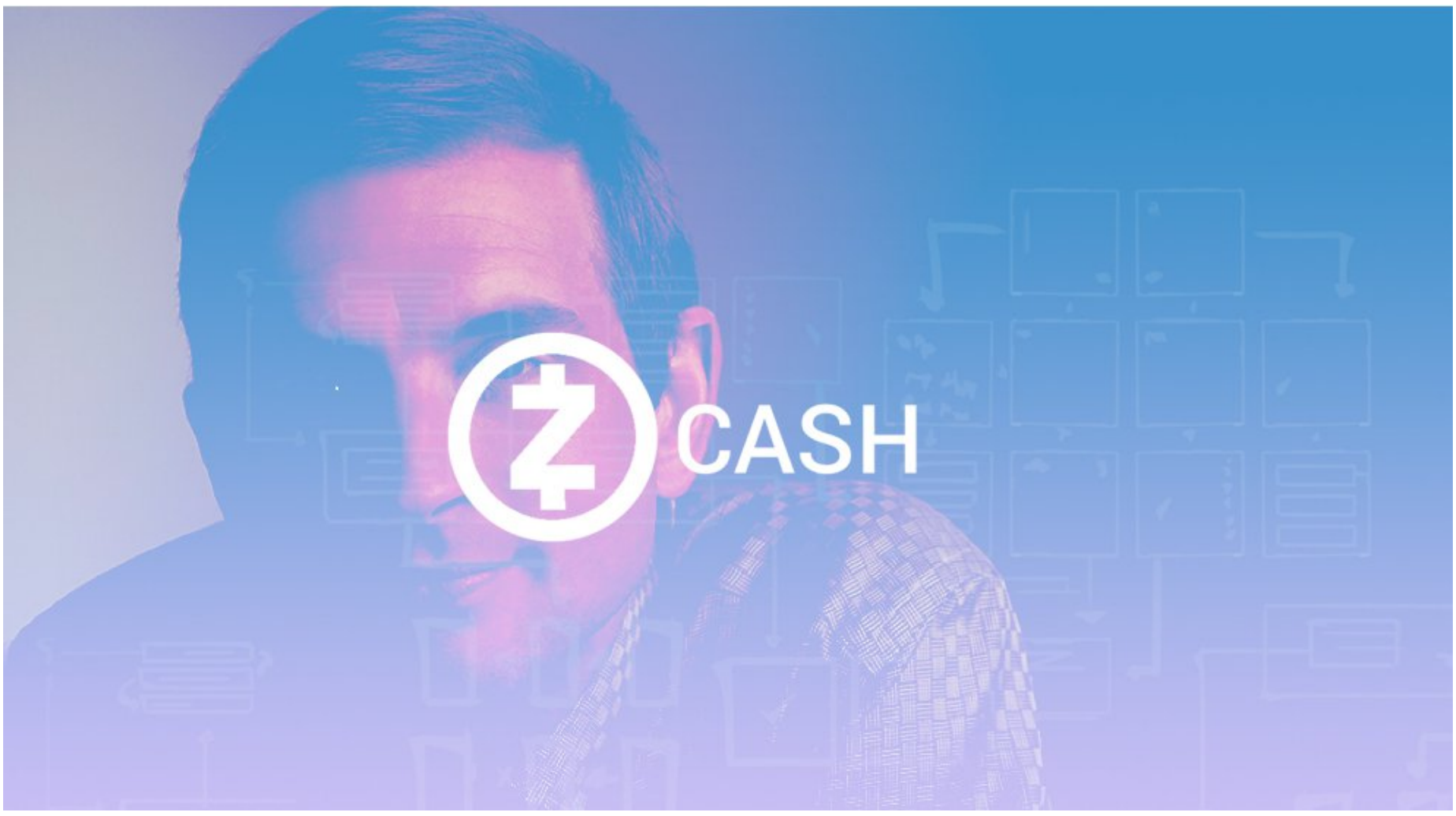
Zcash Creator on the Upcoming Zcash Launch, Privacy and the Unfinished Internet Revolution

Aug 30, 2016 02:46 PM by Giulio Prisco



In January, *Bitcoin Magazine* reported that a public alpha technology preview of Zcash, "a decentralized and open-source cryptocurrency that aims to set a new standard for privacy and anonymity through the use of groundbreaking cryptography," had been released on Github.

Zcash offers total payment confidentiality, while maintaining a decentralized network using a public blockchain. Unlike Bitcoin, Zcash transactions automatically hide the sender, recipient and value of all transactions on the blockchain. Only those with the correct view key can see the contents. Users have complete control and can opt-in to provide others with their view key at their discretion.

Now the Zcash team has announced that the time to release their code and launch the genesis block of the Zcash blockchain is getting close. “When the Zcash genesis block is launched, anyone in the world will be able to mine Zcash and users will be able to send it to anyone in the world with the advantage of full zero-knowledge privacy,” states the announcement. “Our aim in creating the Zcash blockchain is to launch the first open, permissionless financial system with zero-knowledge privacy and best achievable security.”

