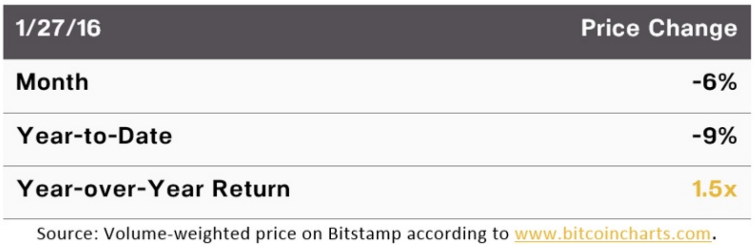
The Governance of Anarchists :: Blockchain Letter, January 2016

Dear Community,

Bitcoin's volume-weighted price on the Bitstamp exchange fell 6% month over month. Year-to-date, bitcoin is off by 9%.

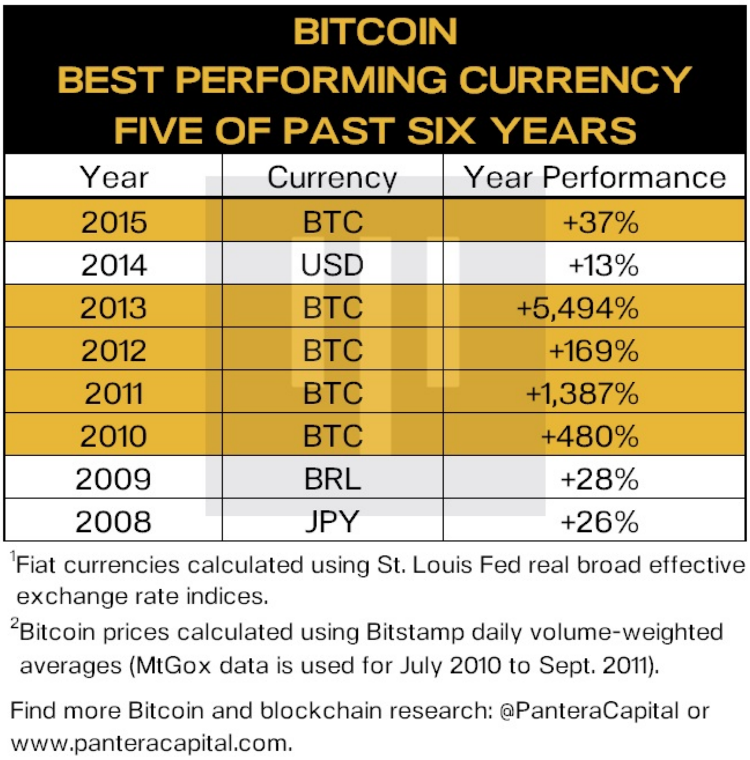


1/27/16	Price Change
Month	-6%
Year-to-Date	-9%
Year-over-Year Return	1.5x

Source: Volume-weighted price on Bitstamp according to www.bitcoincharts.com.

Just Say "No" to "Quantitative Easing"

Bitcoin has been the best performing currency five of the past six years.



BITCOIN
BEST PERFORMING CURRENCY
FIVE OF PAST SIX YEARS

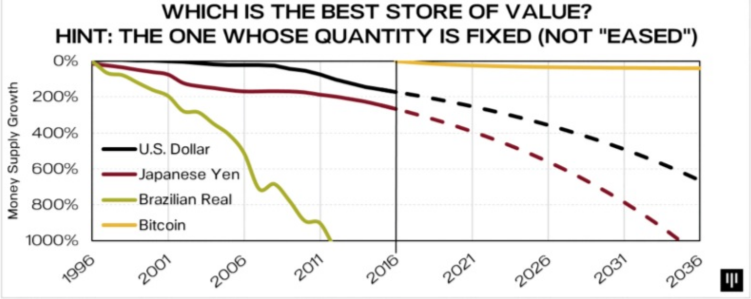
Year	Currency	Year Performance
2015	BTC	+37%
2014	USD	+13%
2013	BTC	+5,494%
2012	BTC	+169%
2011	BTC	+1,387%
2010	BTC	+480%
2009	BRL	+28%
2008	JPY	+26%

[1] Fiat currencies calculated using St. Louis Fed real broad effective exchange rate indices.

