

**Anniversary
Edition**

BUILD

How PwC, Deloitte, EY and KPMG Delve Into Blockchain | 76p. | Life's Code: Blockchain and the Future of Genomics | 104 p. | How Venezuela Became One of the Biggest Markets for Crypto in the World | 60 p. |

ASIA

•BLOCKSHOW EDITION №4•

NOV, 2018

COINTELEGRAPH



BLOCK SHOW

2018 has been a really important year on the BlockShow roadmap. We covered three continents with the famous BlockShow vibe, gathering more than 10 thousand people together. Our community has grown three times since BlockShow Asia 2017, and this is just the beginning!

Being focused on real products instead of empty ICOs, renown experts instead of "no-names", hot topics instead of boring talks, BlockShow produces outstanding quality of content that makes our event as successful as it is.

Welcome to BlockShow Asia 2018, the right place to take stock of this year for the industry to unite as a community and move the technology forward.

Let's make blockchain mature together!



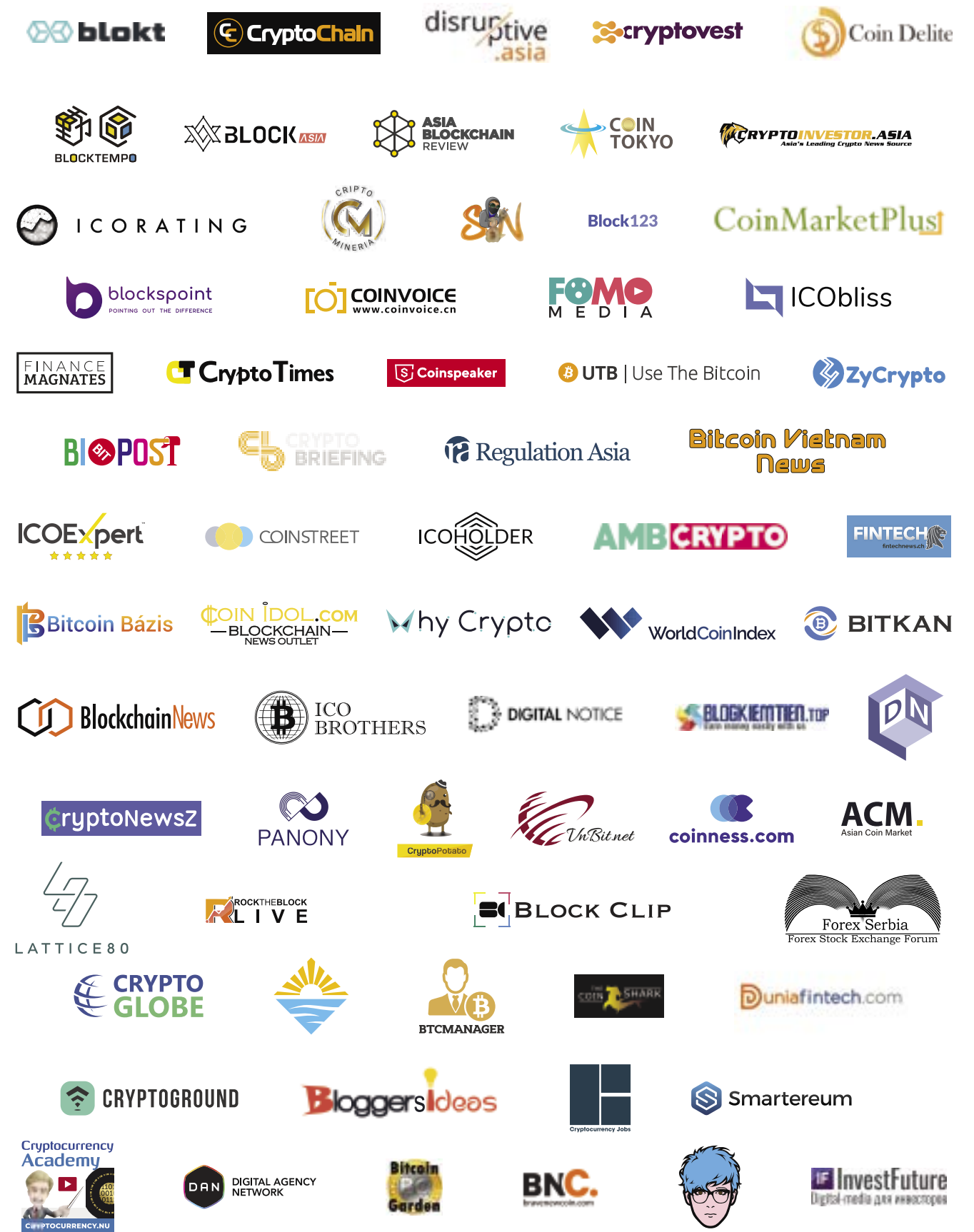
ADDY CREZEE

CEO at BlockShow

THANK YOU



THANK YOU



BLOCKSHOW EDITION



24

EXIT SCAM IN WONDERLAND

BITCONNECT'S
TENTACLES FROM
TEXAS TO GUJARAT

CRIME AND PUNISHMENT

- 12 Crypto Behind Bars: Arrests Making Headlines Across the Globe
- 20 Roger Ver: 'Undercover US Government Agents Go on LocalBitcoins and Arrest People'
- 24 Exit Scam in Wonderland: Bitconnect's Tentacles From Texas to Gujarat
- 36 Crypto Exchange Hacks in Review: Proactive Steps and Expert Advice

MASS ADOPTION

- 44 Important Aspects of Stablecoins: The Difference Between Pegging, Collateralization, and Redeemability
- 48 Untethered: The History of Stablecoin Tether and How It Has Lost Its \$1 Peg
- 54 Nouriel 'Dr. Doom' Roubini: '99 Percent of Cryptocurrencies are Worth Zero'
- 60 How Venezuela Came to Be One of the Biggest Markets for Crypto in the World

BUSINESS

- 70 Which Countries Are Best to Start Blockchain Projects?
- 76 How Big Four Auditors Delve Into Blockchain: PwC, Deloitte, EY and KPMG Approaches Compared
- 84 TOP PEOPLE IN BLOCKCHAIN

CREATIVE CRYPTO MAGAZINE

- 90 The State of Crypto Creativity

FUTURE

- 100 Tom Lee, Speaker at BlockShow Asia: 'Bitcoin is Preparing to Break out'
- 102 Life's Code: Blockchain and the Future of Genomics



BLOCKSHOW

POWERED BY  COINTELEGRAPH

BOUNDLESS PROGRESS

BRINGING BLOCKCHAIN TO THE HEART OF INNOVATION

Returning once more to Singapore, we have come to realize this wonderful city shares so much in common with Blockchain's rapid journey. Here we celebrate how we, as an ecosystem, are removing boundaries as to what is possible, reaping the benefits that arise from Blockchain, and how Singapore supports us as one of the greatest proponents of these changes. It is, by all accounts, one of the most inviting places to do business. As a city-state with highly strategic shipping ports, it exists as a haven for innovation, from its famous Gardens by the Bay project, to its continued sprint to become the world's first truly smart economy. In 2010, Singapore was mentioned as the world's most open economy in the World Economic Forum's Global Enabling Trade Report, standing out as one which focuses on encouraging innovation while empowering its citizens and businesses alike, with low taxes and high quality of life. All this adds to the environment which empowers the Blockchain ideology like no other.



A HUB FOR ADVANCEMENT

There is a youthful vitality to Singapore. Since 1965, it has grown quickly and, as reported in BAV Group's Movers Rankings, continues to do so, making decisions with conviction. As the rest of the world remains tied to its legacy, Singapore is unburdened, free to expand, experiment and progress; this outlook draws not only upon the strategic characteristics of its land, but also its politics: "We see the world as our hinterland, and doing so has allowed us to transcend our physical constraints and avoid being circumscribed by geography," said Singapore's Minister for Trade and Industry, Chan Chun Sing when assuming his post in May (according to The Straits Times report).

For Singapore, it hasn't always been a clear-cut journey. As Asia Nikkei Review recently stated, there have been some growth uncertainties revealed by Monetary Authority of Singapore (MAS), yet in time the city has beaten the odds, steadily growing at the forefront of the world's economy. Much the same, Blockchain is currently experiencing a period of rapid development, recently being reviewed by The Guardian as having the potential to be "one of the most important IT inventions of our age". It represents a whole new ecosystem, one without boundaries; while cryptocurrencies have shown volatility across the board, they have charted a new course in technology.

For Addy Crezee, CEO of BlockShow, this comparison rings true. Returning to Singapore for the second time in a row, he shares his vision of how everything has changed in the past 12 months:

"Singapore is more than just a FinTech center, it is Asia's Blockchain hub. Hundreds of Blockchain companies, offices, and communities are registered here. A year has passed since the first BlockShow Conference in Singapore and, coming back, it's clear that the environment has become much more active! While the increasing number of projects is obvious, there is one more thing worth noting: while ICOs dominated last year, today we witness the growth of product companies. Much remains the same but there are many more experts emerging and businesses have become more stable, serious and mature".



Maturity is the key for the whole BlockShow team. Having been witnessing the rise and cross-industrial spread of the Blockchain technology all over the world, Addy Crezee and his teammates have come to realize that now Blockchain reached its next milestone. That's why our motto for BlockShow Asia 2018 is "Making Blockchain Mature".

Speaking at the ASEAN finance ministers' meeting, Singapore's Financial Minister Heng Swee Keat recently affirmed the city-state's full backing of Blockchain, commenting: "We will support digital innovation in financial science and technology, especially the underlying distributed ledger technology, which can bring us more cost-effective and secure financial transactions", as mentioned in CoinTime's report. This explicit commitment perfectly reflects how Singapore has set its course against the current and propelled towards achieving its beliefs.

RISE TO THE OCCASION

This year has brought a lot of interest and attention to the Blockchain scene, and the spread of ideas is unprecedented. Ever since Nakamoto's solution came to light a decade ago, we have been forced to reimagine many traditional systems after over a century of dependence on centralization. It is a huge opportunity, providing a clean slate which gives new life to the idea of peer-to-peer interaction. To celebrate this supernova of pioneering thought, BlockShow is launching a new segment, EXP20, to promote the most innovative among them, giving companies a chance to convince the jury why their projects can serve as a flagship of this revolution.

EXP20 is a unique showcase of what is happening at the frontline of the Blockchain technology. It brings several of the most exciting startups to stand in front of a board of investors,

to vouch for their ingenuity under the scrutiny of the jury "sharks" who are immune to all the marketing tricks. Not only will it be a thrilling experience for those of you in attendance but we will also be live streaming it across the globe, drawing attention to the highest caliber teams who have turned their expertise to Blockchain to make their impact. The stakes are high — impressing the jury could spell global success, with some of the brightest business minds supporting their vision but, for every team, the risk of leaving empty-handed is equally real.

GROW AS ONE

Growth surrounds us — from this wonderful city to the technology we are here to celebrate. Asia's rapid development is projected to account for 45% of the world's growth by 2020, according to the World Bank, and Singapore has already taken over Silicon Valley as the world's primary incubator for startups, according to the Forbes report.

Where there is opportunity, there are entrepreneurs; it takes a particular kind of person to pursue an untapped market, to take a risk with no promise of return. BlockShow is the same: back in 2016, the team started with a small idea, to promote awareness and growth of Blockchain. Singapore's economy has boomed since its foundation just over 50 years ago. This represents an excellent parallel with BlockShow's explosive development, from what began as one modest conference to the Asia Blockchain Week. Each event draws more of the upper-echelons of global leaders, with attendees including representatives of Deloitte, Wikipedia, Oracle and many more. Last year, the BlockShow audience had grown to over 1,500 attendees — almost three times more than the team's first event attracted. Now, the team are thrilled to be welcoming over 3,000 of you to this event, to hear over 80 speakers (and counting!), from more than 30 countries.

"In 2018, we've already attracted thousands of people to two different parts of the world - Europe and America - and now we're pleased to be wrapping up the year in Asia. Our team has grown threefold; we have united people from different countries, industries, and opinions, and participated in pushing the Blockchain ecosystem forward. This is really important!"

— Addy Crezee, CEO of BlockShow

As Asia Blockchain Week — and the biggest BlockShow ever — are getting closer to their launch, the future of the conference stretches ahead. There can be no way to predict the outcome of what we see here, yet it is certain that there will be even more amazing progress to showcase just around the corner. The weight of Blockchain in the world economy is undeniable; the markets have settled, yet ideas continue to flow. Having consistently attracted some of the most influential speakers from across the sphere, the BlockShow team will continue to stand in parallel with Singapore, as an environment that celebrates innovations.

"We are already planning something really large and elaborate for next year. My team and I are working to switch the whole BlockShow concept from several smaller events into one epic Blockchain-focused occasion — because the market simply won't need a big number of events. Stick around for an extensive update rolling out in 2019 — I guarantee we'll take you by surprise!"

— Addy Crezee, CEO of BlockShow



STATS

COINTELEGRAPH

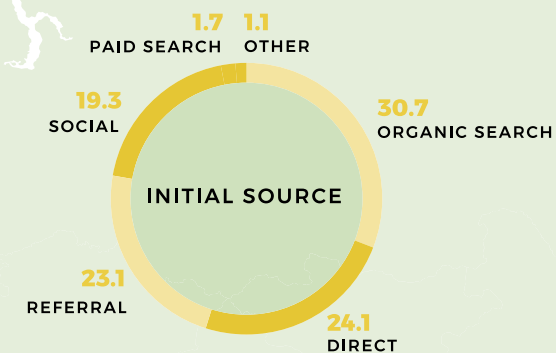
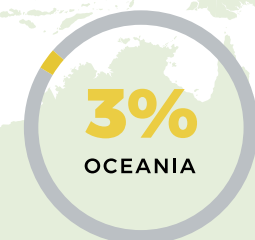
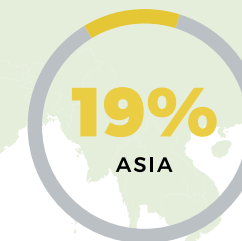
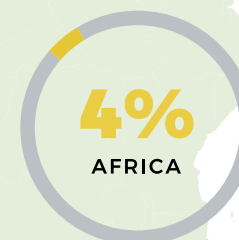
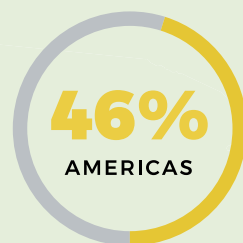
MEDIA GROUP STATS

276 000 000

PAGE VIEWS PER MONTH

67 000 000

UNIQUE VISITORS



10 000 000

UNIQUE VISITORS

60 000 000

PAGEVIEWS PER MONTH

737 k



420 k



98 k



73% of audience with higher education or equivalent

CRYPTO BEHIND BARS: ARRESTS MAKING HEADLINES ACROSS THE GLOBE

From soap actors to former lawmakers, Cointelegraph takes stock of some of the most illustrious arrests of the figures behind crypto's high crimes and misdemeanours this year.