The launch target date for the Zcash blockchain is set for October 28, 2016. In the meantime, the team is busy with a technical audit, carried out with the help of external audit firms and hackers, to review its code and correct vulnerabilities.

Bitcoin Magazine reached out to Zooko Wilcox, Zcash founder and CEO, to find out more.

Zooko explained that the audit process is ongoing. “The external security consultants we're working with are real pros and we're already glad that we are doing this with them,” he said. “We're diagnosing and (in some cases) fixing issues as we go. We'll publish complete reports about everything that the auditors found and how we responded to each issue. We've already spent tens of thousands of dollars on it and before the process is through, the cost may reach 6 figures. This is one of the many reasons why we needed to have funding to create Zcash.” In a more recent update, Zooko has since confirmed that Zcash has already spent 6 figures on the security audits.

“Frankly, the results so far have left me uneasy about the security of Zcash,” admits Zooko. “The auditors haven't yet found any critical bugs that would allow a really harmful attack like remote theft of Zcash, but they have found bugs which could result in lesser damage (like denial-of-service), and many bugs which *might* be harmless or ‘might’ be vulnerable to exploitation and it's hard to tell which. The number of bugs we've found so far makes me think that there are more bugs left in the code that we haven't yet found. It's possible Zcash will follow the example of Bitcoin, where critical bugs were found and fixed in the software even after there was a live blockchain and real money depending on it. This is one of the reasons why nobody should risk more money on Zcash than they can afford to lose.”

The first version that Zcash is releasing on October 28, 2016 is just a daemon and command-line tool that only runs on Linux. “That means there is no GUI at all, so you can't use it at all if you're not a Linux-wielding power user and it doesn't run at all on Mac or Windows,” explains Zooko.

Zooko hopes that that the makers of wallet software for Bitcoin and Ethereum will add Zcash support to their wallets and that they will do it faster and better than the Zcash team could. “After all, we're not GUI experts!” he told *Bitcoin Magazine*. “Our team has a world-class collection of skills in cryptography, infosec, cryptocurrencies, networking and distributed systems and so on, but GUI design and implementation is something we're lacking. I know that some of those wallet makers are already working on this. So, write to your favorite wallet maker today and ask them to add Zcash support!”

Similarly, the Zcash team doesn’t intend to provide a Zcash exchange for bitcoin and fiat. Some of the existing cryptocurrency exchanges around the world are adding Zcash support, but Zooko isn’t at liberty to disclose which ones yet. “Write to your favorite one and request it,” is Zooko’s advice.

On Mining Zcash

How hard Zcash mining will be and whether it could be (at least initially) feasible for PC users without expensive extra hardware, can't be known at this moment. "Our *intent* was to make Zcash mining feasible on commodity hardware, like your laptop when you aren't using it overnight," explains Zooko. "See this post for our reasons for choosing this Proof-of-Work algorithm. However, it is not yet clear to what degree we've succeeded at that, or whether custom mining implementations and large-scale mining operations will be more cost-efficient."

"One of the external security auditors that we've hired — Solar Designer — is tasked with studying our Proof-of-Work algorithm and writing a report about this. We'll publish his report in full, just like the others.

"I really hope that people run Zcash miners on their laptops and servers anyway, even if it isn't profitable, because it is a public service; it supports the decentralized network that provides a private, censorship-resistant, permissionless blockchain to everyone on the Internet.

"Even if this Proof-of-Work algorithm doesn't close the gap between your commodity laptop and a customized, large-scale mining operation, we've definitely succeeded at 'narrowing' the gap, so it is possible that a lot of volunteers running a miner on their commodity hardware will make it unprofitable to invest in building large-scale Zcash mining operations.

"If this approach doesn't work out and customized and scaled-up mining operations do come to dominate, that isn't the end of the world. Then we'll be in the same boat as Bitcoin and Ethereum, which isn't so bad."

According to Zooko, as Zcash was designing its mining algorithm, he was starting to think that there might need to be some kind of "fundamental trade-off" between decentralization and resistance to 51 percent attacks.

"With a wide variety of amateur miners using the idle resources of their

commodity hardware (like Bitcoin in the early days), the blockchain is more vulnerable to 51% attack, but it is highly decentralized. With a small number of professional miners with specialized mining operations (like Bitcoin today), it is less decentralized, but it is stronger against 51% attack. (Because of the greater scale and because the miners have a capital investment tied to the value of the coin, which incentivizes them to protect the value of the coin.)

“We decided to aim for decentralization instead of aiming for 51%-attack-resistance, but if we miss decentralization and we hit 51%-attack-resistance, that's not too bad!”

Enhancing Privacy in Digital Currency

Zooko explained that he doesn’t consider privacy as a property of a single transaction, but rather as an emergent property from a sequence of transactions among a group of people. “It's sort of an inherently social construct in that way; privacy is something you can only get in groups,” he said. “If you buy some Zcash with bitcoin, everyone will be able to see — on the Bitcoin blockchain — to what Bitcoin address you sent your bitcoin (for example, to the address of an exchange that will allow you to trade bitcoin for Zcash). If you then spend your Zcash on something private (say, paying your employees's salaries, or buying psychiatric treatment) using a Zcash private transaction, nobody will be able to see, just by looking at the Zcash blockchain, what you spent it on.”