[2] Bitcoin prices calculated using Bitstamp daily volume-weighted averages (MtGox data is used for July 2010 to Sept. 2011).

Find more Bitcoin and blockchain research: @PanteraCapital or www.panteracapital.com.

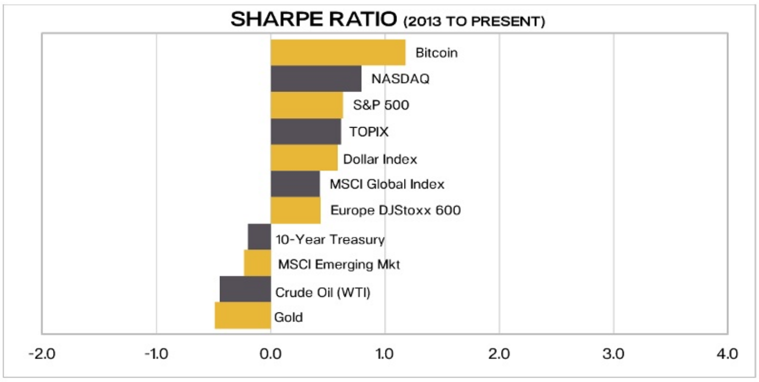
We graphed the money supply change for the best performing currencies in each of the last eight years below. One should instead say "least poorly performing", when referring to quantitatively-eased paper currencies versus hard/fixed assets such as gold, real estate, stocks, and bitcoin.



[1] M1 money supply data of fiat currencies taken from the St. Louis Fed database.
[2] Fiat money supply growth projected using past 20-year compound annual growth rate (CAGR).
[3] The bitcoin forecast is relative to the total bitcoins in circulation on 1/1/2016 (15,031,975 or 72% of total issuable bitcoins).
Find more Bitcoin and blockchain research: @PanteraCapital or www.panteracapital.com.

As more and more countries have embraced "quantitative easing"—explicitly creating a much larger quantity of money—the value of each unit has fallen relative to fixed assets like bitcoin. Bitcoin supply, by design, is fixed, or finite. Supplies of fiat currencies have no such inherent limit. Investors in paper currencies have only one constraint—the supply of paper: one-third of the earth's landmass is covered in trees.

Although bitcoin price volatility is high relative to standard asset classes, this volatility is compensated by the returns. Bitcoin's Sharpe ratio is high relative to these standard asset classes.



Roadshow & Conferences

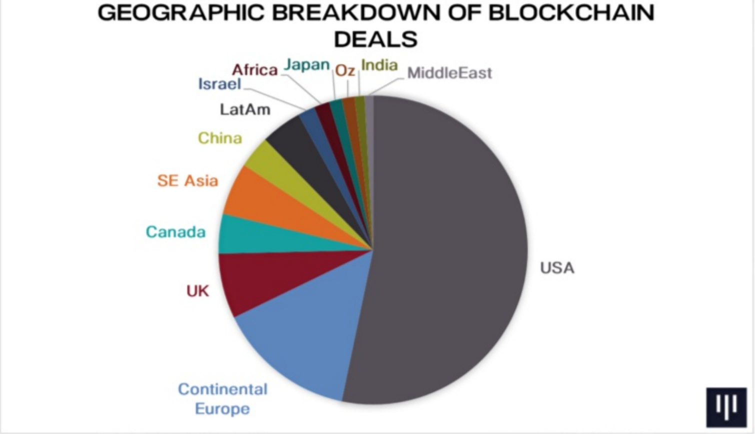
We will be visiting several cities over the next few months to discuss the blockchain ecosystem. Some of our dates include:

- January 28–29, Zurich
- February 1–2, Geneva
- February 9–11, New York City
- February 22–25, Berlin
- March 1–3, Miami
- March 22–25, New York City

If you are interested in a meeting, please contact Pantera's investor relations team at 415–360–3600 or via ir@panteracapital.com.

Geographic Breakdown of Blockchain Deals

Blockchain entrepreneurship is global, just like the technology. We've compiled a geographic breakdown of deals we've documented since 2010, based on our proprietary database.