Ethereum developer Piper Merriam opened the Ethereum Improvement Proposal (EIP) #958 on Github on March 30, presenting the idea of a possible hard fork in the Ethereum (ETH) protocol to invalidate ETH ASICs.

Vlad Zamfir, another developer at the Ethereum Foundation, posed the same question on Twitter on March 28. 57 percent of respondents voted yes to the idea of a hard fork.

Both developers' polls emerge amid rumors that the Chinese ASIC manufacturer Bitmain is on the brink of shipping its first Ethash compatible ASIC miners. Ethash is the Proof-of-Work (PoW) hashing algorithm used by Ethereum and a variety of other altcoins.

Gone are the days when shady dealings in crypto were perceived as immune to the clutches of law enforcement.

Illicit crypto proceeds can be shuttled between wallet addresses at the click of a mouse, and their obfuscation behind the multiple strings of numbers and letters of wallet addresses can create a dizzying — if not impenetrable — cryptographic maze for authorities to navigate.

But the criminals themselves present a more concrete target, and as they interface with everything from crafty code to unwieldy hardware to 'traditional' firearms, there has been some success in 2018 in nabbing some of the year's darkest — and most imaginative — offenders.

Foiled supercomputer Bitcoin heist in Russian nuclear no-man's land



In February, Russian security agents scored a coup against a group of nuclear engineers at a top-secret nuclear warhead facility who tried to use one of the country's most powerful supercomputers to mine Bitcoin (BTC).

The engineers worked at the Federal Nuclear Center in the western city of Sarov — formerly one of the Soviet Union's closed-off cities, unmarked on historic maps and shrouded in secrecy.

As one of the Soviet "closed administrative territorial entities," Sarov was then known as Arzamas-16, and was the center of research and production for the first Soviet atomic bomb and hydrogen bomb under Joseph Stalin.

Special permits are still required today for ordinary Russians to visit it.

With such a stellar off-grid history, you'd think the Bitcoin-hungry nuclear engineers might have suspected that connecting the site's supercomputer — a 1 petaflop titan with a capacity for 1,000 trillion calculations per second — to the internet might draw just a little attention.

As soon as the engineers tried to bring it online, the security department was alerted and was able to foil the scientists, who were peremptorily handed over to the Federal Security Service (FSB).

Tatiana Zalesskaya, the head of the press service for the research institute, told the Interfax news agency that the attempt was a “technically hopeless and criminally punishable offense.”

A criminal case was reportedly duly opened against them.

Contentiously, it has been alleged that the radioactive polonium-210 used to kill ex-FSB agent Alexander Litvinenko in London in 2006 was produced in Sarov, which houses a plant that is said to be the “world’s only commercial producer of the substance,” according to evidence presented before a court in the United Kingdom.

Sarov’s rogue scientists are not the only ones to have thought of using former Soviet military spaces for crypto mining. The Ice Rock Mining firm has plans to — legally — set up mining operations in a former Soviet bunker located in a cave in Almaty, Kazakhstan.

**a 1 petaflop titan with
a capacity for 1,000
trillion calculations
per second**

Caught in the headlights: Thai actor “Boom” arrested on set for alleged crypto fraud family affair



This summer, reports emerged tied to the story of a Finnish millionaire allegedly fooled by a Thai crypto investment scam — to the tune of Bitcoin worth 797 million baht (\$24.62 million) at the time.

According to the Thai Crime Suppression Division (CSD), the 22-year-old Finn, identified as Aarni Otava Saarimaa, claimed he had been lured into investing his Bitcoin into several companies, a casino and the gambling-focused crypto token Dragon Coin.

Saarima’s business partner, the Thai businessman Chonnikan Kaeosali, reportedly first approached the CSD in January this year, outlining how the pair had been drawn to purchase shares in three firms — Expay Group, NX Chain Inc. and DNA 2002 Plc — that were purported to be investors in Dragon Coin. He said they had first been approached in connection with the affair by a local Thai group back in June 2017.

The fraudsters are said to have taken their would-be victims around a Macau-based casino where they claimed the gambling-focused token would soon be used. Saarima subsequently transferred his crypto but never saw returns, shareholder papers nor any proof of investment in Dragon Coin.

As the CSD’s investigations unfolded, they identified a group of nine suspects — three of whom were revealed to be a group of siblings from the Jaravijit family. The suspects are said to have swiftly sold the crypto for local fiat currency, dispersing the spoils between various bank accounts.

It was the arrest of one of the siblings this summer — a dapper 27-year-old soap-opera star known as Jiratpisit “Boom” Jaravijit — that first brought the case to public light.

On Aug. 9, Boom was taken into custody on money laundering charges in the midst of filming at the Major Cineplex Ratchayothin in Bangkok’s Chatuchak district. Local media noted it was the day after the star’s birthday.

It was alleged that the actor had colluded with his siblings to launder the swindled money, after investigations revealed they had bought 14 plots of land worth 176 million baht (\$5.44 million).

Boom’s brother, Prinya Jaravijit, is said to have been the ringleader of the scheme, having reportedly received a tip-off from a Thai banker about the wealthy Finn and then setting the heist in motion. Prinya has reportedly fled to South Korea, while Boom’s sister is said to have made contact with the CSD to turn herself in.

The CSD has sought arrest warrants for a further six suspects and frozen a total of 51 different bank accounts in addition to the siblings’ land.

Boom was temporarily released on a 2 million baht (\$61,827) bail bond on the condition that he would not leave the country, having argued that his arrest on set in a public place was ample proof he had not been intending to flee.

Earlier this month, another Jaravijit sibling turned himself in to deny the fraud charges, while police met two further suspects: Prasit Srisuwan, a well-known stock trader, and Chakris Ahmad.

Boom’s parents, Mr. Suwit and Ms. Lertchatkamol, have also been questioned after police traced that 90 million baht (\$2.78 million) had been transferred to their accounts. Both have denied involvement.

Iceland’s Bitcoin miner heist: A high-gliding fugitive and suspect hardware in Tianjin

This year, what has been described as one of Iceland’s “largest criminal cases in history” has seen an outlandish set of twists and turns, leading all the way to the northern Chinese city of Tianjin.

In February, news broke of a series of unprecedented thefts, involving powerful computing equipment that had been stolen in a “highly organized” Bitcoin mining heist. Three burglaries were reported to have taken place in December 2017 and a fourth in January.

The burglars had allegedly swiped 20 million krónur (around \$180,000) worth of equipment — 600 graphics cards, 100 power supplies, 100 motherboards, 100 memory discs and 100 CPU processors — from a house in the municipality of Reykjanesbær.



They had also allegedly broken into data centers across both Reykjanesbær and Borgarbyggð, with a total of 600 computers stolen from both places, worth 200 million krónur (almost \$2 million). The whereabouts of the equipment, including the computers — said to have been used for Bitcoin mining — remained untraceable, even as authorities monitored energy consumption for suspicious increases.

Police are said to have initially arrested eleven suspects — two of which were ordered to remain in custody, after the Icelandic IT firm Advania produced incriminating surveillance footage taken at the data center in Reykjanesbær. The authorities soon recovered most of the stolen equipment, yet the 600 computers remained elusive. Both suspects were reported in local media as being “uncooperative.”

Then, on April 17, one of the detainees escaped at 1 a.m. from his custody in an “open” (low-security) prison, just a week before authorities were due to move forward with an indictment.

The fugitive, Sindri Thor Stefánsson, fled the country on a passport bearing another man’s name, boarding a passenger plane to Sweden that was embarrassingly revealed to have been carrying Iceland’s prime minister.

Stefánsson subsequently released a statement claiming he had been “legally allowed” to travel on the day he boarded the plane to Stockholm, as his custody ruling expired April 16 and a judge had requested 24 hours to consider its renewal. This, according, to him, left a brief interim during which the warrant for his custody was legally invalid.

He vowed to return home “soon,” telling reporters he would be challenging his two-and-a-half-month custody at the European Court of Human Rights.

Days later, he was arrested in central Amsterdam, after a photo published on Instagram with the hashtag #teamsindri allegedly gave him away, according to media outlet Iceland Monitor. Police at the time did not confirm this was the case.

Despite #teamsindri reportedly briefly trending across Icelandic Twitter, the case last month came to a head when a judge charged Stefánsson — alongside six others — with the theft of the 600 computers. While Stefánsson’s charge has been confirmed as theft, it remains unclear what role the other six defendants are charged with as having in the incident.

Just days after Stefánsson’s Amsterdam stint, police in the northern Chinese city of Tianjin seized 600 computers used to mine Bitcoin, after abnormal electricity usage attracted the attention of the local power grid operator. Local media outlets reported the case as being the “largest power theft case in recent years,” but it notably also drew the attention of authorities back in Iceland, who suspected the exact number match of suspect hardware was more than just an uncanny coincidence.

Icelandic police subsequently reached out to Chinese authorities to try to link the two cases, yet no results have been reported since then.



Allegedly incriminating Instagram snap of Stefánsson in Amsterdam: Source: Iceland Monitor

“One of the best out there”: A teenage SIM-swapping crypto hacker with a taste for luxury cars

Last month, Californian police nabbed a hacker who allegedly stole Bitcoin worth over \$1 million via a series of so-called ‘SIM-swapping’ heists — also known as ‘port-out scams.’ The 19-year-old suspect, identified as Xzavvyer Narvaez, is said to have specialized in stealing cell phone numbers and using them to hijack online financial and social media accounts tied to those numbers.

A SIM-swap attack results in the victim suddenly losing all service, with any incoming calls or text messages redirected to the attacker’s device. As many firms use automated messages or phone calls to handle customer authentication, SIM swaps can be a goldmine in deft hands.

Prosecutors allege that Narvaez used his ill-gotten crypto proceeds to purchase luxury goods, including a \$200,000

high-performance McLaren sport car, which were tracked through records obtained from Bitcoin payment provider BitPay.

According to cybercrime blog Krebs on Security, the investigators interviewed several alleged victims of Narvaez, one of whom claimed he was robbed of \$150,000 in crypto after his SIM was hijacked.

Between March and June 2018 alone, Narvaez’s account on crypto exchange Bittrex reportedly saw a flow of a staggering 157 BTC. He subsequently faced charges on four counts of using personal identifying information without authorization; four counts of altering and damaging computer data with intent to defraud or obtain money, or other value; and grand theft of personal property of a value over \$950,000, according to court documents.

VICE’s parallel investigations traced Narvaez’s impressive “credentials” in the SIM-swapping underworld, with one source telling the magazine that he was considered “one of the best [...] out there.” VICE’s source provided screenshots of Narvaez’s former Instagram account, which allegedly featured euphoric photos of his fresh, 2018 snow white McLaren, accompanied by the caption “live fast, die young.”

Narvaez is said to have come under the radar of law enforcement following the arrest of one Joel Ortiz, described as “a gifted 20-year-old college student from Boston” who was charged this July with using SIM swaps to swipe over \$5 million in crypto from 40 different victims.

A redacted “statement of facts” in the case obtained by Krebs revealed that records obtained from Google had traced that a cellular device used by Ortiz to commit SIM swaps had at one point been used to access the Google account identified as Xzavvyer.Narvaez@gmail.com.

“Fake news”: OKEx CEO “detained” for alleged fraud

The most recent high-profile, crypto-related “detention” involves OKEx CEO Star Xu, who was the subject of a host of conflicting media reports — and even one viral dumpling-related anecdote — following his sudden tête-à-tête with Chinese authorities this month.

Xu has robustly hit back at rumors that fraud was the reason for his purported ‘arrest,’ after local media reported that he had faced problems at his hotel from a group of investors in WFEE Coin, a blockchain WiFi sharing project they claimed Xu held shares in.

In an unrelated case this July, Florida police reportedly arrested a 25-year-old, Ricky Joseph Handschumacher, who was accused of being part of a multi-state, cyber-fraud SIM-swapping ring that operated over the course of two years.

The gang of nine — scattered across different states — was initially tracked in February, when a “worried mom” overheard her son talking on the phone impersonating a telecoms firm employee. The group is alleged to have “routinely paid” employees at cell phone companies to assist in their schemes and to even have discussed a plan to hack accounts belonging to the CEO of the high-profile Gemini Trust company — namely those of Bitcoin billionaire Tyler Winklevoss.

Handschumacher himself posted multiple flashy purchases — including a pickup truck, multiple all-terrain vehicles and jet skis — on his public Facebook profile. Subpoenas to Coinbase revealed he had sold 82 BTC through his account, “virtually all” of which were not purchased on the platform.

As law enforcement closed in on this host of spry and unabashed millennial SIM swappers, in August, a U.S. investor filed a \$224 million lawsuit, taking on telecoms giant AT&T. Michael Terpin accused the firm of alleged negligence, claiming that \$24 million in crypto was stolen via a “digital identity theft” of his cell phone account.

His complaint alleged that:

“What AT&T did was like a hotel giving a thief with a fake ID a room key and a key to the room safe to steal jewelry in the safe from the rightful owner.”

The allegedly defrauded victims had reportedly contacted Shanghai police, who “summoned” the CEO to a police station on Sept. 10 to “put [him] through a round of questioning to get to the bottom of the rumors,” as tech news source ZeroHedge wrote at the time.

A photograph of a police report about Xu on local news outlet Sina Technology appeared to confirm that the police had been notified at 5:59 p.m. on Sept. 10.

At the same time, alternative sources in China claimed the investors were in fact traders incensed by system failures

on the OKEx exchange itself. As Bitcoin (BTC) tumbled on Sept. 5, OKEx platform crashes are alleged to have left users unable to close or otherwise salvage their positions, with losses all the more acute in the case of leveraged trades.

Cointelegraph's own Chinese sources have since thrown some degree of light on what had spiralled into a sordid media affair, substantiating suspicions that much of the hearsay was indeed “fake news.”

The sources have emphasized that Xu was the one who approached the police of his own accord. In their account, on Sept. 10, Xu had arrived at the Shanghai office of OK Group to meet with customers and conduct other business affairs. He had also — incidentally — made an appointment at the office to meet with a prospective personal fitness coach.

There, the first troubles with the disgruntled investors are said to have begun — who are thought to have been a mix of OKCoin and WFEE Coin investors. Some ambiguity remains as to their exact identity — and whether they were indeed railing against problems tied to the OKEx exchange or held Xu responsible for the vicissitudes of the WFEE token, or a mix of both.

Having gotten wind of Xu's visit to Shanghai, the aggrieved group is alleged to have been responsible for vandalizing the sign at the city's OK Group office, as appears to be shown in the following photograph:

An alarmed Xu is said to have headed back to his hotel, telling his prospective coach to make her way there as well,

so as to resume their meeting. The investors are alleged to have then followed the woman's tracks, suspecting she would lead them to Xu. There, they are alleged to have knocked on the door of the CEO's room, threatening him.