Zooko is persuaded that a Zcash economy could emerge in the long term. “The dream is that people all around the world use Zcash and other cryptocurrencies directly, to cooperate and organize with one another in safety and privacy,” he told *Bitcoin Magazine*. “This will give them freedom from corrupt regimes, banks and unstable national currencies.”

Zooko imagines that this is a long-term type of dream that will come true in time. “When it does start happening, it could happen fast, but it might be years or decades before it begins. It might even turn out that the tipping point for this new

way of cooperating and organizing won't be the cash-like functionality that we currently emphasize, but instead, new features like custom tokens, multisig, Distributed Autonomous Organizations and other sorts of 'smart contracts'."

"Eventually I imagine these sorts of technologies will become part of the fabric of our society, like the Internet has become during my lifetime."

Zooko strongly objected to the suggestion of "the inevitable use of Zcash to buy child porn or fund the ISIS." This is what he said:

"I don't even think it is a valid question. It's kind of a 'have you stopped beating your wife?' question. I don't think it is 'inevitable' that child pornographers and ISIS will use Zcash. ISIS is currently working on deploying 8th century technology. If they ever start to use blockchain technology like Bitcoin and Zcash, it will be because it has become part of the fabric of our society, like the Internet, so that bad guys (along with everyone else) can hardly *not* use it."

Continuing the Unfinished Revolution

Zooko added that he remembers when the Internet was new and there was a lot of hand-wringing about how it might be used for crime. "I think that story faded away approximately when the first generation of digital natives started reading news," he said. "Younger people today don't appear to know that there was a time when the Internet was a scary new technology that should be regulated or banned in order to prevent crime."

"We first wanted to push outward the boundaries of human knowledge by scientific exploration," concludes Zooko. "Now these scientific discoveries (by us and many, many others) look like they can radically empower people — individuals, small groups, and also giant organizations like corporations and governments.

“The Internet is an unfinished revolution. I remember what the world was like before the Internet. You didn't talk to people from other countries! National boundaries were communication boundaries. And you couldn't talk to or share information with almost all of the people in your own country, either. You were dependent on a small number of personal acquaintances and information gatekeepers.

“The Internet changed all that, and it changed the world, and it changed all of our lives for the better. The myriad ways that the Internet has remade and improved our lives is impossible to even measure.

“But it is an unfinished revolution, because although it allows you to share information with potentially billions of people, it doesn't provide a way for you to organize with them. You can't cooperate with them to allocate resources. You can't pool your resources with them, you can't help them pay their bills or make sure they get food, such as by hiring them, buying something from them, or donating to them. And they can't do that for you. You can't enter into an enforceable agreement (a contract) with a group of people, unless your group fits into a product from the small number of gatekeepers that control such possibilities.

“What is our role in history? I want to be able to look back and say that we played even a small part in reigniting the unfinished revolution. I want to be able to say we were there, pushing for that great transformation that began to wash away the suffocating mass of inefficiency, corruption, and isolation — the transformation that unlocked the potential of billions of humans who had been trapped behind walls — cooperation boundaries! If we can help that happen, and help it happen *sooner*, before it is too late for so many people, then it will have been worth it, whatever else happens.”

by Giulio Prisco

Giulio Prisco is a writer specialized in science, technology and business. He is persuaded that Bitcoin

and its underlying technology are about to bring disruptive positive changes to finance, business, and society.

KEYWORDS: #bitcoin #internet #people #bugs #magazine

Related Articles:

NOV 05, 2014

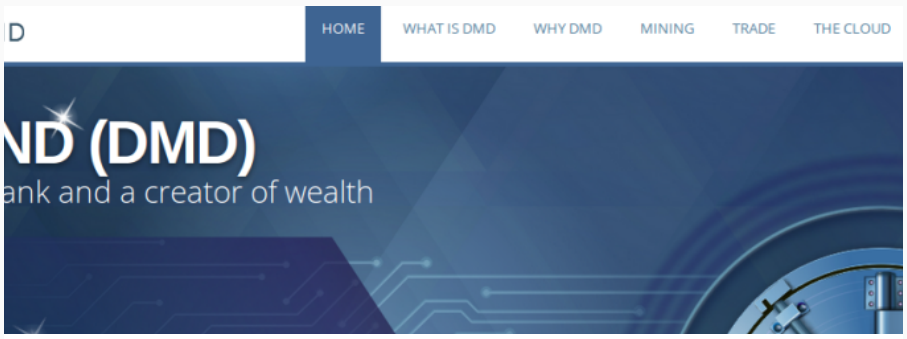
Bitcoin Payment Company BitSend Launches GPS Check-in Cryptocurrency Checkcoin CKC

#ALTCOINS

NOV 11, 2014

Swarm #1: Tom and Gary's Global Party Pandemic

#ALTCOINS



JUN 16, 2015

After Two Years of Development, Bitcoin Alternative Diamond Coin (DMD) Offers 50% Annual Interest

JAN 28, 2016

Ethereum Overtakes Litecoin in Market Cap after Continued Upward Trend

#ALTCOINS

#ALTCOINS