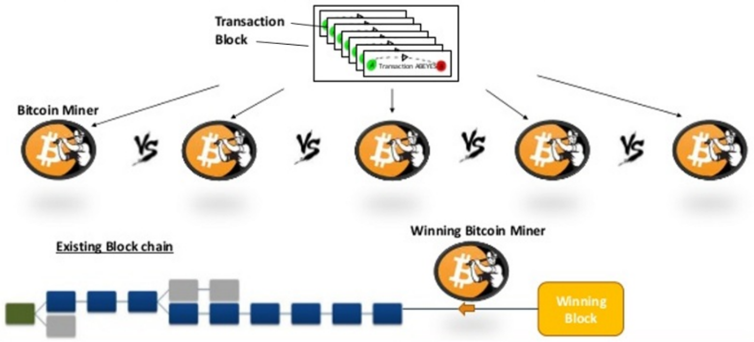
The Governance of Anarchists

The governance of anarchists is more difficult than it sounds.

OK, that's said in jest. But governance challenges are a large part of Bitcoin's current scalability debate.

Technical Background

The bitcoin protocol is powered by Bitcoin miners, who gather transactions into blocks. Miners "publish" blocks to the "official ledger" every 10 minutes on average by solving a computationally difficult puzzle. Miners who solve this puzzle correctly receive a subsidy of freshly minted bitcoins for their work, plus the sum of transaction fees paid by bitcoin users whose transactions are included in the block.



Full nodes on the network check transactions and validate blocks, relaying information about these to other nodes. There are also lightweight nodes which simply listen for transactions which affect them, trusting that blocks from miners are generally OK, thereby reducing the resources required to run them.

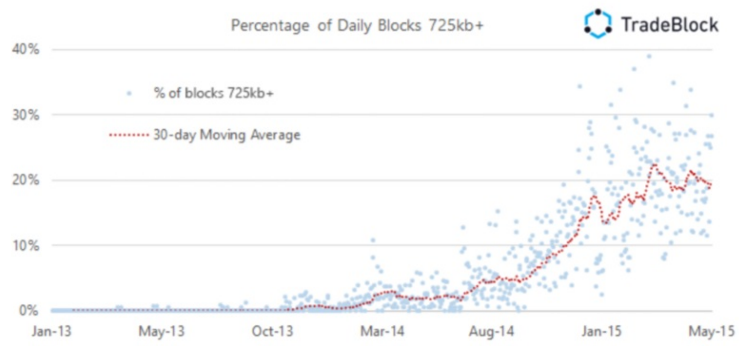
A normal bitcoin transaction is 250 bytes worth of data. There is a hard-coded 1 Megabyte (MB) limit on the transactional data included in blocks (this is the *block size*). This limit was introduced years ago as a means of preventing denial-of-service flooding of the young network.

Why Is There an Issue with Scalability/Block Size?

Bitcoin adoption is increasing and hence the number of transactions is increasing. Hitting the 1 MB block size limit is in sight.

Over the past year, there have been increasing number of full blocks, in some cases causing transaction backlogs for a few hours, meaning longer than usual delays for transactions to clear. More recently, there have been instances of deliberate flooding of the network with normal-fee transactions over the course of several days (any transactions paying less fees than these flooding transactions, which were many at the time, were forced to wait hours for processing).

Data published by blockchain analysis website TradeBlock in June 2015 demonstrated that the average size of blocks had increased from around 125KB to 425KB since 2013.



Up until that point, the daily volume of bitcoin transactions had increased 2.5 times leading to capacity issues on approximately 3% of transactions. An additional complication is the fact that bitcoin miners are not obliged to fill blocks to their maximum. They are able to set custom block size limits below the 1 MB threshold.

Consequences

In the short term, transactional congestion along these lines is far from ideal. Bitcoin is touted partly for its reliably low transaction times. As such, the rate of Bitcoin adoption may slow in proportion to the extent of the network's congestion.

In the longer term, transactional capacity is even more of an issue, insofar as Bitcoin is often imagined as a ubiquitous global payment network, such as VISA, in the future. Bitcoin, at the very least, will need to have a tantamount transactional throughput.

VISA handles on average around 2,000 transactions per second (tps). It has a peak capacity of around 56,000 tps. However, they never actually use more than about a third of this, even during peak shopping periods.

PayPal, in contrast, handles around 10 million transactions per day for an average of 115 tps.