After four tense hours, Xu is said to have alerted the police. The investors are again alleged to have followed his trail, whereupon Xu called a group of “henchmen” to join him at the police station. At this point, the investors are said to have taken fright and approached the authorities themselves.

In an interview published soon after his release, Xu confirmed he had been held by Shanghai police, seeming to imply he had made the contact on his own initiative:

“In Shanghai, someone reported that I was defrauding. I went to the police station to explain the situation and proved to the police that I did not swindle.”

On Twitter, OKEx COO Cheung also stated that Xu had been encircled by a group in Shanghai, although in his account, the police are said to have arrived to the scene themselves and moved all parties involved to the station. Cheung alleged that:

“While Star was invited to help with the investigation and those people was detained, they raised a fraud complaint against Star. Star stayed to clarify and then left afterward.”



As for the WFEE connection, OK Blockchain Capital (OKBC) — a strategic partner of OKEx and a subsidiary of OK Group — has publicly refuted the allegations that Xu had any shares in the project, tweeting on Sept. 12 that:

“The rumor that OK Group founder Star Xu [is] a shareholder of WFEE is fake. Mr. Xu has no equity relationship with WFEE and its company.”

OKBC has further clarified its own relationship with WFEE, stating that “OKBC is one of the institutional investors of WFEE.” WFEE reportedly “acquired OKBC's and several other capitals' investments [...] when it was still the prime partner of WeShare WiFi — a global leading WiFi sharing company.” The firm added that it had not been notified of subsequent changes to the WFEE white paper, as OKBC “neither participates in” WFEE's operations, nor in its “results.”

OKBC has also pointed to the fact that OKEx had warned its users of the potential risks posed by WFEE in August and included WFEE in their first “Token Delisting/Hiding Guideline [sic].”

So... what of the dumplings?

Amid the flurry of “twisted” media reports, one viral anecdote alleged that the band of investors had brought a hungry — and short-of-cash — Xu some sustenance, namely dumplings, as he underwent questioning at the police station. The story, despite its oddity, appears to have had some traction. Cointelegraph's Chinese sources, for their part, dismissed it out-of-hand as an unthinkable and breathless piece of confected hearsay. 🥟

According to Cointelegraph's sources, no one was witness to Xu's departure from the station, and it remains unclear how long he spent there.

Xu has stated that while it is “normal” for citizens to exercise their right to make such allegations, he has equally fulfilled his “duty” as a citizen by cooperating with the authorities. In terms of his alleged responsibility for system “abnormalities” on the exchange, Xu has responded that:

“I am not a legal person of OKEx, nor am I a shareholder or a director.”

This point was echoed in Cheung's parallel tweets, in which the COO stressed that “Star is the founder of OK Group, [and] although we are good friends, he does not run OKEx.” Cheung has added that he felt “disappointed that the story was twisted before the truth came out.”

Local news outlet Jiemian has meanwhile reported that seven out of a total of 300 investors who claimed to have “suffered heavy losses” on the OKEx exchange have since reached a form of settlement with Xu. Notably, repeated system failures are alleged to have caused a total economic loss of “around 300 million yuan.”

In his post-release interview, Xu stressed that while leveraged trading is a “neutral tool in itself,” it is “not suitable for ordinary investors” as the potential for accelerated net profits and losses requires “professional knowledge” to manage the risks involved.

As Jiemian noted, while OKEx offers investors the opportunity to add as much as 20 times leverage to their contracts, unlike traditional futures trading platforms, the exchange operates without regulatory oversight.



Photo showing the apparent vandalism of OK Group's entrance sign at the Shanghai office



ROGER VER

**‘UNDERCOVER
U.S. GOVERNMENT
AGENTS GO ON
LOCALBITCOINS AND
ARREST PEOPLE’**

***“Because the supply
of Bitcoin was limited,
as more and more people
demanded to start
using it as money,
the price would
have to go up
and go up a lot.”***

Roger Ver is one of the most famous personas in the crypto industry. He calls himself “the first investor into the crypto industry,” being involved with it since 2011. Studying computer science and economics “as a young man” helped him understand the technology behind Bitcoin.

“There was absolutely no doubt in my mind that people were going to start using it as money. And like anything, the price is set by supply and demand.

Roger was seen as the “Bitcoin Jesus,” strongly advocating for the Bitcoin Core philosophy, until November 2017, when he proclaimed that Bitcoin Cash was “the real Bitcoin,” with “bigger market cap, trade volume and user base in the future.”

Why did he do that?

I am on the exact same side I have always been, which is peer-to-peer electronic cash for the world. And sadly, using a bunch of censorship, propaganda, personal attacks and trolling on the internet, the BTC version of Bitcoin has morphed from having the goal [to] be peer-to-peer electronic cash for the world into being a peer-to-peer science project or store-of-value project.

“But I’m someone who wants to enable every individual everywhere on the planet to be able to send or receive money with anyone else instantly, for free and [without the] need [of] permission from anybody else. A peer-to-peer store of value doesn’t enable that, Bitcoin Cash does.

“If you look at it objectively, Bitcoin Cash is the same version of Bitcoin described in the Bitcoin white paper.

“It is the same version of Bitcoin that I got involved with in 2011 and started investing in. I am investing in that because it is the exact same version of Bitcoin that I have been involved in for almost eight years, full time.

“And the thing that everyone is calling Bitcoin in the media today — it has the name ‘Bitcoin’ but it doesn’t have any of the characteristics that made Bitcoin popular to begin with and it doesn’t have most of the entrepreneurs that made Bitcoin popular to begin with.”

CATHERINE ROSS: A LOT OF PEOPLE CONSIDERED YOU THE SO-CALLED BITCOIN JESUS. RIGHT NOW, IT MIGHT LOOK LIKE YOU HAVE CHOSEN ANOTHER PATH. SO HOW WOULD YOU RESPOND TO THAT?

Roger Ver: I think anybody [who] thinks that I’ve chosen another way should stop [doing it] and look at the situation more deeply. I [have] the exact same speech about Bitcoin that I have been giving since 2011. And that speech that I have been giving since 2011 is still completely true about Bitcoin Cash. It is no longer true about the version of Bitcoin that everyone is calling ‘Bitcoin’ [now].

So that means I am promoting the same version of Bitcoin. And the thing that has the ticker symbol ‘BTC,’ it is Bitcoin in [the] name only, its essence is no longer Bitcoin.

But in Roger’s opinion, even Bitcoin Cash is not a perfect version of peer-to-peer cash, and there’s “always room to improve anything in the world.”

Does that mean we might see some other cryptocurrency overtake Bitcoin and Bitcoin Cash?

“Maybe. There is a 1,001 [*2,079, at the press time] different cryptocurrencies out there competing for market share. And at the end of the day, that is a good thing.

“It’s a Darwinian evolution of cryptocurrencies, and at the end of the day, we end up with stronger, more robust, more useful cryptocurrencies for the world to use.

“And Bitcoin — BTC — is not guaranteed to be the winner in the end. Neither is Bitcoin Cash. And if something better comes along, [something] that brings more economic freedom to the world and has the ability to give more people more control of their own finances, I will gladly promote that.



“I am going to promote whatever I think is the best tool to bring more economic freedom to the world.

“Today I think that tool is Bitcoin Cash. But tomorrow, if it [were] something different, I would promote something different.”

I SAW YOUR RECENT TWEET ABOUT REGULATION. THERE ARE A LOT OF JURISDICTIONS THAT TEND TO ACCEPT CRYPTO OR BE VERY FRIENDLY TOWARD BLOCKCHAIN AND CRYPTOCURRENCY ECOSYSTEMS...

RV: New York is not one of them.

CR:DO YOU THINK THE UNITED STATES HAS A FAIR REGULATORY FRAMEWORK IN THE SPACE?

RV: No, it’s not fair. [The government officials] literally have secret undercover government agents going on LocalBitcoins, trying to buy Bitcoins from people. And when they sell them the Bitcoins, they arrest the people and toss them in jail for years. This is madness! And this needs to [be] stopped.

It is madness [that is] happening in the U.S.!

Shame on the U.S. for doing that sort of thing! No civilized country would lock people in jail for years for selling Bitcoin to another person who wants to buy it because they didn’t get permission from some politician.

CR:DO YOU MEAN THAT THE U.S. IS NOT SUITABLE FOR DOING BUSINESS IN CRYPTO?

RV: Man, you are living on the edge [by] doing business in the U.S. — when it comes to cryptocurrency. You are living dangerously to do so.

CR: AND WHERE IS THE MOST FRIENDLY ECOSYSTEM IN THE WORLD [FOR CRYPTO]?

RV: Malta is definitely toward the top of that list — it is not at the very top, [though].

[There are] countries that have the most economic freedom around the world — Singapore, Hong Kong, Switzerland, Malta, Cyprus.

You are living on the edge [by] doing business in the U.S. — when it comes to cryptocurrency.

The U.S. is falling further and further down that list of countries with economic freedom around the world, and it is sad. As someone who is originally from the U.S., it is sad to see that.

CR: YOU’VE BEEN IN THE INDUSTRY FOR ALMOST EIGHT YEARS NOW, WHAT DOES THE FUTURE LOOK LIKE FOR CRYPTO AND BLOCKCHAIN?

RV: The future is more and more adoption, more usage, [and] more integration into the society that we live in around the world. And the regulations can only slow it down, but they can’t stop it. ⚡



EXIT SCAM IN WONDERLAND

BITCONNECT'S TENTACLES FROM TEXAS TO GUJARAT

An American musical prelude

Bitconnect, the now-defunct crypto lending and exchange platform that has been ousted as a ruinous Ponzi scheme, has memorably been compared by the Silver Miller law firm to the fleeting 2011 Broadway musical “Wonderland,” based on the dizzying impossibilities of Alice’s adventures in Lewis Carroll’s celebrated novel.

Silver Miller’s first class action complaint was filed on behalf of six defrauded Bitconnect investors in late January, just weeks after the Texas Securities Commissioner issued an emergency cease-and-desist order against Bitconnect for the selling of unlicensed securities.

The complaint unconventionally opened with the following lyrics:

“Welcome to Wonderland / Where everything you see / I mean from ‘A’ to ‘Z’ / Ain’t what it seems to be. / Welcome to Wonderland / Set phasers up to stun / Turn off the lights when done / Good luck and thanks a ton / Ciao, baby, gotta run!”

In the ensuing months, the federal court for the Southern District of Florida has appointed two lead co-plaintiffs for the class action’s third amended complaint, who will represent all potential plaintiffs in the case. One of the lead plaintiffs, said to be domiciled in Dubai, alleges his out-of-pocket investment loss at Bitconnect totaled 150.28 Bitcoin (BTC), valued at the time at over \$1.6 million.

If the musical allusions have sadly disappeared from the most recent court documents, the number of potential plaintiffs looks set to burgeon. David Silver told Cointelegraph in an interview that the law firm “anticipate[s] thousands of people filing claims if and when this case gets certified and we hopefully recover assets to disperse.”

According to Silver, plaintiffs were duped into taking the Wonderland-like impossibilities of the Bitconnect looking glass for “improbable possibles” and clung to the “sliver of a chance” that the high-yield investment scheme was legit. As cited in Silver Miller court documents, Bitconnect described itself as an “all-in-one” Bitcoin and crypto platform, where:

“It is entirely possible to find the independence we all desire, in a community of like-minded, freedom-loving individuals who, like you, are seeking the possibility of income stability in a very unstable world.”

This purported “income stability” amounted to the promise — regardless of the amount of the initial investment — of a one percent daily return, which Bitconnect alleged would be “generated by its own proprietary trading bot and volatility software.” According to this Wonderland algorithm, a \$1,000 investment stood to return \$50 million within three years of daily compounded interest, as the first Silver Miller complaint noted.

Bitconnect is alleged to have run a global Ponzi investment scheme as of late 2016 that enlisted multi-level affiliate marketers through a referral program that rewarded them for luring investors to purchase Bitconnect native tokens (BCC) on the Bitconnect BCC exchange, using either Bitcoin or fiat currency.

These investors were solicited to participate in the so-called Bitconnect lending program, pitched as an “opportunity” for them to lend their BCCs back to Bitconnect, which the firm would then use its “trading bot” to generate “guaranteed” profits on their behalf, of the aforementioned astronomical proportions.

Those who successfully solicited further investors were promised even higher returns.

It further marketed a Bitconnect staking program, in which investors were given the offer to hold their BCCs in the platform's Bitconnect-QT wallet as yet another means of pocketing hefty profits.

While Silver Miller's action represents the ongoing U.S. private litigation against the scheme — parallel to which federal muscle has also been working — recent developments in India have exposed a murky web of incidents that taint the highest echelons of the country's political class.

The case's corporate defendant, Bitconnect, while hiding behind a shadowy U.K. address, has wreaked havoc through its army of recruiters that range from viral American Youtubers — resulting in Youtube's own implication as a defendant in the Silver Miller class action — to shrewd promoters in the moneyed state of Gujarat, the home turf of India's current prime minister.

At the fulcrum of the Indian chapter is the city of Surat, known for its diamond moguls and textile export tycoons. Cointelegraph spoke to Kashif Raza of the Indian crypto litigation duo 'Crypto Kanoon' to investigate the scandal; an ever-thickening plot of alleged kidnappings and extortions, which has led to the arrest of a former lawmaker from India's ruling party just this week.

.....

“Curiouser and Curiouser!”
Cried Alice

If Wonderland is known for the Queen of Heart's imperious command to paint white roses red, in Modi's post-demonetization of India, Google trends showed a startling spike in one particular search query that hoped for an equally dubious chromatic transformation: “how to convert black money into white money.”

As part of Prime Minister Narendra Modi's attempts to clamp down on tax evasion, in November 2016, he announced the government would be invalidating 500 and 1,000 rupee bills — which accounted for 86 percent of the currency in circulation at the time.

“Black money” is a term used to describe undeclared income that escapes taxes, and Modi gave Indians until Dec. 30, 2016 to deposit their soon-to-be-defunct high-denomination notes, whose sum total was worth a staggering 15 trillion Indian rupee (\$208 billion).

The subsequent panic reportedly saw some 45 billion rupee (\$650 million) flow in to Gujarat's wealthy port city of Surat, to be hidden away in assets including cryptocurrencies, according to an accountant interviewed by Bloomberg last month, who asked to remain anonymous.

This was the fertile soil in which Bitconnect's India chapter took root. And over the course of the next year, as Bitcoin soared to all-time industry highs, so did the BCC token. But in January 2018, after receiving its first warnings from U.S. regulators, Bitconnect shuttered up shop, triggering a crash in the token, which plummeted from its Dec. 29, 2017 high of \$437 to almost zero.



The subsequent crimes and misdemeanours of livid Bitconnect investors are alleged to have taken place in February, although they first came to the public's eye only in April.

