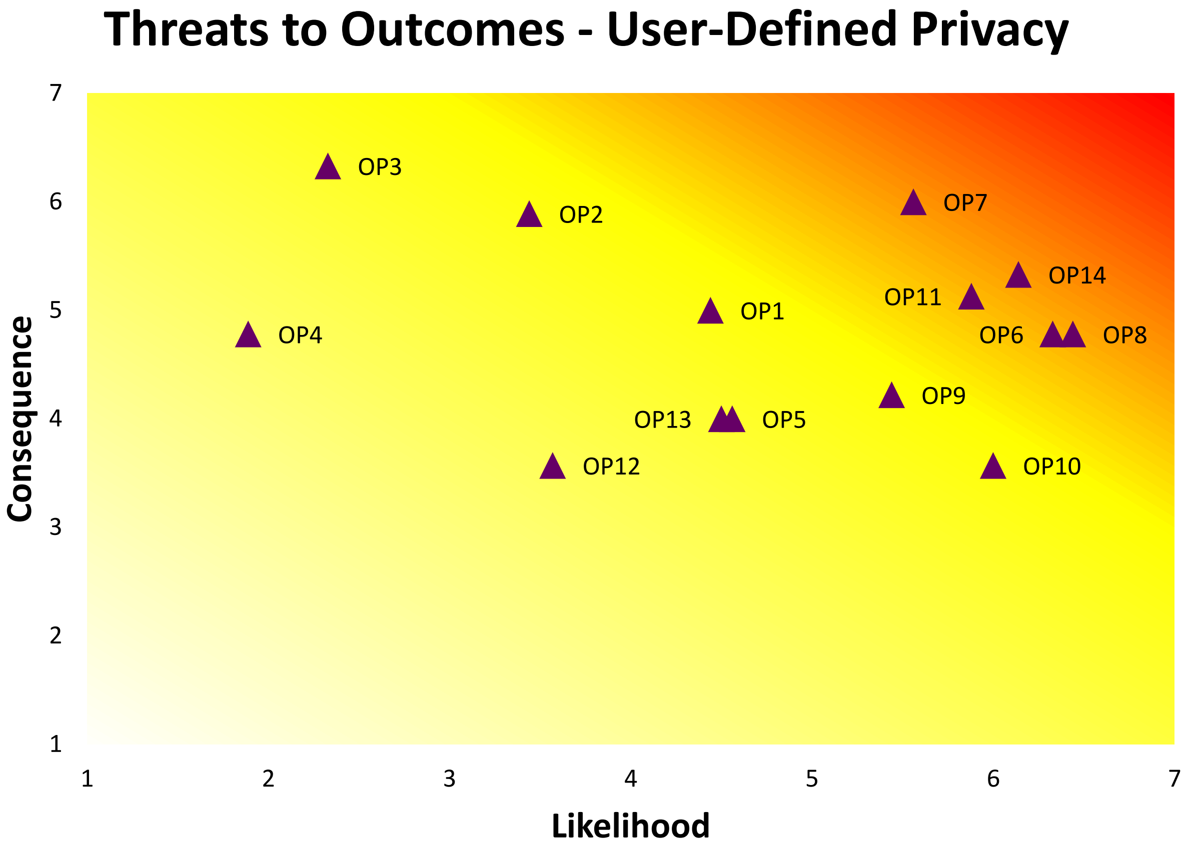


OG1	A government bans remittances
OG2	A government bans Bitcoin
OG3	Power outages degrade Bitcoin’s utility in third world countries
OG4	Bitcoin kidnappings become common
OG5	Not enough smartphones
OG6	Third-world users lack financial sophistication
OG7	Third-world users lack technical sophistication
OG8	Insufficient Internet/mobile phone access
OG9	People habitually store their money under the bed
OG10	Lack of Bitcoin convertibility to local currency
OG11	Lack of local merchants accepting Bitcoin
OG12	Lack of services that accept Bitcoin remittances and pay out in local currency
OG13	Property rights protections are insufficient