Today, the Bitcoin network is restricted to a sustained rate of 7 tps as per the 1 MB block size. Considering the imminent wave of machine-to-machine transactions that Bitcoin has newly enabled, the ideal number of transactions per second bitcoin would need to be able to accommodate is perhaps two or three orders of magnitude greater than VISA's 56,000 tps.

To accomplish many of Bitcoin's major applications and longer-term visions, it will need to be able to scale far beyond its current state.

In Search of a Solution

Simply increasing the block size from 1 MB seems like easiest solution to implement, as it seemingly only requires changing a single value in the code. In actuality, this could result in unintended ramifications and require other changes of the codebase that may carry unintended ramifications themselves.

A seemingly simple increase like this would result in increasing the power required to run full nodes, which increases the cost of their upkeep. Recall that full nodes are primarily responsible for relaying and validating bitcoin transactions and blocks. As such, they are the bedrock of the network. The more people who use full nodes to process payments, the greater the Bitcoin network is decentralized—decentralization being the technology's most valuable feature, enabling many of its benefits (censorship resistance, fungibility, trustlessness, etc.).

Increasing the cost of full node upkeep means less individuals can afford to host them. Less individual participation means greater concentration of network nodes, resulting in increases of systemic centralization risks. Basically, Bitcoin starts to look more and more like a traditional, centralized shared database, carrying more and more of the same risks of centralized databases while losing many, if not all, of the benefits of a distributed ledger.

To mitigate Bitcoin systemic risk, Bitcoin's development policy is that any proposed changes require a "convincing, broad consensus" to be implemented (specific criteria varies based on the particular changes). This standard is purposefully vague at face to encourage the greatest amount of diligence in arriving to consensus-backed solutions. The issue of Bitcoin's scalability is of sufficient controversy that the protocol's developers are entertaining this greater amount of diligence before moving forward with any particular proposal.

Brief History

Although Bitcoin's scalability has been discussed by the developers throughout the technology's lifetime, only within the past year has the issue gained prominence and spurred controversy.

In short, several initial blog posts and articles bringing the scalability issue forefront generated some fear, uncertainty, and doubt about the adoption rate/future of Bitcoin. These, by and large, exaggerated the trend of an increasing number of transactions filling up blocks (a consequence of Bitcoin's hard-earned success).

Inappropriately, developers of the XT scalability proposal banked on this uncertainty about Bitcoin's scalability to garner support for changes they and a minority of others wanted to see made to Bitcoin, while other major Bitcoin developers maintained that the only true scalability solutions, those which preserve Bitcoin's decentralized nature, were still a ways out. Namely, these solutions include the "Lightning Network" proposal and other 'off-chain' scalability solutions. These best preserve the critical properties of bitcoin (fungibility, trustlessness, etc.).

The mental need to relieve uncertainty and insecurity, in addition to the unchecked promotion of the XT proposal, resulted in some significant XT adoption and unwarranted animosity towards some developers.

Proposals: Core, Classic, XT, and Others

The controversy over Bitcoin's scalability has resulted in several sects forming in support of particular proposals. Each individual sect includes a diversity of ecosystem participants, including: developers maintaining Bitcoin's code, miners, merchants, businesses building on top of Blockchain, casual users, and other interested parties.

Only three proposals have gained any significant traction, but following XT developer Mike Hearn's wholesale exit from the Bitcoin project, now only two major scalability proposals remain viable: Bitcoin Core and Bitcoin Classic.

Bitcoin Core

Bitcoin Core proponents seek to minimize systemic risk to Bitcoin, even if this means Bitcoin businesses must work to tweak the way they interact with Bitcoin, potentially inhibiting the rate of Bitcoin adoption.

However, lower-/no-risk scalability solutions, such as Segregated Witness (a proposal that shrinks the average size of transactions, thus creating more space for transactions), continue to be developed and deployed.

Bitcoin Core's approach to Bitcoin development also puts preserving the protocol's decentralized nature before all else. Part of this decentralization preservation entails maintaining the highest level of backwards compatibility for Bitcoin software—which hard forking (a change to the system which is not backwards compatible; everyone needs to upgrade or things can go wrong) inherently prohibit. Backwards compatible software maximizes the number of full nodes able to participate in the network, preserving/maximizing decentralization of the network.