Malice in Surat

On Feb. 23, a Surat-based builder by the name of Shailesh Bhatt charged into the office of Gujarat state home minister Pradipsinh Jadeja and claimed that 10 Amreli-district cops had kidnapped and extorted him for 176 BTC, worth 9.45 crore* rupee (around \$1.31 million).

* A crore rupee denotes 10 million rupee and is equal to 100 lakh rupee in the Indian numbering system (1 lakh denotes 100,000 rupee). The band of 10 was alleged to have comprised not only rank-and-file constables, but to have included Superintendent (SP) Jagdish Patel, as well as local Crime Branch Inspector, Anant Patel.

warned him that local authorities — supposedly both the Enforcement Directorate (ED) and the CBI — had him under close watch for his dealings in crypto. After his initial confinement by officer Nair, Bhatt is said to have argued his ransom down to 5 crore rupee (\$693,450), which is said to have been paid via a so-called ‘hawala’ broker.

Then, on Feb. 11, Bhatt claimed that Paladiya called him for a meeting in Gandhinagar, where they were both abducted by a band of cops in official government vehicles near a fuel station and whisked off to Keshav Farm House at Chiloda.

There, Bhatt alleged, "they beat me up inside a room and threatened to kill me in a fake encounter if I did not hand over my Bitcoins":

"Amreli SP Jagdish Patel and Amreli inspector Anant Patel were involved. I was forced to transfer 13 crore rupee [\$1.8 million] in Bitcoins to Paladiya's account."

The plot thickened. For not only were the crème-de-la-crème of state police implicated, but Bhatt accused Paladiya himself of double-crossing him in cahoots with his influential uncle, a former Member of the Legislative Assembly (MLA) for the ruling Bharatiya Janata Party (BJP), Nalin Kotadiya:

"I contacted Paladiya post-demonetization in 2016 to invest my money. He advised me to invest in Bitcoins and knew about my investment."

He further claimed that Kotadiya himself pressured him into paying the ransom. More on Kotadiya later.

By April 9, the Gujarat's elite Criminal Investigation Department (CID) had filed a First Information Report (FIR) against the 10 implicated cops, even though Director General of Police (DGP) CID Ashish Bhatia stated at the time that:

“The FIR has been filed on the basis of evidence found by the team so far. In his application, Shailesh Bhatt had mentioned the transfer of 200 Bitcoins worth 12 crore rupee [\$1.66 million] from the digital wallet of his business partner, Kirit Paladiya. Another 32 crore rupee [\$4.4 million] were allegedly paid for their release from a farmhouse. Later, 78.5 lakh rupee [\$108,872] were allegedly paid to get the Bitcoins back. All these transactions mentioned in the application could not be proven.”

As a builder and “businessman” reportedly known to have a penchant for Bitcoin trading and other “business verticals,” Bhatt is said to have been among those who declared their hidden incomes under the Modi government's Income Declaration Scheme (IDS) after demonetization.

On Feb. 9, he alleged that state Central Bureau of Investigation (CBI) officer Sunil Nair threatened him over the phone and summoned him to the Gandhinagar CBI office, where he was allegedly beaten in a ‘torture room’ and asked to pay 10 crore rupee (\$1.38 million).

Bhatt claimed he had been primed for the call by one of his business aides, Kirit Paladiya, who is alleged to have



Conspiratorial cops

On July 20, the Indian Express covered a chargesheet which the Gujarat CID is said to have filed before a sessions court in Ahmedabad the previous day. The chargesheet outlined how the now-jailed and suspended SP Jagdish Patel had allegedly been in “constant” communication with his junior, Inspector Anant Patel, with the band of cops alleged to have received 1.32 crore rupee (\$1.83 million) in booty from Paladiya following Bhatt’s abduction.

As per the chargesheet, on Feb. 16, Anant is alleged to have given 9,087,575 rupee (\$125,797) to SP Jagdish, who sent this money to his relative, one Bhavesh Jagdish Patel, a resident of Thaltej, Ahmedabad. The money is said to have been delivered by Anant and two local crime branch (LCB) cops in government vehicles. At Bhavesh’s house, the money was allegedly counted, with 1 lakh rupee (\$1,387) deemed to be “missing”:

“The money was counted again and 10,000 rupee [\$139] was found to be missing. Bhavesh then called Jagdish and told him about it, to which Jagdish said, ‘No problem. You keep the bag that has 90 lakh rupee [\$124,821].”



A wolf in sheep’s clothing?

In parallel to emerging details of this quagmire of police corruption, the now-infamous

extortion case made an about-turn when Bhatt himself was accused of an earlier — and even more explosive — extortion of a staggering 1.55 billion rupee (\$215 million) worth of crypto and cash at gunpoint — including around 2,400 BTC — from two colleagues of a local Bitconnect promoter, Satish Kumbhani.

As CID’s Bhatia has reportedly stated, Kumbhani of Surat “floated” a company called Bitconnect and “lured people like Bhatt to invest for huge returns. Bhatt ended up investing 2 crore rupee (\$277,380) in BitConnect [token]. However, its promoters shut shop in January 2018 and went underground.”

Then, when word broke of Bhatt’s Feb. 23 complaint at the Home Ministry, Jagdish is accused of contacting Anant and organizing for the booty to be moved from Bhavesh’s house to a friend, one Hardrik Mahida.

“On March 6, Jagdish Patel was in Ahmedabad. At that time, accused Anant Patel was trying to cover up his crime and also demanding money for legal expenses for himself and other accused policemen. The then Amreli district Superintendent of Police gave 40 lakh rupee (\$55,476) to Anant Patel to cover up his role and also policemen of his department [...] [Jagdish handed over] 40 lakh rupee to Anant Patel and his staff Vijay Vadher, Sanjay Padmani and Pratap Der on April 6 at Pakwan cross roads, Ahmedabad. Jagdish’s presence has been captured in the CCTV footage.”

The chargesheet, citing further CCTV footage as evidence, then accused the suspended SP of approaching Bhatt’s friend Dharmendrasinh Gohil’s house at Pachchai village in Bhavnagar to — euphemistically — “reach a compromise.”

After this ploy allegedly failed, Jagish is said to have thrown “mobile instruments and SIM cards into the Sabarmati river” — the very devices that would have incriminated his scheming with the co-accused Anant and Ketan Patel.

In a press note, the CID is reported to have stated that Bhatt’s misdemeanours were uncovered when its sleuths went on the trail of how he had himself acquired the hefty sum of Bitcoin of which he claimed to have been robbed.

The sleuths uncovered two earlier kidnappings — this time allegedly masterminded by Bhatt himself — involving nine accomplices, which included the builder’s nephew Nikunj Bhatt.

In apparent vengeance against those responsible for the Bitconnect heist, Bhatt and nine others are said to have posed as local tax officers and kidnapped a small-time Bitconnect employee named Piyush Savaliya on Jan. 30. Savaliya is said to have been held hostage at gunpoint, also at a shadowy farmhouse — so apparently beloved by Gujarat’s criminal underworld — but this time one located in Surat.

When Savaliya claimed he was unable to avail the men of their desired crypto, according to Bhatia:

“[The next day, Feb. 1], Bhatt’s men kidnapped Dhaval Mavani at gunpoint [...] [who was] also attached with the bankrupt

firm BitConnect. Bhatt’s accomplices forced Mavani to transfer 2,256 Bitcoins, worth 131 crore rupee [\$18.2 million] into their account. The builder and his accomplices also transferred another 166 Bitcoins, worth 9.64 crore rupee [\$1.34 million] into their account.”

The CID’s press release reportedly added that Bhatt and his cohorts extorted a further 14.50 crore rupee (\$2.01 million) in cash, which was secured through a local ‘angadia’ — an informal network of Gujarati couriers.

Bhatt is reported to have distributed the spoils among his nine accomplices, keeping around 700 BTC for himself and allegedly asking his tech-savvy nephew, Nikunj, to make the transactions.

When the sleuths tracked the beleaguered Savaliya down, he claimed Bhatt had paid him 34.50 lakh rupee (\$47,848) to keep silent and to release a “false” statement denying the



Conspiracy, take two — this time, a failed one

Another chargesheet floating around, which was also filed

by the Gujarat CID in July, alleges that when the accused policeman themselves got wind of Bhatt’s earlier crimes, they themselves met on Feb. 15 at a hotel in Ankleshwar in Surat to conspire to silence him and prevent him from lodging his complaint at the Home Ministry. They are then said to have redoubled their efforts Feb. 21, when Inspector Patel, lawyer Ketan Patel, his brother Jatin Patel, Kirit Paladiya and an “independent witness” Vishal Sakadsariya are said to have met at yet another hotel to further scheme about ways in which to prevent Bhatt from coming forward.



“Icing on the cake”

In Cointelegraph’s correspondence with Raza Kashif, he sketched out the political

backdrop of the unfolding crypto scandal, with its tarnished cops, victims-alleged-perpetrators and even former BJP lawmakers accused of being behind-the-scenes puppeteers:

kidnappings. Mavani, for his part, was reportedly warned never to be sighted in Gujarat again: Police sources claim he has left the country.

As the allegations against Bhatt’s shady past surfaced, the builder himself absconded. Speaking to local media outlet The Quint, the builder’s lawyer said:

“The charges levied against him are false and part of a larger conspiracy. There is no Savaliya or Mavani; in fact, Mavani was not even in India when the alleged offence transpired. The police [are] fabricating the whole story about Savaliya getting 34 lakh rupee (\$47,066) for staying mum.”

Nonetheless, both Nikunj Bhatt and a further alleged accomplice, Dilip Kanani, were arrested in May on charges of kidnapping and extortion, with CID reportedly recovering 152 Bitcoins worth 8.5 crore rupee (\$1.18 million) from the duo.

The chargesheet alleges that Ketan and Anant Patel attempted to trace the vanished Mavani — even sending four fellow cops to pursue him all the way to Mumbai — in what emerged as being a false trail.

Mavani’s whereabouts are still unknown.

At this point, you’d be forgiven for losing track of the countless names and double-crossed co-conspirators allegedly embroiled in the case. As Times of India jocularly reported, the CID detectives faced a similar headache and have reportedly created monikers for the different “protagonists” of the many-tentacled incident based on the “unique passwords of their Bitcoin e-wallets or phones”:

“We identify Ketan Patel as “Loq,” and Shailesh Bhatt as “Choco,” a CID official is reported to have confessed.

“As we know, General elections are due to be held in India in April or May 2019 to constitute the 17th Lok Sabha. The opposition parties in India are leaving no stone unturned to corner BJP.

“The Indian National Congress (INC, often called Congress party) has been trying to prove that ‘Demonetization’ was a tactical blunder and [the] Bhartiya Janta Party (BJP) took this step to make their own black money into white money.

“The Bitconnect scam proved to be the icing on the cake for the opposition parties, as the name of the main protagonists is a former BJP MLA and he has been arrested by the Ahmedabad crime branch recently.”

Kashif referred to the arrest of the aforementioned ex-Member for the Legislative Assembly for the BJP, Nalin Kotadiya, the uncle of Bhatt’s allegedly duplicitous former aide, Kirit Paladiya.

Kotadiya was remanded in police custody just on Sept. 10.

Let’s backtrack to the immediate aftermath, when Kotadiya was first tainted by Bhatt’s brush.

In late April, after the allegations of extortion and conspiracy, with the disgraced band of rogue Amreli cops against him had surfaced, Kotadiya at first attempted to hit back, dismissing the claims as misinformation, with the bizarre defense that:

“I am a man of public life. I meet people and talk to them on the phone. It does not mean I am involved in criminal acts with the people I meet or talk to on the phone.”

Kotadiya more pointedly drew attention to the fact that the alleged BTC transfers remained to be proven, quipping that “if the Bitcoins were not transferred, the question that arises is where the money came from.” He claimed that SP Jagdish Patel was being “pressured” to implicate him in the case and even more explosively that:

“Bhatt accepted that he was investing money from people affiliated with political parties. To protect them, attempts are being made to fix me in the case.”

He then circulated a WhatsApp video, reposted on Youtube in late April, in which, attired in pink, he claimed he had duly informed authorities about the Bitcoin heist and attributed the full blame for the extortion scandal and conspiracy to Bhatt.

As one alleged conspiratorial mastermind accused another of the selfsame, Kotadiya moreover threatened to leak evidence that would implicate even more local politicians in the scandal.

By mid-May, despite Kotadiya’s protestations, his failure to turn himself in led a local Ahmedabad court to issue an arrest warrant against him. The CID’s plea reportedly alleged that the accused former-BJP figure had evaded the unit’s clutches:

“There is material evidence substantiating the allegation of [crimes] against Kotadiya. It has also emerged from the record that though summons were issued twice, Kotadiya, despite promising cooperation, did not present himself before the investigating agency.”

The CID plea alleged that in early May, Kotadiya had sent the agency a fax saying he would appear before them on May 12, but then failed to do so. On May 7, he was also reported to have released a press statement claiming he was being “framed by the conspirators.” But CID’s plea is said to have pressed on, stating that:

“We have concrete evidence against Kotadiya. He is a politically influential person. His evading arrest could be could be an attempt to delay the investigation and create hindrances to it.”

Meanwhile, May 4 saw the arrest of Kirit Paldiya, Bhatt’s accused former aide and Kotadiya’s nephew. His interrogation is reported to have revealed that Paladiya — in complicity with Kotadiya, the Amreli police SP and inspector, and lawyer Ketan Patel and his brother — had plotted to apportion the extorted Bitcoin spoils between them, allegedly reserving 15 percent to be split between Kotadiya, the lawyer, and his brother, and 15 percent to be split between the police officers.

Kotadiya himself is alleged to have received 66 lakh rupee (\$91,535) — of which Paladiya is said to have given 35 lakh rupee (\$48,540) in total to two family members through a Surat-based angadia firm. 25 lakh rupee (\$34,672) of this was said to have been recovered by CID officials at the time.

As Kotadiya himself remained underground, by mid-June, an Ahmedabad sessions judge declared Kotadiya a "proclaimed offender" under section 82 of the Code of Criminal Procedure (CrPC) in response to an application by the CID and asked him to appear before the court within 30 days. Scathing news reports at the time pointed to Kotadiya’s political background, as well as characterizing him as a “leader” of the Patidar caste, a socio-economically prominent lineage within Gujarati society.

Nabbed “fast asleep” on a construction site

Just last week, Kotadiya’s time was finally up.

On Sept. 10, the Times of India reported that the ex-MLA for the BJP had been nabbed after four months in hiding. He was reportedly found “fast asleep” on the second floor of the under-construction railway quarters in Amalner, in Dhule, Maharashtra.