Threats to Outcomes - Liberty and Dignity



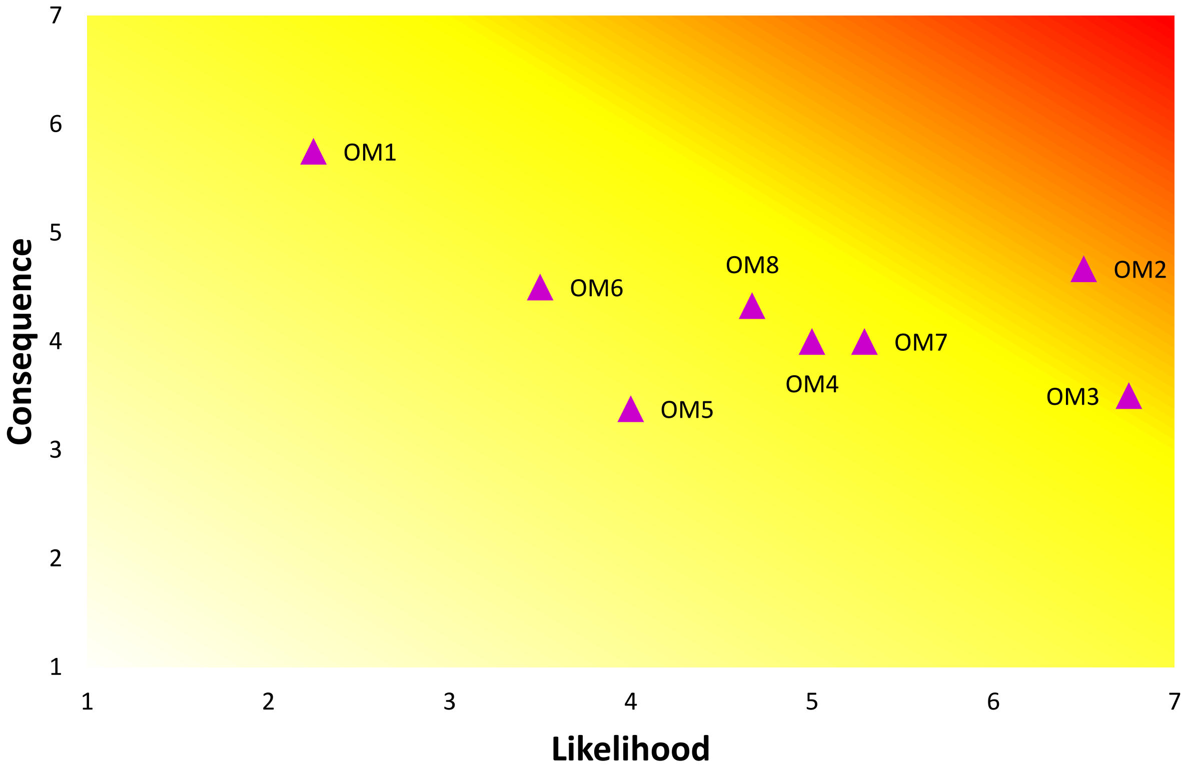
OL1 Governments ban Bitcoin use
OL2 Governments condition Bitcoin use on registration or identity requirements
OL3 Governments bar certain uses of Bitcoin
OL4 Governments blacklist certain Bitcoin addresses
OL5 Businesses condition Bitcoin use on registration or identity requirements
OL6 Businesses bar certain uses of Bitcoin
OL7 Businesses blacklist certain Bitcoin addresses
OL8 People shy away from controversial expenditures because of public blockchain
OL9 Consumers don’t trust that Bitcoin transactions will remain private from other individuals
OL10 Consumers don’t trust that Bitcoin transactions will remain private from the government
OL11 Consumers don’t trust that Bitcoin transactions will remain private from businesses
OL12 Anonymous Bitcoin transactions are re-identified
OL13 Private Bitcoin transactions are revealed
OL14 The blockchain, combined with Internet, social media, and transactional data, reveals everything
OL15 Services meant to provide private Bitcoin transactions fail to materialize
OL16 Services meant to provide private Bitcoin transactions don’t actually provide privacy