Read more about Bitcoin Core's development philosophy and scalability roadmap here: https://bitcoincore.org/en/2015/12/23/capacity-increases-faq/.

Other Scalability Proposals

Most, if not all, of the alternative scalability proposals relative to Core (including the now infamous Bitcoin XT) require some sort of hard fork for implementation. A hard fork is a change to the system which is not backwards compatible, effectively splitting the blockchain into at least two incompatible blockchains, which may or may not reconvene into a single blockchain at a future point.

In the case of one alternative scalability proposal, Bitcoin Classic: in theory, implementing an immediate 2MB change would immediately alleviate block congestion but would require a hard fork. Hard forking carries with it certain systemic risks:

- Bitcoins received from before the fork can be spent twice, once on both sides of the fork. This creates a high double-spend risk.
- Bitcoins received after the fork are only guaranteed to be spendable on the side of the fork they were received on. This means some users will have to lose money to restore Bitcoin to a single chain.

In essence, if a hard fork goes bad, it will likely cause large-scale confusion and make Bitcoin incredibly difficult to use until the situation is resolved. There's also a very real chance of total system failure if a hard fork's deployment is not well-coordinated across the entire network.

For the past year, discussion and research about the risk-reward of hard forking the network in its current state has taken place. The technical consensus is that hard forks as prescribed by alternative scalability proposals should only be considered if absolutely necessary. This same consensus of Bitcoin developers has determined that this absolute necessity condition is unmet given the current state of the network. Yet, human short-sightedness and drives to resolve uncertainty continue to fuel support of the quick fixes, which may put the long-term future of the project at major and truly needless risk.

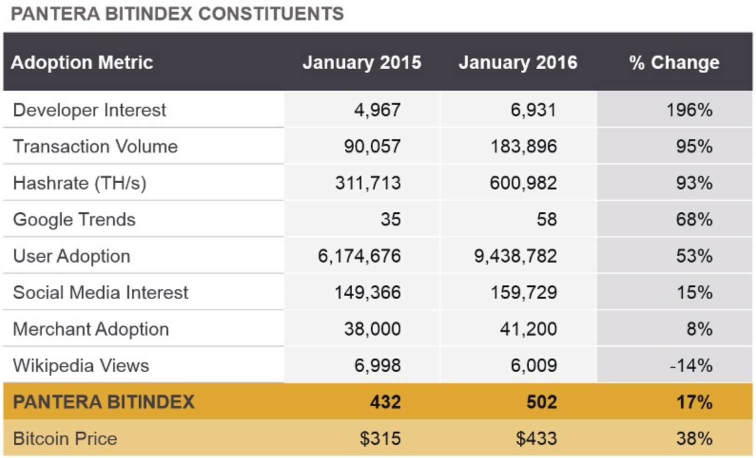
Mike Hearn & "The Resolution of the Bitcoin Project"

Mike Hearn was a long-time Bitcoin developer and one of the chief developers of the XT scalability proposal. Ultimately, his proposal did not gain enough traction in the ecosystem—in fact, before his "Bitcoin is a failure" media campaign, it was facing more and more dissent in the community.

In his Medium post, Mike has some valid points of concern on the need for a scalability solution, but general ecosystem consensus never disputed the need to scale. The denial-of-service attacks that afflicted nodes running the XT solution were no more than an unfortunate coincidence. We think Mike over-exaggerates his statements about Blockstream and the Scaling Bitcoin initiatives.

Most of all, his assertion that "Bitcoin has failed" is incorrect. There is only a need for scalability because of rapid transaction growth and other non-financial use cases of blockchain emerging—a nice problem to have. As evidence of Bitcoin's continuing success, emergent companies building privatized blockchains (“bankchains”) have begun poaching developer talent from the Bitcoin project—Mike, himself, is an example.