He is alleged to have been hiding out there with laborers for the past two months, according to Deepan Bhadrán, deputy commissioner of police for the Ahmedabad crime branch. The Times further claims that Kotadiya had eschewed using mobile phones to make sure he was off-grid, using relatives’ and other borrowed cars to travel between locations. A crime branch source is quoted as saying:

“When we [eventually] found him, he was sleeping on a mattress and there was just an earthen pot of water in the room.”

An Amreli-born contractor at the Amalner railway quarters is said to have first noticed him, giving the golden tip-off.

.....



Opposition intrigues

As Raza Kashif noted, the BJP’s embroilment has been a political gold mine for the opposition party, the Indian National Congress (INC).

In early July, senior congressional leader Shaktisinh Gohil alleged that the “mega Bitcoin scam” was being used to cover-up shifty conversions of black into white money by the members of the majority BJP party.

As Kashif wrote in his correspondence with Cointelegraph, Gohil claimed that the Gujarat scam had emerged as involving “more than \$726 million (5,000 crore rupee) [...] with some reports pegging the figure at \$12.7 billion (88,000 crore rupee).”

Gohil used the case for all the political mileage he could muster, demanding a Supreme Court-monitored investigation into the matter:

“The finger of suspicion of this massive scam of illegal cryptocurrency directly points to several top Bharatiya Janata Party leaders

and a mastermind — an absconding BJP leader and former MLA Nalin Kotadiya.”

As the Deccan Herald put it, Gohil alleged that “extortion of crypto using government authorities at the behest of top BJP leaders in Gujarat has become a norm,” claiming that “political pressure” had muscled in on the local CID to hush the case up and launch the subsequent complaint against the Surat builder:

“Instead of [Bhatt] being the complainant in the first case, the CID at the behest of MoS Home made the police the complainant [...] Who are the top BJP leaders against whom Kotadiya has damning evidence? We demand an impartial Supreme Court-monitored judicial investigation.”

Gohil’s allegations further claimed the Bitcoin had been widely used to carry out “illegal transactions” post-demonetization, something he implied would not have surfaced were it not for the scandal first unearthed by Mr. Bhatt.

As Kashif outlined in his correspondence, Gohil drew upon the full extent of the alleged Bitconnect scandal — which extends well beyond the web of alleged extortions and kidnappings we have mostly been tracing so far:

“[News of the Bitconnect scam] transmitted a shockwave in the country at a time when the nation was already trying to recover from India’s biggest bank fraud case of \$2 billion (over 13,000 crore rupee), a fraud [that had been] planned and executed by [diamantaire] Nirav Modi and his uncle Mehul Choksi. The Bitconnect fraud is six times bigger than the [aforementioned] bank fraud, which took all the headlines in the Indian media.”

As the Times of India has reported, tracing the full extent of Bitconnect’s tentacles in India brings a unique hurdle, in that many of its investors are accused of laundering their “black” cash into the scam post-demonetization.

Even after Bitconnect scrambled late January the CID’s Bhatia told the Times that the bureau has received few complaints, allegedly because so much black money is thought to have been siphoned into the the scheme.

While the Times itself considers that the Bitconnect swindle may indeed have “siphoned off more money than Nirav [Modi’s banking fraud],” Bhatia stressed:

“So far, we have received complaints for cheating worth 1.14 crore rupee (\$158,106).”



Ciao baby, gotta run!

So what of the Bitconnect promoters themselves? Has the protective cloak of black cash and the newsworthy distractions of lurid

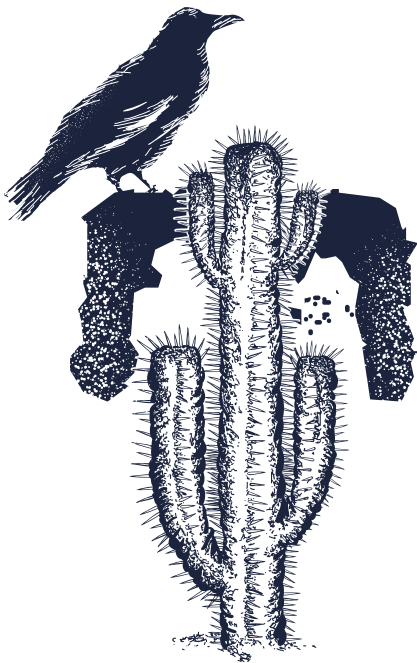
kidnappings and extortions really allowed them to get away scot-free?

Last month, police finally arrested a suspect, Divyesh Darji, who is said to have held “held seminars [and] events in India and other countries” promoting the Wonderland promises of Bitconnect. Darji, a resident of Surat, had reportedly already been issued with a look-out circular and was arrested on Aug. 18 in the Delhi airport, after a tip-off from local immigration services.

In his interview with Cointelegraph, Raza Kashif described Darji as a local and respected “influencer,” who enjoyed a number of high-profile and esteemed local connections, which he presumably made excellent use of to propagate the Bitconnect affair.

Darji’s still-active LinkedIn profile claims — in somewhat shrill ALL CAPS — that:

“I AM HAVING DEGREE OF M.COM. LL.B., B.ED., N.D. & HAD EXPERIENCE OF TEACHING +2 STUDENT & COLLEGE FOR 25 YEARS. I AM GOOD NET WORKER AND HAVING GOOD LEADERSHIP QUALITIES. RIGHT NOW I AM HAVING ENOUGH



KNOWLEDGE ABOUT CRYPTO CURRENCY AND BITCOIN AND MAKING WEALTH THROUGH THAT [sic].”

A recent Times article cites CID crime officials as alleging that Darji enjoyed “10 percent commission” on investments he brought in:

“He was fluent in English and ran several social welfare programs. He had a big following and Khumbani hence roped him in [...] Darji had brought investments of 4,100 crore rupee [around \$567.6 million], while the total amount invested in Bitconnect could be around 41,000 crore rupee [around \$5.6 billion].”

As for Satish Kumbhani, he is reported to still be absconding. A senior CID crime officer is quoted by the Times as saying that the unit has “begun the process of getting a warrant issued against [him] and will then press for a red-corner notice (RCN)” to trace him:

“Kumbhani was tracked down to South Korea some time ago, but by the time we could react, he had flown back to Dubai. He supposedly handled the worldwide operations of the company and may have possession of a large amount of money in Bitcoins, which belongs to investors.”

Meanwhile, the U.S. states of Illinois and Arizona implored the CID last week to seize the property of the Gujarat Bitconnect promoters, the outcome of which remains to be seen.

.....



The aftermath?

As Raza shrewdly noted, the INC has to date called four press conferences in response to the Bitconnect-related scandals, capitalizing

on its potential to tarnish the BJP ahead of the forthcoming elections. In the wake of multiple high-profile scandals, he added that:

“Back-to-back in the last five months, the magnitude of [a string of] frauds has come to 1 lakh crores rupee [around \$13.87 billion]. For a developing country like India

to face scams of this magnitude, [it] has shaken people’s confidence in the system.”

Raza noted that news of the Bitconnect-related extortions broke after the Reserve Bank of India’s (RBI) notorious circular directing all banks to extract themselves from relationships with crypto exchanges and traders had already been issued on April 5.

But Raza nonetheless stressed:

“News like this makes life tougher for the average crypto trader in India [...] the opposition party [INC] is opposing cryptocurrency now, because they have said that the ruling party used crypto to make their black money white. Now, if they come into power, they will not positively regulate crypto, because if the current party [BJP] goes into opposition, they will turn around and say that ‘once upon a time, you used to trash us for our involvement in crypto, and now you yourselves are regulating it!’ So this is not a good sign actually.”

In his correspondence, he added that as they bide their time until the next date of hearings devoted to the RBI restrictions, India’s crypto exchanges and traders have found their “messiah” in the “form of the p2p model”:

“Timely regulation will help curb these scams to mushroom in India. The main protagonists, in this case, took the advantage of ‘fear’ and ‘negativity’ surrounding this industry in India. Possession of ‘Bitcoin’ is not illegal in India and most of the exchanges in India are self-regulated and follow stricter norms on KYC than banks.

“There is a huge challenge in India when you approach a police station to file a complaint against a Bitcoin fraud, as there is a high probability that you might be sent back without [them] even listening to your complaint. The fraudsters know this fact and they take maximum advantage of looting the general public in the name of high-return promises.”

As of press time, Shailesh’s Bhatt’s whereabouts remain unknown. With Kotadiya still remanded in custody, the case is poised to send further shockwaves through the crypto community and to provide further grist to the mill of India’s opposition politicians.



Coda

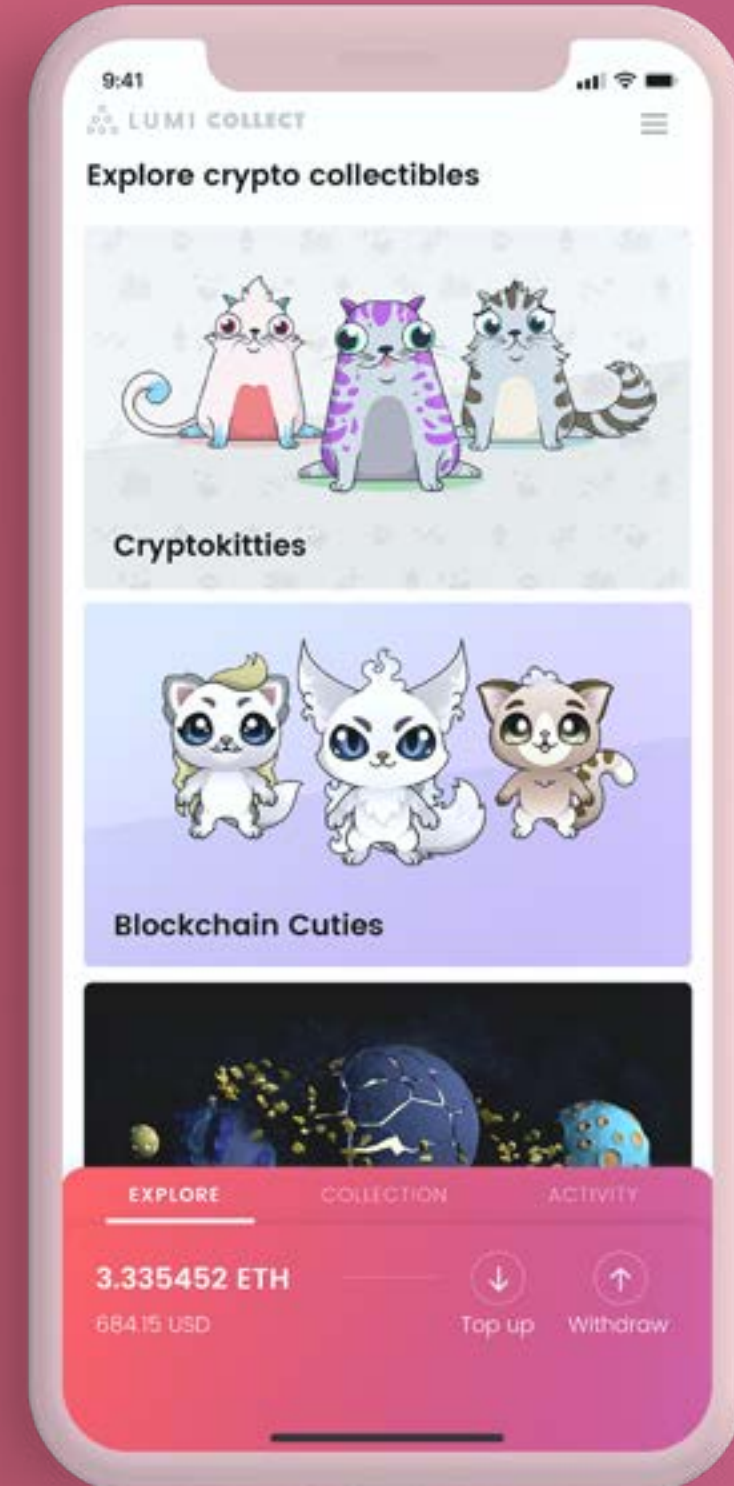
As the final scores in Bitconnect’s Gujarat chapter remain to be settled, globally, the scandal has meanwhile

bequeathed to us one of the most jarring memes in industry history. It started from a viral video of one Carlos Matos, a Bitconnect recruiter born in the Bronx who “serenaded” the audience at the platform’s first annual ceremony in back in 2017, in Pattay, Thailand. ⚡





Crypto wallet



Collectibles wallet



CRYPTO EXCHANGE HACKS IN REVIEW:

PROACTIVE STEPS & EXPERT ADVICE

Has the cryptocurrency exchange which you typically trade on already been hacked? If not yet, this is highly possible. Centralized exchanges, which Vitalik Buterin wished would “burn in hell,” can manipulate users' funds and face regular attacks, while decentralized ones seem to have not yet found a balanced compromise between security and usability. At the same time, the experience of traditional banks in ensuring cybersecurity is still not in demand within the crypto industry, which leads to users’ millions of dollars theft or data breach, like in an incident happened to Atlas Quantum account owners on Aug. 25.

The top five attacks on crypto exchanges are well known to traders and studied by cybersecurity specialists around the world. The list is headed by Mt. Gox, which has recently started accepting refunding claims of the traders affected by the hack.



Country: US

Founders: Jed McCaleb, Mark Karpeles

Funds stolen: 1.35 million BTC

Mt. Gox

Mt. Gox was first hacked in 2011, and then in 2014. The hackers compromised the account belonging to an auditor of the exchange. In the first case, 500,000 BTC — equivalent to \$8.75 million — were stolen from the accounts and from the depository as a result of the exchange's database being hacked. In the second case, attackers managed to withdraw much more — 850,000 BTC.

Civil investigators, unfamiliar with the subtleties of the cryptocurrency industry, were able to confirm the movement of only 200,000 BTC, which hackers transferred to their wallet by altering a nominal value of one Bitcoin to one cent. What happened to the rest of the assets is still unknown. The exchange terminated its operation in February 2014, resulting in three powerful blows to the Bitcoin exchange rate. Thus, in 2011, the cryptocurrency price fell from \$32 to several cents; in 2014, from \$720 to \$550; and in 2018, Mt. Gox arbitration manager Nobuaki Kobayashi sold a total of 35,841 BTC in the falling market, accelerating its further fall. Recent activities of Mt. Gox administration infuriated the deceived users, who demanded to "just give the people their money in BTC!"

PROTECTION ADVICE

Some cryptocurrency exchanges strengthen their defences by working with trustworthy security auditors who have proven hack-proofing expertise and white hat skills. They prefer to work with one contractor in relation to audits, DDoS mitigation, scans and site updates.

This minimizes the risk of audit-related vulnerability and access to stored funds falling into the wrong hands. For higher protection, additional banking tools are used — such as segregated master wallets, cold storage, layers of withdrawal authorization, IP address verification and email confirmation, two factor authentication (2FA) login and a crypto debit card, which can all be used to verify payments and user logins to the exchange.

iBitt COO Chris Schwarzenbach shared with Cointelegraph that the highest level of cybersecurity is only possible with a centralized exchange service, which has the development resources, security team, hidden servers and responsive control necessary to run military-grade security for a crypto exchange.