Threats to Outcomes - User-Defined Privacy

OP1	Governments require each party to know the other in Bitcoin transactions
OP2	Governments require the Bitcoin protocol to identify parties to transactions
OP3	Governments require Bitcoin transactions to include identity information and be published
OP4	Governments bar Bitcoin transactions from being user-identified
OP5	Businesses require each party to know the other in bitcon transcations
OP6	Governments subpoena or gather by warrant Bitcoin businesses’ data
OP7	Governments seize data excessively using warrants and subpoenas
OP8	Governments require businesses to turn over data about customers
OP9	Governments monitor Bitcoin transactions at ISP/backbone level
OP10	Algorithmic monitoring of Bitcoin transactions becomes commonplace
OP11	Identity “leaks” make private transactions public
OP12	Someone cracks an encryption standard used in the Bitcoin protocol
OP13	Someone cracks an encryption standard used in a Bitcoin service
OP14	Users don’t understand how Bitcoin transactions affect privacy

Threats to Outcomes - Stable Money Supply



OM1 Bitcoin community too readily changes Bitcoin supply
OM2 Bitcoin perceived as “volatile”
OM3 Bitcon prices against other currencies rise and fall
OM4 Failure of a fiat currency drives a buying spree of Bitcoin
OM5 Central banks manage their money well
OM6 Miners and developers agree to lift the cap on Bitcoin production
OM7 A large holder cashes out of bitcon
OM8 Multiple alternative digital currencies are seen as expanding the money supply

Response Characterization

With Bitcoin's key characteristics in hand and the most prominent threats in view, we are positioned to characterize the responses that will control threats to Bitcoin.

Determining the most important threats is not as simple as picking the threats with the highest likelihood and consequence, though those threats are certainly worth noting. Many threats restate one another in different ways or from different perspectives. So this step classifies the more substantial threats, grouping them together so they can receive the appropriate response.

We selected the top 40% of threats (by likelihood x consequence) because at this threshold each of Bitcoin's essential dimensions has at least one threat. From these top threats, a suite of threat themes emerges. Some of the themes below clearly deserve more attention than others, but each of the following issue areas should be the subject of some response and tracking over time to see if the threat environment gets better or worse.

For each theme there are certain types of response that are appropriate. Response types fall into four categories:

> *Acceptance*: Threats that are low in likelihood, low in consequence, or both can be accepted, as they are not significant risks. Threats that are impossible to address cost-effectively are also candidates for acceptance (and mitigation).
>
> *Prevention*: The ideal response, if available, is to change circumstances so that significant threats cannot manifest themselves.
>
> *Interdiction*: If intervening with the actor or actors that contribute to the threat can reduce its likelihood or consequence, this is the response to use.
>
> *Mitigation*: When a threat will manifest itself, efforts to reduce its consequences are the appropriate response.

For each area below, we summarize the area, sample the top threat or threats, and identify the responses that are available, as well as measures of success when they exist.

Software Development

Decentralized software development inures the protocol and software against capture by any central authority, so that the Bitcoin infrastructure serves the Bitcoin community as determined by the community. The top threat to decentralized software development is not a threat to the development process itself, but rather the potential that the Bitcoin protocol has a major error. This is a low-likelihood, high-consequence threat with a (likelihood x consequence) “multiple” that is low compared to threats to other dimensions of Bitcoin. Assuming it does not materialize, this threat will continue to drop in likelihood as time tests the protocol from every direction.

Top threat:

- A significant bug exists in the protocol

Response:

Acceptance – Naturally occurring testing of the Bitcoin protocol and software is the most appropriate response. Nothing additional is needed.