Metrics of the ecosystem tell us one thing and one thing only—Bitcoin is thriving:



PANTERA BITINDEX CONSTITUENTS

Adoption Metric	January 2015	January 2016	% Change
Developer Interest	4,967	6,931	196%
Transaction Volume	90,057	183,896	95%
Hashrate (TH/s)	311,713	600,982	93%
Google Trends	35	58	68%
User Adoption	6,174,676	9,438,782	53%
Social Media Interest	149,366	159,729	15%
Merchant Adoption	38,000	41,200	8%
Wikipedia Views	6,998	6,009	-14%
PANTERA BITINDEX	**432**	**502**	**17%**
Bitcoin Price	$315	$433	38%

If the past is indicative of what may happen in the future, we should not be worried. The Internet went through scalability issues of routing and those problems were resolved in time. Whether the scalability route Bitcoin takes ends up being Core, Classic, etc., a governance model for Bitcoin development and a path towards the technology’s future scalability must emerge. Mike’s article may have been the kick in the pants needed to spur some progress, which it more or less has from what we’ve seen on the issue since.

Bitcoin Governance

There is no formal or accurate way to gauge Bitcoin participant consensus. However, it does seem the majority of participants are in favor of Bitcoin’s success, i.e., the technology’s global ubiquity as the Money-over-Internet Protocol. Certainly, this rough consensus splinters about how exactly the technology will scale to achieve this ubiquity.

In lieu of a formal governance model or way of gauging consensus, some members of the community believe that miner hashing power in support of some solution will ultimately dictate which scalability proposal wins. The counterpoint is that the bitcoins miners mine are only as valuable as bitcoin users find them, so miners must take into account what the users want, which may differ.

Others believe that whichever scalability solution the consumer service and blockchain application providers—who facilitate bitcoin accessibility, usefulness, and, hence, value—select will be the determining factor. Again, the counterpoint is that the ecosystem is comprised of many disparate interests that each, in some way, lend to bitcoin its value. These companies could alienate themselves by aggressively pursuing a particular proposal against the grain.

What is clear is that there is no formal model of governance by which major and necessary decisions like those needed about Bitcoin’s scalability can be processed, moved forward, decided on, and ultimately implemented. Any governance or formal consensus-gauging currently possible is simply too loose to advance an agenda reliably.

What we have now: a“pure democracy” a la “voting by selectively updating software”, impassioned, armchair discussion on a myriad of internet forums, and a developer technical consensus, with a critical disconnect between these two latter groups.

A difficult to change Bitcoin is a resilient Bitcoin. No doubt, this loose model of governance has its benefits—namely, it minimizes the systemic risks of centralization and centralized entities pushing agendas that could undermine the value proposition of the network—but it is a double-edged sword. Preventing half-baked changes to the protocol or changes that may corrupt Bitcoin's chief principles and features is valuable, but ensuring the network's viability as it breaches into the mainstream, which can only be done by consensus-backed codebase changes, faces similar difficulty.

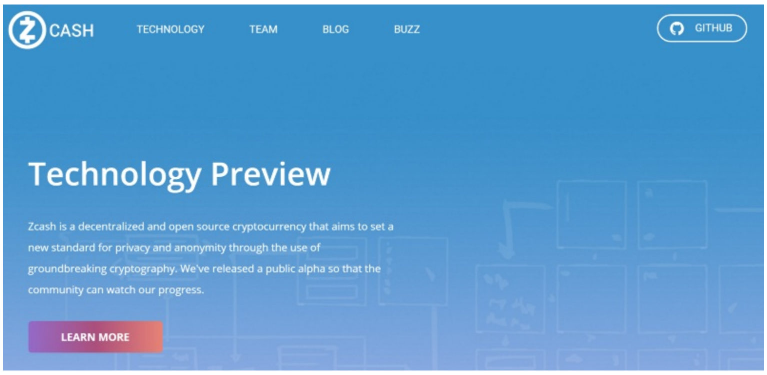
The Bitcoin scalability issue became a controversy because of a lack of leadership in a time of uncertainty. No anarchist wants to be looked to as "governor" but like how many successful nations first began, the well-intentioned must step up to the plate and facilitate the establishment of a scalable Bitcoin—in terms of the tech itself and its development governance. This will form a basis from which we, the ecosystem, can prosper and grow, visions aligned, and without disruption. We've seen great improvement in this from Bitcoin's core developers in recent days post-Hearn.

Ultimately, we will continue to monitor the scalability discussion closely and contribute in what ways we can. We have no doubt Bitcoin will persevere.