BitFloor

Country: US

Founders: Roman Shtylman

Funds stolen: 24,000 BTC

BitFloor suffered from the second largest hack in crypto history back in September 2012. It all started when the exchange's server crashed, either under the influence of a DDoS-attack or because of a power outage in the data center — as was claimed by its owner Roman Shtylman.

Four days after, the hackers used a backup copy of the key from the hot wallet of the exchange, where the funds of

traders were stored, and withdrew 24,000 BTC. Shtilman made an unsuccessful attempt to compensate the victims by selling a stake in BitFloor's property, but could not find an interested party. In 2013, the exchange closed, leaving the affected investors with nothing.

PROTECTION ADVICE

According to security experts, Bitfloor made two errors at once that led to such a severe financial loss. The first was storing the data in an unencrypted way — which Shtylman honestly confessed to — and the second one, which only aggravated the situation, was leaving large sums of money in an online-accessible hot wallet.

The simplest action to be done by any exchange in order to prevent the theft of coins is to keep the majority of its funds in “cold storage,” which ensures that private keys never touch any computer accessible from the internet. ThomasV, the lead developer of the Electrum client, provided seven key recommendations for cryptocurrency exchanges:

- *Don't store more Bitcoin outside cold storage than you can afford to lose and remain solvent*
- *Deposits should be sent to cold storage addresses directly*
- *Transfer from cold storage to hot storage should be manual only*
- *An attacker shouldn't be able to disguise a theft as a series of withdrawals from customers*
- *If a withdrawal request exceeds the amount available in the hot wallet, the customer should have to wait. Receiving coins 24 hours later is better than never*
- *Clone your database to a place where an attacker cannot irreversibly modify or delete it from the server*
- *Send digitally signed account statements to customers regularly, using a key that is not on the public server*

Poloniex

Poloniex takes the 3rd place in the long list of victims. In May 2017, hackers discovered a critical vulnerability in the exchange's software — all the withdrawal requests being simultaneously sent, were automatically processed regardless of the account balance. The owner of Poloniex, Tristan D'Agosta, did not name the exact amount of the stolen goods, but announced that the total users' funds were reduced at the time of hack equivalent by 12.3 percent or 97 BTC.

To cover the losses Poloniex had to cut all users' balances by this amount. These funds were temporarily frozen and then returned to users from personal funds, with an increase in the exchange's fees going up 1.5 percent. Users found this decision acceptable, and Poloniex saved its reputation and continued to work — periodically undergoing minor attacks. Now the exchange belongs to the American payment system Circle.

PROTECTION ADVICE

Tristan D'Agosta publicly revealed in his BitcoinTalk post what crucial mistakes had been made by the administration:

Country: US
Founders: Tristan D'Agosta
Funds stolen: 97 BTC

“The major problem here was that withdrawals should have been queued at every step of the way. This could not have happened if withdrawal requests were processed sequentially instead of simultaneously. Additionally, auditing and security features were not explicitly looking for negative balances. They add deposits and withdrawals and check that accounts are in balance. If you have 2 BTC, withdraw 10 BTC, and are left with -8 BTC, the software would see that you deposited 2, withdrew 10, and have exactly what you should: -8.”

Agosta has also advised on precautionary measures to be done in order to prevent such irreversible damage and shared new changes in the exchange's security system:

“Withdrawals and order creation have been switched to a queued method, where the first step is to add the task to a global execution queue that is processed sequentially. Each step of critical database operations is verified before proceeding, and such operations are in the process of being converted to transactions. I have hired additional developers to help with tightening up security at Poloniex, as well as created a bug bounty.”

Bitstamp

Country: Slovenia
Founders: Merlak brothers
Funds stolen: 19,000 BTC



In 2015, Bitstamp lost 19,000 BTC, which were stolen by hackers from the exchange's hot wallet. At that time, the losses were equivalent to \$5 million. Surprisingly, a banal phishing attack was used by hackers — the exchange employees received personal emails and messages in Skype from seemingly friendly sources.

What's maybe even more surprising is that the person responsible for security, Bitstamp system administrator Luka Kodrich, clicked the link and downloaded malware onto the working computer, after which the exchange was hacked. Bitstamp hurried to notify traders about what was happening, however, the attackers had already stolen the funds. Compensation did not followed, but the security regime was toughened that helped the exchange recover quickly. For the purpose of developing multi-signature protection Bitstamp has partnered with BitGo

Now, carrying out transactions on Bitstamp requires using multisignature, and 98 percent of the cryptocurrency is stored in a cold wallet..

Bitfinex

Bitfinex became the victim of hackers in August 2016. Unknown people used a bug in the multisignature system, which was supported by BitGo's partner company. The hackers deceived the BitGo algorithms in an unknown way, forcing them to approve transactions and withdrew about 120,000 BTC from the hot wallet, worth the equivalent of \$72 million at the exchange rate at that time.

The Bitfinex founders confronted the users about the fact that financial losses would be distributed among all the users, 36.067 percent of whose coins would be frozen. These funds were later compensated by BFX tokens, which could be converted into U.S. dollars at the exchange rate, or into shares of iFinex Inc., which belongs to Bitfinex founder. This chosen — and seemingly proper — policy helped the exchange stay in the top until today.

Country: British Virgin Islands
Founders: Rafael Nicole
Funds stolen: 120,000 BTC

PROTECTION ADVICE

Emin Gün Sirer, a famous computer scientist, specialist in hacking researches, and professor at Cornell University, suggested a solution that does not break Bitcoin's all-too-critical irreversibility when dealing with strangers, but allows someone to take back his funds in the event of a hack:

“The special thing about vaults is that they come with two keys. One key is used to unlock the vault and move your funds to a regular wallet. The other one, called a recovery key, is used when you notice that your funds were hacked and moved out of the vault by a hacker. You can then use your recovery key to undo the hack — you have 24 hours to notice and launch the recovery and get back all the funds. Notice that you cannot fool a merchant with this trick and revert a real transaction. All you can do is take back your own money from someone who is trying to steal it. If I may say so myself, it's a pretty ingenious scheme. It's almost like someone ought to work on it.”

Chronicle of 2018

Despite all the hopes of the crypto community, the year has not brought anything new to the established practice of securing the exchange sites, and 2018 is being marked by numerous attacks made with the help of new sophisticated hacking tricks. According to the Wall Street Journal, since the beginning of the year, hackers have managed to steal more than \$800 million and are not going to stop there.

Coincheck

Country: Japan
Founders: Koichiro Wada, Yusuke Otsuka
Funds stolen: 523 million NEM

Coincheck was attacked by hackers in the last days of January 2018. The target, as in most cases, was the hot wallet of the exchange, from which 523 million NEM tokens were stolen. Despite all the previous examples, the exchange continued to keep users' funds and even their own funds in the hot wallet and did not use the multisignature for protection.

Will the hackers cash out the stolen goods? Hardly. The crypto community united after this theft and finally began to actively exchange information in order to prevent further movements of stolen funds. In particular, the ShapeShift instant exchange service has banned the exchange of NEM coins. This example was followed by other services, since 11 anonymous addresses, which the stolen tokens had been transferred to, have been tagged with a sign "coincheck_stolen_funds_do_not_accept_trades: owner_of_this_account_is_hacker," so it isn't difficult to track any transaction made by hackers. The investigation of the incident and the development of compensation options for users are continuing.

PROTECTION ADVICE

Coincheck's example emphasized the importance of properly organized storage of users' funds on the exchange. Security layers and warning triggers are a must for any exchange service, says Nick Moore, CEO at Investa, a U.K. crypto exchange which also operates debit cards and ATMs:

"We hold minimal coins in our hot wallets and operate a time delay on withdrawals with manual review process, so the ability to hack account and amount of coins held on exchange is low. The risk of loss is minimized through the manual procedures of moving coins to cold storage when we identify that any excess funds have accumulated and are not needed for immediate liquidity. Storing the funds on cold wallets ensure they cannot be hacked and keeping a minimal float in hot wallets helps to save the liquidity."

"I'm sure users don't mind waiting a little longer for their withdrawals, when they realize that this is one of the best ways to fight the hackers."

BitGrail

Country: Italy
Founders: Francesco Firano
Funds stolen: \$170 million

On Feb. 13, BitGrail lost \$170 million in Nano (XRB) as a result of hacking attacks. At the same time, the founders of the exchange started a public discussion with developers of Nano's blockchain in order to define which side was responsible for the bug that led to the hack.

The developers of the cryptocurrency accused BitGrail of giving insufficient attention to ensuring security — in particular, in the absence of the authentication procedure for users. Later the exchange stopped working and turned over the investigation to the police.

The authorities of Florence confiscated all the cryptocurrency from the BitGrail deposit to secure the claim of the affected users, and the Nano Foundation promised to take part in the protection of their interests and compensation for losses.



Coinrail

Country: South Korea
Founders: Lee Nuss
Funds stolen: \$40 million

Coinrail fell victim to a hacking attack on June 10, 2018 and lost a total of \$40 million in 11 cryptocurrencies. Immediately after the attack, the representatives of the exchange were not ready to provide any intelligible information, so the details of the theft were revealed by the participants in the Pundi X project, whose tokens were also among the kidnapped.

A month later, on July 15, the exchange resumed trading and offered the victims two compensation schemes: a gradual refund through the purchase of stolen cryptocurrency and compensation with Coinrail RAIL tokens, which can then be converted into a cryptocurrency at the inner rate.

PROTECTION ADVICE

Rik Ferguson, an analyst at cybersecurity firm Trend Micro, believes the problem is in the weakness of the development team, insufficient cybersecurity education of the staff and poor investment in fraud analytics:

"By and large these exchanges are small businesses and they are most often in permanent startup mode, facilitating transactions. These organizations have small security teams, if they have one at all, little to no experience in securing a financial institution and generally a very large, attractive pile of money."

Bithumb

Country: South Korea
Founders: Kim De Shi
Funds stolen: \$30 million

Bithumb was hacked on June 19, just a few days after it updated its security systems. \$30 million, which was 10 percent of the total trading volume, was stolen by the attackers. This is the second incident in the chronicle of Bithumb. The first occurred on June 29, 2017, when the personal data of 30,000 users — equivalent to three percent of all the users by that time — was compromised. Hackers tried to access users' one-time passwords, but the exchange froze trades and made changes to the security system.

Bithumb spends eight percent of profits on security, strictly follows the rule "5.5.7" when five percent of employees are IT specialists having the confirmed expertise, 5% possess the skills to ensure cybersecurity, and at least seven percent of the company's profits are spent on its funds protection.

At the time of the hack, the exchange discovered a potential threat and was already withdrawing users' funds to a cold wallet. Affected traders were promised to be compensated from the personal funds of Bithumb administration.

PROTECTION ADVICE

Charlie Lee in a tweet expressed hopes for the restoration of the exchange and gave users concise advice, warning against such situations:

As I've said many times, be smart and only keep on exchange coins that you are actively trading. It's best to withdraw right after trading."

Bancor

Country: Switzerland
Founders: Guy Benarzi
Funds stolen: \$23 million

Bancor, a decentralized exchange created in opposition to centralized ones, to which Vitalik Buterin has recently addressed his angry "burn in hell" statement, was attacked by hackers on July 9, 2018. It is noteworthy that this happened a day after the exchange expressed in the official Twitter post the full agreement with Vitalik Buterin about centralized decisions and stated that decentralized exchanges are the future.

From the exchange's hot wallet, hackers withdrew a total of \$23.5 million. Almost half of the stolen funds was made up of their own BNT tokens (\$10 million), Ethereum

(\$12.5 million) and Pundi X (\$1 million). Its tokens were immediately frozen, which caused a flurry of criticism from the cryptocurrency community, because such actions directly contradict the principle of decentralization. Charlie Lee summed up the overall view in his Twitter, announcing that Bancor can manipulate users' funds.

As for users' tokens, Bancor immediately created a coalition with the instant exchange service Changelly, through which the hackers tried to withdraw funds. Transactions were frozen there as well.

How do banks deal with this?

Classic banks and banking services have been subject to various attacks since their emergence — that is, for several centuries. And over this time, they have been learning to resist such threats. The only difference is that 50 years ago, banks were attacked by criminals such as Bonnie and Clyde, and now they are attacked by hackers and internet scammers.

Classic banks follow the "5.5.7" formula and have international information security standards — for example, CobiT, which is considered entry level and is then supplemented by numerous internal regulations and scenarios for responding to intervention attempts.

Director of special projects at Group-IB Ruslan Yusufov is sure that the response to incidents must include both systems and an early warning and response plan that will allow all employees to act in accordance with regulations in the event of an incident. Everything is like that in the banking sector. A similar scheme was used by the Bancor exchange, which instantly froze its own tokens, calculated

the services through which the withdrawal was planned, and entered into a coalition with them to freeze the stolen assets.

Criticism on the part of the crypto community in this case is less important than efforts to preserve the investors' funds.

According to statistics, hackers, when attacking crypto exchanges, use tools that have been repeatedly tested on fiat banks. A study of 400 successful hacking attacks on the blockchain systems showed that popular banking services like TrickBot trojan, Vawtrak, Qadars, Triba, and Marcher were slightly modified for crypto exchanges and brought success to hackers in this way as well.

Nevertheless, the security systems of classical banks successfully resist hackers, and the established practice of tracking transactions allows customers to return the stolen funds. Why not borrow this experience? Unfortunately, in ICO teams — including those who create cryptocurrency exchanges — there is not a single IT specialist with the experience in the field of information security of banks.

Is it possible to return the money?

As practice shows, after powerful hacking attacks, crypto exchanges most often use three ways to compensate the affected users:

- 1. Rollback to a previous state or freeze transactions (Bitstamp, Ethereum and Bancor did this, but this contradicts the principle of blockchain's irreversibility).
- 2. Compensation at the expense of other users (this way was chosen by Poloniex).
- 3. Return the funds of the exchange from its own profit or by issuing exchange tokens (Bitfinex and Coinrail).

Thus, stable, large exchanges that are interested in continuing its operation will offer newer and newer ways of compensating for lost funds. And this is good news for the cryptocurrency industry. Obviously, the practice when the exchange owners tried to hide information from the community about the details of the theft and disappear themselves is being slowly abandoned.

Will cryptocurrency exchanges cope with the problem of hacking attacks sometime soon? Absolutely not. There are two main approaches to hacking exchanges. The first is to gain access to accounts and closed-functionality through the hacking of the founders' accounts and then to use malicious programs from the arsenal of bank attacks. The second is an attack on the infrastructure of the exchange itself, through the hacking of a web application linking the client to his money on the exchange servers or an attack on so-called hot wallets.