Decentralized Mining

Miners produce the public ledger, or “blockchain,” which is the record of all Bitcoin transactions. Centralized mining would give a small group control over the content of the blockchain, which they could use contrary to the interests of the community, so decentralized mining is essential for Bitcoin’s success. The wrong interaction between the Bitcoin “proof of work,” technical conditions with respect to computing technology, and economics could produce centralized mining. Though the chance of this happening is generally low, the consequence is high.

Top threats:

- Mining becomes too expensive for anyone but a small number of specialists
- Miners execute a 51% attack
- Mining becomes economically infeasible

Response:

Prevention – Make sure the mining protocols and the economics of mining prevent these outcomes.

Measurement:

- number of miners or mining pools
- concentration of mining

Nodes

Nodes are the computers and servers around the world that maintain copies of the public transaction register. Having many nodes keeps the blockchain beyond the reach of any central actor and is key to the operation of the Bitcoin protocol.

Top threats:

- Blockchain “bloat” raises costs of running nodes
- DDoS attacks

- There being no benefit to running a node, the number of nodes/user shrinks
- Transaction volume becomes so high that only backbone-datacenter nodes can handle it

Responses:

Prevention – Make sure the economics of running nodes works to sustain their numbers.
Interdiction (node operators) – Prepare to thwart DDOS attacks.

Measurement:

- number of nodes
- number of DDOS attacks on nodes, number of successful DDOS attacks on nodes

Banking

Banks and other financial services providers are well-positioned to provide a broad interface between Bitcoin and traditional money systems. Their doing so would produce tremendous gains in adoption. They presently appear reluctant to provide services to Bitcoin businesses or to provide Bitcoin services themselves.

Top threats:

- No explicit outlawing, but banks decide any Bitcoin activity is too risky to deal with and they close accounts of users
- Lack of bitcoin convertibility to local currency
- Lack of services that accept Bitcoin remittances and pay out in local currency

Responses:

Interdiction (banks) – Educate and inform banks about Bitcoin and the fact that Bitcoin businesses can be as sound as any. Encourage banks to provide Bitcoin services themselves.
Interdiction (regulators) – Discourage any discouragement of banks to serve Bitcoin businesses or to provide Bitcoin services themselves.
(See also: “Reputation” below)

Measurement:

- number of banks serving Bitcoin businesses
- number of traditional bank accounts held by Bitcoin businesses
- number of banks providing Bitcoin-based services (overall and by country/currency)

Money Supply

The reality and perception of Bitcoin as a stable and reliable money supply will be an important part of its success, redounding to the benefit of many other dimensions of Bitcoin success, such as banking, development of Bitcoin businesses, consumer acceptance, and global financial inclusion. In countries where fiat money is poorly managed, the option of using Bitcoin to store value can preserve wealth and in turn provide essential margins of housing, nutrition, health care, and other human necessities.

Top threats:

- Bitcoin perceived as “volatile”
- Manipulations of the price of Bitcoin create the appearance of volatility, unreliability
- Speculators manipulate the price of Bitcoin
- A government produces its own digital currency
- Bitcoin prices against other currencies rise and fall
- A large holder cashes out of Bitcoin
- Multiple alternative digital currencies are seen as expanding the money supply
- Failure of a fiat currency drives a buying spree of Bitcoin

Responses:

Acceptance: Volatility cannot be countered directly. It will, however, fall naturally as adoption increases to Bitcoin’s worldwide scale and as Bitcoin trading deepens.

Interdiction (fraudsters) – Support efforts to counter genuinely fraudulent manipulations of Bitcoin’s price against other currencies (not to include investing, speculation, arbitrage, and other sophisticated price-discovery behaviors).

Interdiction (governments) – Oppose government policies or practices that manipulate Bitcoin prices or interfere with normal price discovery in Bitcoin markets.

Mitigation – Educate the public about the decrease in volatility that Bitcoin will experience at scale, the insignificance to payment models that convert in and out of Bitcoin in near real-time, and (when they occur) the large transactions that have affected Bitcoin’s price against other currencies.