Portfolio Developments

Zcash

Our latest portfolio company Zcash is announcing the launch of their public alpha release. Zcash is the company behind the implementation of the Zerocash protocol, a way to provide completely anonymous cryptocurrency transactions. Users may transact between each other directly, without revealing the origin, destination, or amount of the payment.



Technology Preview

Zcash is a decentralized and open source cryptocurrency that aims to set a new standard for privacy and anonymity through the use of groundbreaking cryptography. We've released a public alpha so that the community can watch our progress.

Transactions are verified by zero-knowledge proofs, a mathematical means by which to prove a something with very little information (information, in this case, which does not include much transactional metadata). If Bitcoin is HTTP for money, Zerocash is HTTPS. A user can forgo his or her own privacy and reveal proof that the transaction was his or hers, a la selective disclosure. Transaction metadata in the blockchain is confidential by default but can be revealed under specific circumstances. This allows the best of both worlds, strong privacy and blockchain-caliber transparency.

Zcash published its source code on Github and is now allowing anyone to test out the software. It is a "testnet" and not allowing movement of any actual money yet. The launch, which will enable transactions of real value, is about six months out.

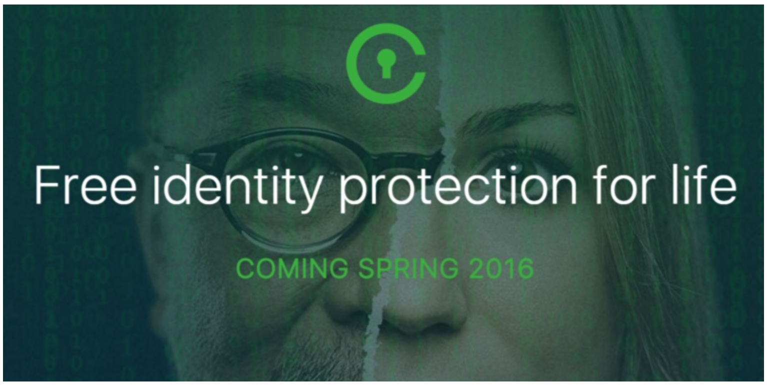
Zooko Wilcox-O'Hearn, a computer security specialist who has designed multiple network protocols that incorporate concepts such as self-contained economies and secure reputation systems, heads the team. The team includes highly talented engineers and scientists, one of whom is Matthew Green, one of the investors of the Zerocash protocol and an expert in applied cryptography and network security. The project has garnered support from many of the blockchain elite such as Gavin

Andresen, Greg Maxwell, Nick Szabo, Adam Back, and Vitalik Buterin.

For more information about Zcash, visit http://z.cash/.

Civic

Pantera recently invested in Civic, a blockchain-based digital identity protection service.



Civic fills a gap between consumers and credit bureaus. After registering with Civic, its product verifies your identity, then “locks it down”. When there is a need to check credit, Civic does not need do a hard check through a credit agency, thus avoiding effects on credit scores. Users can control how they want to be notified upon any identity or credit issues.

It differs from other identity protection products in that it prevents fraud instead of simply alerting you of fraud after-the-fact, potentially avoiding effects on credit score. Utilization of the Blockchain provides:

- An open framework,
- Trustless offline capabilities, and
- Auditing trails (security and prevention of fraud).

For more information about Civic, visit http://civic.com.

Interesting times,

Dan Morehead
Chief Executive Officer
@Dan_Pantera

PANTERA PUBLICATIONS

We tweet Bitcoin news and insights at @PanteraCapital and @Dan_Pantera.

You can subscribe to our publications by visiting www.panteracapital.com/subscribe or by e-mailingir@panteracapital.com:

- *Public Letter:* a monthly letter with our thoughts on significant market and ecosystem-related developments. Also includes our thoughts on blockchain venture capital and news on our portfolio companies for accredited investors.
- *Investor Letter:* Public Letter plus exclusive information for accredited investors.
- *White Papers:* periodic, original blockchain research and academic papers.
- *Portfolio Company Profiles:* inside looks into some of our portfolio

companies, featuring our perspectives and overviews of each company’s industry positioning.

Most of our content is publicly available at www.panteracapital.com/research. However, the SEC mandates that only accredited investors can access certain information. If you are an accredited investor, register here to access restricted content.