Consequently, the protection of digital assets can be achieved by the joint efforts of users and crypto banks serving the turnover of cryptocurrencies. Bancor's head of public relations, Nate Hindman, made a statement after the hack:

"These mechanisms include a real-time blacklist that tracks offending addresses and stolen assets, as well as an emergency fund that compensates projects when thefts occur. There is plenty more to do here and we look forward to working with our peers across the industry to make everyone [is] stronger and smarter as we move forward together. Collaboration is not just a concept, it's a practice — and we are grateful for the support and assistance."

At the same time, Hindman believes that it is impossible to completely eliminate the possibility of hacking attacks,

since attackers develop their own strategies along with the crypto industry, but these attacks can be resisted if market participants unite for joint actions and exchange of information.

As for ordinary users, the tips for preserving digital assets from hackers' are well known:

- Do not keep funds in hot wallets.
- Choose well-known exchanges that disclose security policies.
- Use the functionality provided by the exchange to the maximum, including 2FA.
- Distribute funds between several wallets and exchanges.

Probably cryptocurrency exchanges are so often hacked because it is easy to do — and punishment for this is not regulated yet. More exchanges are attacked, more people are left without money, and someone gets away with it. But this year, things may change, since all this has started to seriously concern regulators in state and even world scale.

Along with the G20, an entire consortia of summits are being held, devoted to the issue of regulating the activity of crypto exchanges. For example, one of the Futurama Blockchain Innovators Summit concept authors Joshua Hong reported to Cointelegraph:

"There are many unreported hacking incidents of major exchanges. So, from the perspective of regular user, we do not know how severe the level of hacking [is] for most exchanges. For example, Bithumb was recently hacked, but its trading volume or commission revenue didn't seem to get affected at all. On the other hand, other exchanges had to shut down their operation after a single blow of hacking."

The exchanges leaders positively react to such initiative. One of them, investment strategist at Bithumb Alex Lee expressed his personal interest to take part in such discussions:

"[The] best answers to the problems in our industry can be found through proactive sharing of each other's stories in highly personable ways. So, no matter what the issues are, be it crypto exchanges getting hacked or regulators feeling the pressure from disgruntled token investors who lost money, the solution can be found through community interactions and honest, open conversations."

IMPORTANT ASPECTS OF STABLECOINS:

THE DIFFERENCE BETWEEN PEGGING, COLLATERALIZATION, AND REDEEMABILITY



Stablecoins have been making the headlines in recent months, attracting big investors, tempted by the allure of a on 'non-volatile' cryptocurrency. At first, we usually pay attention to the backing connection, in other words, to the coin's stabilizing mechanism. Broadly speaking, this is broken down into 3 categories: asset-backed (including fiat), crypto-backed, and non-backed stablecoins (including algorithms and the Seigniorage shares' approach).

This is a great way of introducing the concept of stablecoins and a good basis for providing an overview, but it doesn't paint a full picture in terms of how the composition of stablecoins can ultimately affect

its utility and usability. To do this, we need to include 3 additional, but equally important, aspects into stablecoin discussions, i.e. pegging, collateralization, and redeemability.

These 3 aspects provide a more rounded explanation of how stablecoins work, how they are constructed, and how their utility and usability ultimately depend on it.

PEGGING

What is pegging?

Pegging is commonly associated with the world of foreign exchange, where the currency of one country is fixed or "pegged" to that of a country with a more stable economy. The main

goal of currency pegs is to bring stability to more volatile economies, but it's also a beneficial mechanism for trading partners to make exports more competitive while keeping import costs down.

Currency pegs stem from the Gold Standard that originated in early 18th century England, and the Bretton Woods agreement that was implemented after World War 2. Under this agreement, most Western European countries fixed their currencies to that of the United States, who in turn pegged the US Dollar to gold. Although the agreement was finally dissolved in 1973, it was very effective in the post-war era to stabilize economies and promote growth.

With cryptocurrencies today, we see the idea of stablecoins, such as USDVault, TrueUSD, Tether, Circle, Gemini, and Paxos Standard pegging 1:1 to a steady fiat currency like the US Dollar.

But the phenomenon is also still present in a traditional economy. Many countries use pegging to fix their currency, most commonly to either the USD or EUR. Very rarely though is it 1:1. Examples include the Hong Kong Dollar, pegged to the USD at a rate of 7.75 to 7.85, and the Danish Krone pegged to the EUR at 7.46.

Different types of pegging

There are different types of pegging mechanisms and not all pegs are a 100% fixed.

Crawling peg

A crawling peg is a fixed exchange rate but one that is allowed to fluctuate between the par value of the pegged currency and a range of predetermined rates. The par value may be periodically adjusted to account for inflation and other market conditions to increase stability. This allows an exchange rate to adjust over a period of time instead of a sudden currency devaluation.

A commonly referenced example, refers to Mexico, which implemented a crawling peg against the USD in the 1990's. This allowed it to gradually devalue its currency (hence the term crawl) over time, until it reached an acceptable exchange rate, thereby

avoiding economic instability associated with dramatic currency devaluations.

Adjustable peg

An adjustable peg is also a fixed exchange rate, but one that has a predetermined level of flexibility built into it (normally between one and two percent). If the rate moves beyond this range, the central bank will intervene to bring the rate back to the target peg. The goal is to allow a country to stay competitive in the export market.

Many developing Asian nations have been known to operate such an exchange rate regime in the past, including Indonesia, Malaysia, the Philippines, and South Korea, to restrict the degree of fluctuation towards the dollar and to allow for cheap exports.

Basket peg

With a basket peg, a currency will be pegged to more than one currency in a weighted mechanism, comprising currencies of its most important trading partners. The reason a country might use a basket peg is the same reason an investor would diversify their portfolio; to make the currency even more stable and hedge against the risks a single pegged currency might face when the anchor currency suddenly devalues, such as high inflation.

Examples here include the Chinese RMB, which is pegged against a basket of 24 different currencies, and the Fijian Dollar, which is pegged against five different currencies.

Commodity peg

A currency can also be pegged to a reliable commodity, such as gold. For many years, before WW2 and the Bretton Woods agreement, the Gold Standard was widely used to stabilize currencies. However, governments and economists believe the practice can actually stifle growth. Although central banks might still hold some

gold as a form of backing, the last currency to decouple from gold was the Swiss Franc in early 2000.

Many cryptocurrencies have been designed with a Gold Standard style mechanism in mind, where one token would be backed by a specific quantity in gold, such as Digix and OneGram for example. That has mixed results, because for investors, prices of commodities are not a relevant unit of account. It doesn't necessarily have to be gold. Venezuela launched the Petro, an oil-backed cryptocurrency pegged to the price of barrels of Venezuelan crude oil.

COLLATERALIZATION
What is collateralization?

Collateral is defined as “To offer an asset as a surety that a debt will be repaid.” Basically, it's the asset that the borrower leverages to secure a loan from the lender. The most common example we'll all be familiar with is mortgages, where the bank customer is able to obtain a loan to buy a house based on the provision that the bank may repossess the house if the customer defaults on their repayments. The house serves as backing or security on the loan and reduces the lender's risk.

The same principle can be applied to car financing, buying jewelry, or art. Businesses can also leverage their existing equipment to obtain financing. With stablecoins, the collateral refers to the commodity or fiat (i.e. USD, EUR). For every fiat collateralized token a platform issues, they should hold an equal amount of fiat currency as collateral, but this is not always the case, as we'll see later. The same goes for commodity-backed assets, for every token a gold backed stablecoin platform issues, they should hold an equal value of physical gold as collateral, but, again, this does not always happen.

Difference between backing and collateral

When a currency is backed by another commodity or asset, it does not necessarily mean the holder of the currency has that surety to exchange it, or have a claim on, the backed commodity. If we look at the Venezuelan Petro, example above, a holder of Petro tokens cannot exchange it for a physical barrel of crude oil. However, it does mean that physical barrels of crude oil are held in reserves to stabilize the cryptocurrency and to give it a fixed exchange rate.

It's the same principle with gold-backed currencies, where physical gold might be held in reserves to back the currency and to stabilize

it, but holders of the currency do not necessarily have a claim on the physical gold, only that they can redeem their currency at a fixed exchange rate against the gold.

Collateralization is different though. As Investopedia states it, “Collateralization occurs when a borrower pledges an asset as recourse to the lender in the event that the borrower defaults on the initial loan.” That means in the case of collateralized cryptocurrencies, the holder of such a coin has an actual claim on the collateral, i.e. they can exchange it directly for its value in gold, USD, or even other cryptocurrencies.

Level of backing

Most asset-backed stablecoins will claim to be fully backed by the underlying asset. However, understandably, these claims are subject to be scrutinized unless backed up by unbiased, 3rd party auditing entities. One of the most famous stablecoins, Tether (USDT), has been under fire for months since they parted ways with their auditor and have not been able to provide conclusive evidence that they hold 1:1 US dollars in reserve for every USDT that they issue and therefore might be severely under-collateralized.

Other stablecoins like Saga, are actually backed by a fractional reserve (i.e. they don't hold the entire backed asset in physical reserves) and pegged to the International Monetary Fund's

SDR (Special Drawing Rights), an international reserve asset.

On the other hand, a gold-backed stablecoin such as USDVault, is fully collateralized, meaning physical gold reserves to back issued tokens are held in vaults, which are transparently audited to make sure the stated value of gold actually exists, and a hedge mechanism is in place to maintain 1:1 USD price stability.

It is also possible for stablecoins to be over-collateralized. This is often the case when the actual collateral is another cryptocurrency, like with BitShares (BitUSD, BitCNY) and MakerDAO (DAI).

The issue with crypto-backed stablecoins is that the underlying asset can be just as volatile as the actual coin. So to counter that, the stablecoin will be over-collateralized, sometimes as much as 200%, so that when the backing cryptocurrency falls 25%, 50% or even 75%, there is still more than 100% of the value left to keep the price of the stablecoin from fluctuating. The important thing to determine is that, whether we are talking about the backing of a stablecoin or securing a loan, is the underlying asset adequate and reliable enough to achieve its purpose, i.e. to act as a security or to maintain stability?

REDEEMABILITY

Redeemability is closely related to our previous discussion on backing and collateralization. When a stablecoin is backed by a certain asset, it does not necessarily mean that the holder can redeem their token in exchange for that underlying asset.

If we look at Tether as an example, it's backed 1:1 by USD, but is not directly redeemable for USD. On the other hand, TrueUSD, a stablecoin designed on the same basis, i.e. backed 1:1 by the US dollar, is in fact, redeemable 1:1 with the US dollar.

In more traditional financial markets, the question of redemption is very valid in bankruptcy law, and dictates certain conditions that have to be met before an individual can actually redeem their claim on an asset, for said asset. Basically, unless explicitly and unambiguously stated, when a currency is backed by an asset, the user should not assume that they automatically have a legal claim on that asset.

There are various benefits for asset redeemable stablecoins. One being that it serves as a confirmation in itself that the underlying collateral actually exists, that it's not a baseless claim. It also provides practical use cases to users, such as, in the case of gold-backed stable coins, not having to convert to fiat for redemption and therefore avoid exposure to currency fees and price fluctuations.

CONCLUSION

As the market matures, stablecoins are becoming a more prevalent presence in the cryptocurrency space. New investors are continually looking to get into the crypto market, but at low risk and high security, while seasoned investors are looking for options to stabilize their portfolios and a safe haven in case of severe market downturns.

This continued search is sure to bring up some interesting mixing and matching of pegs and backings. Who says you can't have a stable coin backed by Ether and pegged to the Japanese Yen? Ethereum Founder and cryptocurrency influencer, Vitalik Buterin, had the following to say on the need for effective stablecoins:

“Are stable-value assets necessary? Given the high level of interest in "blockchain technology" coupled with disinterest in "Bitcoin the currency" that we see among so many in the mainstream world, perhaps the time is ripe for stable-currency or multi-currency systems to take over.”



This article does not contain investment advice or recommendations. Every investment and trading move involves risk, you should conduct your own research when making a decision.

UNTETHERED:

THE HISTORY OF STABLECOIN TETHER AND HOW IT HAS LOST ITS \$1 PEG

Tether, a cryptocurrency that has long been a point of contention in the community, has seemingly been uppegged from the US Dollar.

The stablecoin, by virtue of that very description, was linked to the US Dollar at a 1:1 ratio. Simply put, every Tether token that was minted had to be backed by a US Dollar.

Concerns around the validity of Tether's reserves of fiat currency corresponding to the circulating amount of tokens seem to have taken its toll. On October 15, the cryptocurrency dipped below the \$1 mark amid a wave of

negative sentiment that has led to an apparent sell-off of Tether tokens.

Another factor that may have influenced the drop in value of Tether was a report at the beginning of the month which stated that both Tether and Bitfinex, the exchange responsible for issuing the tokens, had parted ways with Noble Bank in Puerto Rico.

This was followed by Bitfinex temporarily suspending fiat wire deposits - with no specific reason given for the decision. It could well be that the closure of its Puerto Rican bank account has exacerbated the situation.

Tether is still trading below \$1 according to data from CoinMarketCap.

Image source:
CoinMarketCap



Revolutionizing privacy & turns activities into an asset

1. Platform 2. Token 3. DApps

1. Platform

The Quras project has been evolving and expanding its reach to provide a smart and secure solution for a wide range of different applications. It began with a passion to create a secure, anonymous blockchain for the healthcare industry, by achieving a level of previously unobtainable security and efficiency. Quras is now ready to change the way businesses and individuals define "secure". Utilizing an open source approach, Quras gives the user complete control over the management of their own rights, data and assets, while ensuring the utmost protection from any external interference.

2. Token

Quras is issuing tokens on Quras blockchain. It will be listed on major exchanges in 2019.

3. DApps

- ✓ Decentralized wallet
- ✓ P2P Chat Function
- ✓ Games to win free tokens directly to your wallet
- ✓ Own fee distribution of tokens by just taking a walking
- ✓ OTC trade function



quras.io

A HISTORY OF TETHER

Tether, as it is known today, was launched in November 2014, after it was rebranded from the original project Realcoin.

The project was initially founded by Bitcoin Foundation director Brock Pierce, alongside software engineer Craig Sellars, and entrepreneur Reeve Collins. The RealCoin startup laid the foundation for Tether’s operation before the name change came about.

The premise of the cryptocurrency was simple, to provide a utility token that represented certain fiat currencies at a 1:1 ratio, with the benefits of cross-border payments facilitated by blockchain technology.

The cryptocurrency was built and operated using an OmniLayer platform, a software layer built on the Bitcoin protocol. Thus, every time new Tether tokens were issued, these could be tracked on the platform, allowing the wider cryptocurrency community to keep tabs on how many new Tethers were released.