Measurement:

- volatility
- public perception re: volatility
- number of instances of fraudulent price manipulation and their extent
- number of instances of governmental price manipulation and their extent

Privacy

Rapid and massive change in information technology over the last two decades has acutely challenged people’s ability to control information about themselves and to protect privacy as they see fit. Both governments and corporations are taking advantage of this for their purposes, to intensely oversee and investigate their populations in the case of government, and to study, monitor, and market to consumers in the case of corporations.

Bitcoin users are responsible for protecting their privacy in the first instance. In need of knowledge about the privacy consequences of Bitcoin use, they must determine what privacy they want, and when they want to trade personal information for goods they prize more. Unsurprisingly in light of news about U.S. government surveillance since the summer of 2013, governments are perceived as the greater threat to privacy in the Bitcoin ecosystem. They may directly utilize the Bitcoin blockchain, require data collection by Bitcoin businesses, seize data gathered by Bitcoin businesses, or even seek to amend the protocol and software for law enforcement purposes.

Top threats:

- Governments seize data excessively using warrants and subpoenas
- Users don't understand how Bitcoin transactions affect privacy
- Governments subpoena or gather by warrant Bitcoin businesses' data
- Identity "leaks" make private transactions public
- Governments monitor Bitcoin transactions at ISP/backbone level
- Governments require each party to know the other in Bitcoin transactions
- Algorithmic monitoring of Bitcoin transactions becomes commonplace
- Governments require the Bitcoin protocol to identify parties to transactions

Responses:

Prevention (consumers) – Educate consumers about privacy consequences of varied Bitcoin uses.
Prevention (businesses) – Promote privacy excellence among Bitcoin businesses, including robust privacy policies and practices, and defend Bitcoin businesses in defending their privacy promises.
Interdiction (government) – Support reasonable laws regarding government acquisition of data for law enforcement purposes.
Interdiction (government) – Oppose illegal Bitcoin-related data seizures wherever they occur.
Interdiction (government) – Oppose anti-privacy regulation of Bitcoin businesses and transactions.
Interdiction – Oppose illegal and illegitimate Bitcoin-related data collection and processing.

Measures:

- consumer surveys of privacy perceptions with respect to Bitcoin
- adequacy of laws regarding government acquisition of data for law enforcement purposes
- prevalence and robustness of privacy/information policies offered by Bitcoin businesses

Consumers/Markets

A flourishing, successful community of users is essential to Bitcoin's success, and removing impediments to successful marketplaces is a worthwhile and achievable goal. This includes educating individual consumers and businesses of all kinds about the benefits of using Bitcoin, promoting good business practices in the Bitcoin community, and promoting security in the use and holding of Bitcoin.

Top threats:

- People can’t find retailers that accept Bitcoin
- Lack of local merchants accepting Bitcoin
- Users decline to adopt Bitcoin
- Consumers have a hard time dealing with long strings as addresses
- Compromise of Bitcoin wallets produce widespread theft
- Lack of Bitcoin convertibility to local currency
- Lack of services that accept Bitcoin remittances and pay out in local currency
- A Bitcoin business suffers DDOS attacks
- A Bitcoin business suffers DDOS attacks
- Users regard Bitcoin as insecure
- A Bitcoin business is hacked and Bitcoins are stolen
- A mismanaged Bitcoin business casts doubt on Bitcoin
- A mismanaged Bitcoin business casts doubt on Bitcoin
- People don’t understand fractions of Bitcoin beyond hundredths

Responses:

Interdiction (businesses) – Foster Bitcoin-based payments and acceptance of Bitcoin.
Interdiction (businesses) – Promote trustworthy management of Bitcoin businesses.
Interdiction (consumers) – Educate consumer about Bitcoin services and ease of use.
Interdiction (consumers) – Promote security in holding and transferring Bitcoin.

Measures:

- number of Bitcoin users
- transaction rate reflecting consumer use

Regulation

The expense and market dislocations created by poorly crafted regulations will have acute effects in the Bitcoin ecosystem because of their disproportionately large effects on the many new and small Bitcoin businesses. There is no reason to seek exemption for Bitcoin businesses from well-crafted and meritorious regulation, of course, and there is no reason for special, new regulation of Bitcoin or other digital currencies. Early, uninformed policymaker commentary on Bitcoin should give way to the sensible, thought-through regulations that protect consumers while embracing Bitcoin’s benefits. The Bitcoin ecosystem will benefit from clear, fair, and predictable tax rules that treat Bitcoin equally to other systems for transmitting and storing value.

Top threats:

- Revenue agencies produce unwieldy rules re: digital currency transactions

- Government regulations of Bitcoin exchanges raise costs
- Revenue agencies produce unwieldy rules re: digital currency transactions
- Government regulations raise barriers to entry
- Revenue agencies require reporting of payments
- A government seizes a Bitcoin business's assets
- A government subpoenas investors in Bitcoin businesses

Responses:

Interdiction (governments) – Oppose poorly crafted regulation and tax rules.
Interdiction (governments) – Oppose unwarranted investigations and seizures.

Reputation

The reputation of Bitcoin will have substantial effects on its acceptance and adoption. Bitcoin's reputation is at risk from an interesting union between bad actors, who may use Bitcoin for genuinely wrongful purposes, and the politicians and media who will emphasize and exploit examples of wrongful use for their purposes. The vast potential benefits of Bitcoin are almost always ignored by attention-grabbing media stories and the occasional attention-seeking politician or regulator. Inherently wrongful uses of Bitcoin should be opposed, of course (without giving support for morals legislation or censorship). Exaggerated claims and FUD-mongering about Bitcoin should also be opposed. (FUD = "Fear, Uncertainty, and Doubt") The foundation should relentlessly promote illustrations of the benefits Bitcoin can deliver to people around the globe.

Top threats:

- Politicians and regulators talk about Bitcoin being used to buy drugs
- Politicians talk about Bitcoin being used to support "narcoterrorism"
- Bad reputation of Bitcoin causes customers to shy away
- Politicians and regulators talk about Bitcoin being used to buy child porn
- People use Bitcoin to buy and sell child porn
- Potential investors in Bitcoin businesses hear bad things about Bitcoin
- Terrorists use Bitcoin
- Bitcoin is used for gambling
- Drug dealers use Bitcoin
- Politicians and regulators seek to thwart use of Bitcoin for gambling
- Politicians and regulators talk about Bitcoin being used for gambling
- Drug cartels use Bitcoin
- People come to believe Bitcoin is only for drugs and terrorist financing

Responses:

Interdiction (bad actors) – Oppose Bitcoin uses for purposes wrong in themselves (i.e., *malum in se* – not *malum prohbidum*).
Interdiction (politicians/media) – Oppose FUD-mongering.
Mitigation – Show that beneficial Bitcoin uses and outcomes outweigh costs of wrongful uses.

Measures:

- public opinion surveys regarding Bitcoin and its uses

Summary

Having captured Bitcoin's essence in the asset characterization section, this study assessed the threats to Bitcoin's essential characteristics that are the most likely and consequential. These most important threats should be addressed first and most adroitly. The response characterization grouped these threats into categories.

The response characterization shows what initiatives might do the most to ward off threats to the Bitcoin ecosystem and remove barriers to Bitcoin's success. It also makes clear what audiences should be the object of the Bitcoin Foundation's communications and educational efforts.

Though this study cannot substitute for judgments about how to respond to events as they unfold, it should be a helpful guide to thinking about issues that arise. Unfolding history is the best teacher, of course, and this study should be renewed regularly so that the foundation's efforts can be tuned while the quality, focus, and success of its past work can be judged.

Success for the Bitcoin ecosystem, of course, holds out results that should be universally appreciated: greater global financial inclusion, advances for human liberty and dignity, greater privacy for the law-abiding, and a stable money supply that permits better economic planning and saving. It is an audacious goal, but the right one for a revolutionary technology: Bitcoin should allow every one of the world's people to have a brighter future.