Tether’s account balances according to the ‘Transparency’ page on its website. Source: Tether

Current Balances			
USD		EUR	
Total Assets	\$2,352,698,729.15	Total Assets	€40,091,809.09
Liabilities (Tether in Circulation on Omni)		Liabilities (Tether in Circulation on Omni)	
Total Authorized	\$3,020,000,000.00	Total Authorized	€1,610.54
Less: Authorized but not issued	- \$66,078,763.48	Less: Authorized but not issued	- €168.55
Less: Quarantined Tether	- \$30,950,010.00	Less: Quarantined Tether	- €0.00
Liabilities (Tether in Circulation on ETH)		Liabilities (Tether in Circulation on ETH)	
Total Authorized	\$60,109,562.10	Total Authorized	€50,000,000.00
Less: Authorized but not issued	- \$25,108,983.00	Less: Authorized but not issued	- €10,000,000.00
Total Liabilities	\$2,337,371,745.62	Total Liabilities	€40,091,443.99
Shareholder Equity	\$15,326,983.52	Shareholder Equity	€358.01

USDT and EURT issuing address on Omni
What's holding USDT on Omni
(Bancor Contract USDT)



TETHER AND BITFINEX

Tether has had an interesting association with Hong Kong based exchange platform Bitfinex. The exchange integrated Tether into its operation in January 2015, but the relationship has come under intense scrutiny over the last few years.

According to Tether’s official website, the company shares the same leadership as Bitfinex. JL van der Velde is CEO of both companies, and Giancarlo Devasini is the chief financial operator of both operations as well.

The main reason for this has been spikes in the value of Bitcoin and other cryptocurrencies following the periodic issuance of new Tether tokens. Critics have claimed that the newly minted tokens were being used to prop up or manipulate the value of other cryptocurrencies.

While there is nothing to stop people from buying Bitcoin with fiat currencies or various cryptocurrencies on a multitude of exchanges, the use of Tether to do this has been disconcerting for one major reason.

Since its inception, Tether has asserted that it always has the necessary fiat reserves to back all circulating tokens in the market. The website even provides a real-time ledger of Tether tokens in conjunction with their underlying monetary reserve.

However, there have been claims that not all Tether tokens which are issued, have the necessary fiat currency reserve to back it up.

NO OFFICIAL AUDIT

While Tether’s balance sheet on its website claims to provide a transparent reflection of its accounts, Tether has failed to complete an audit of its accounts by a third-party - which was promised in 2017.

The crypto community began to put pressure on the company to conduct a full audit to allay fears of inadequate cash reserves to the number of Tether tokens. To this end, Tether acquired the services of Friedman LLP to conduct a short review of its account balances.

Following that, the company published a memo of a short report from Friedman LLP with the company’s accounts - in the hopes of appeasing the concerns of various parties online:

“We hope that the community considers the attached memorandum for what it is: a good faith effort on our behalf to provide an interim analysis of our cash position and our issued and outstanding tokens, as part of ongoing efforts to further professionalize the transparency mechanisms of Tether Limited.”

CONFLICTING REPORTS

Following the dissolved relationship between Tether and Friedman LLP, Bitmex released a report that speculated that Tether had the necessary cash reserves in a bank account in Puerto Rico.

While that report may have settled some concerns around the validity of Tether’s claims, a research paper published in June from the University of Texas blamed Tether for Bitcoin price manipulation in 2017.

By using algorithms to analyze market data, the report claimed that purchases with Tether were timed after downturns in the cryptocurrency markets which resulted in price increases in the value of Bitcoin.

In the same month, a law firm in the US released a report stating the Tether did actually have the adequate reserve of fiat currency to back tokens in circulation. Law firm Freeh Sporkin & Sullivan LLP had access to two of Tether’s bank accounts to release its findings — which were not an official audit.

In response to the report, Tether’s general counsel Stuart Hoegner told Bloomberg that mainstream accounting firms would not conduct official audits on companies working with cryptocurrencies:

“The bottom line is an audit cannot be obtained [...] The big four firms are anathema to that level of risk. We’ve gone for what we think is the next best thing.”

As various critiques came out in public, Bitfinex eventually threatened legal action against parties that were questioning the authenticity of their operation in November 2017.

Both Bitfinex and Tether then received government subpoenas in December 2017 from the Commodity Futures Trading Commission (CFTC) in response to the concerns raised towards the end of the year.

With the pressure firmly on, Tether got Friedman back to conduct a full audit in January 2018. But less than a month into the process, Tether stopped the auditing process, claiming that it wouldn’t be completed in a reasonable period of time, according to Bloomberg:

“Given the excruciatingly detailed procedures Friedman was undertaking for the relatively simple balance sheet of Tether, it became clear that an audit would be unattainable in a reasonable timeframe.”

MAJOR STABLECOIN COMPETITORS LAUNCHED

While Tether has long been hailed as the original stablecoin pegged to the US Dollar, its duopoly with TrueUSD, has been disrupted by the approval of two new stablecoins linked to the Dollar.

In September, Paxos and Gemini launched two new stablecoins called the Gemini dollar (GUSD) and the Paxos Standard (PAX), which are both backed by the US dollar on a 1:1 ratio.

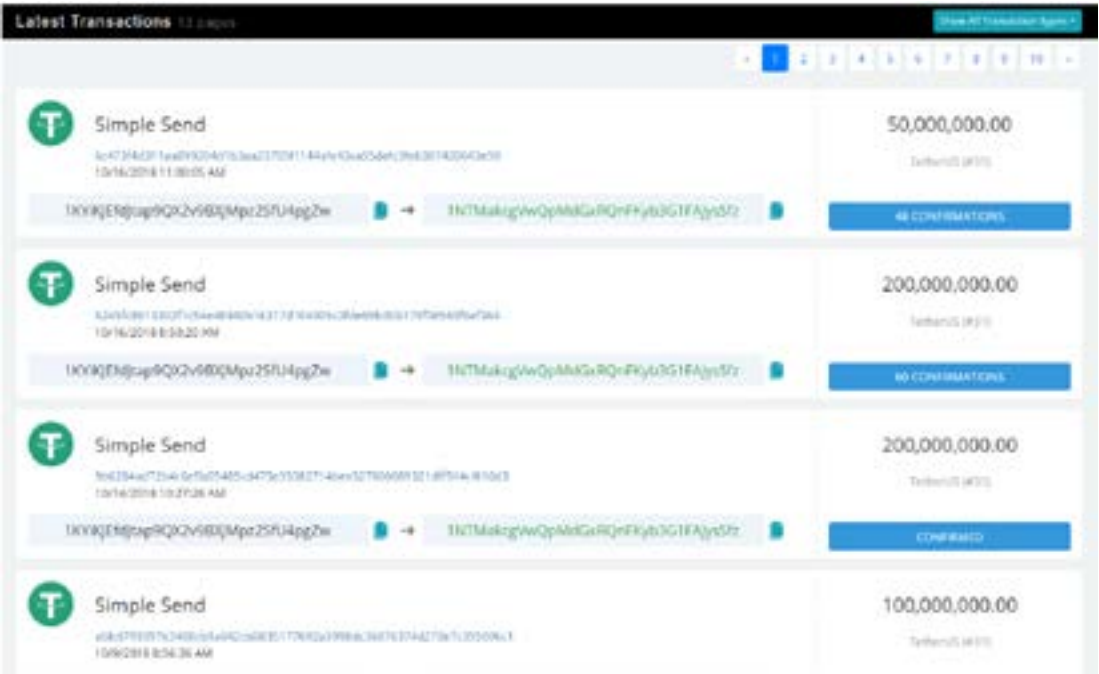
Both stablecoins are based on the Ethereum blockchain using ERC-20 token standards, which also ensures full transparency of these coins, as Ethereum can verify the smart contract of both ERC-20 tokens.

This should also rule out the need for third-party service providers and exchanges in order to make transactions with these stablecoins.

NEW TETHER CONTINUES TO BE MINTED THROUGHOUT 2018

Despite all of this media attention, Tether tokens have continued to be issued through the year, according to data from Omni Explorer.

Source: Omni Explorer



In August, more than \$500 million worth of tokens were released, but the focus of many reports was on the apparent lack of effect this had on market prices these issuances were having.

CRYPTO COMMUNITY WANTS TRANSPARENCY

An overarching theme of the Tether saga has been the lack of trustworthy transparency when it comes to the necessary reserves of fiat currency to back-up newly minted coins.

To date, Tether has not undertaken or released an official third party audit of its accounts. While the community would love to give them the benefit of the doubt, hundreds of millions of dollars have been spent on Tether tokens and this necessitates a transparent and trustworthy audit.

If the company had carried out this process, at whatever cost and given timeframe, all fears could have been allayed. The failure to do so has led to serious uncertainty, the consequences of which are apparent in the current valuation of Tether tokens.

The launch of new stablecoins by highly reputable service providers has the potential to provide a viable alternative to Tether. The pressure is firmly on the company to prove it is running a transparent operation. ⚡



According to CoinMarketCap

Find more insights in our data that might surprise you today.

CoinMarketCap.com/data-room



NOURIEL 'DR. DOOM' ROUBINI:

'99 PERCENT OF CRYPTOCURRENCIES ARE WORTH ZERO'

Nouriel Roubini is a New York-based economist that famously predicted the 2008 financial crisis when only a few considered there might be a threat to the existing course of events at the time.

A Harvard alumnus and now a professor at NYU Stern School of Business, Mr. Roubini has always been critical of the crypto and blockchain industry. Oct.11, 2018 he testified at the Congressional hearing on Capitol Hill, Washington D.C., warning U.S. senators about “the mother or father of all scams and bubbles,” — crypto.

We met with Mr. Roubini during BlockShow Americas in Las Vegas and talked about why he doesn’t believe in smart contracts, thinks Ethereum is a scam, and the fact that he might want to give the industry another try.

On being “against” the crypto industry

“I’m not against [it], I’m open to any type of innovation, but I’m an expert on financial crises and asset bubbles. And I became famous [by] predicting the global financial crisis — the burst of that bubble.

I can see a bubble when there is one — and to me, this entire space has been the mother and the father of all financial bubbles and now it’s [going to] burst.



Last year, almost everybody I knew was asking me every other day, “Should I buy Bitcoin?”

And the price of Bitcoin doubled, tripled, quadrupled, and went to \$20,000. And when that bubble burst, it collapsed — collapsed from \$20,000 down to \$6,000 today (at the time of the interview).

If you bought it at the peak, you lost 70 percent of your value. And it's typical of all these financial bubbles: They go up until they collapse. And Bitcoin is actually the best [example], because the average cryptocurrency has lost, in the last nine months, more than 90 percent of their value.

I spoke about the bubble existing and this bubble going bust. And guess what? In the last year, [it] has gone bust. So I think I've been vindicated and proven right.

Bitcoin could go to the moon or zero, I'm not going to make a penny either way because I'm neither short or long.

And I'm just an academic that speaks his mind. And I saw a big bubble, and I think that it's fair as an intellectual to discuss these things and then figure out what's going wrong.”

On future price movement and Ethereum being a “scam”

“An academic study suggests that 81 percent of all ICOs were a scam to begin with; 11 percent of them have failed or have died; and of the remaining eight percent that is traded on exchanges, the top 10 have lost on average, in the last year, 95 percent of their value — more than Bitcoin.

So, there was a bubble — and everybody was riding the bubble, everybody was issuing an ICO, raising money — but now it's gone bust.

I think that they've lost already 95 percent of their value and they could lose another 95 percent.

I would say 99 percent of cryptocurrencies are worth zero. Just because some people believe in something alternative to fiat currencies — alternative to gold — then, like collectibles, some people are going to hold some Bitcoin. Bitcoin is not going to disappear. But, you know, Ethereum is a bubble and it's a bit of a scam — it's worth nothing — XRP, all the other ones, they're all going bust.”

CATHERINE ROSS: WHY DO YOU THINK ETHEREUM IS A SCAM?

It's a scam because the technology. They talk about smart contracts — there's nothing about them that is smart, they're all buggy. They're not real contracts because you have to enforce certain contracts, you cannot have just the code.

They've tried things that have failed: Their DAO was a failure.

You know, there's a lot of people [who] talk about their DApps or their distributed apps. 75 percent of those apps are what? CryptoKitties, Ponzi schemes and other pyramid schemes, and other casino games, like Las Vegas. So, after a decade, what does Ethereum have to show us? CryptoKitties and Ponzi schemes? And that's what they're doing? They're not doing anything that is of any use to anybody.

CR: BUT IF A SMART CONTRACT IS A TECHNOLOGY, — AND YOU SAID “IT’S BUGGY” — TECHNOLOGY CAN BE BUGGY AND IT CAN BE FIXED. DON’T YOU THINK WE NEED MORE TIME TO SEE THE TECHNOLOGY RISE AND SMART CONTRACTS WORKING BETTER?

NR: I don't believe, first of all, in smart contracts. By definition, any contract has to be enforced by lawyers — [there is nothing that is enforced] by itself. So, the idea that you put everything in a code in a contract is silly to begin with. And, you know, a typical other program has less than one percent of bugs in its code, and a typical smart contract has 10 percent of its code is buggy [sic].

I mean, this is the reality where we are in now.



And by the way, the broader question about cryptocurrency is that they are not scalable, and there's no system that makes them scalable; they're not decentralized because the entire system is [becoming] centralized; and they are not secure because there are so many ways to hack them.

So, it doesn't have any functions [it] should have: It's not scalable, it's not secure, it's not decentralized. So, what is it worth for? With Bitcoin, you can do five transactions per second; with Visa, you can do 25,000 transactions per second.

They've [the blockchain community] been saying for a decade, “We are going to resolve it with proof-of-stake rather than proof-of-work.” It has not worked yet. And even if there was something scalable, it's going to be centralized and therefore is not secure. So, there's a fundamental flaw in the technology.

At least financial systems that we know are centralized, yes, but they're secure and they're scalable.

They've been talking about fixing it, but Vitalik Buterin, who is the creator of Ethereum, said you cannot have a blockchain system that has three characteristic of the same time: being scalable, decentralized, and secure.

On trusting the financial system

CR: EVEN AFTER THE 2008 GLOBAL FINANCIAL CRISIS, YOU STILL BELIEVE IN THE TRADITIONAL FINANCIAL BANKING SYSTEM?

Traditional financial systems are centralized — and there's nothing wrong with institutional centralizing in my view. They [the blockchain community] criticize it, saying “We want it decentralized.”

But I prefer a centralized system with a trusted authority — but at least they're secure and scalable.

There's a lot of talk about decentralization: Miners are centralized as an oligopoly, coders are centralized, exchanges are centralized — as 99 percent of all transactions occur on a centralized exchange — and there's a massive concentration of wealth. This is worse than North Korea in terms of income and wealth inequality.

The reality is just the opposite: It's a totally centralized system.

[At the same time] there are many problems with the traditional financial systems. And I've been one of the biggest critics of the financial system. And I believe that there are ways to [democratize] finance and [to]

make it more efficient, but this is not based on blockchain.

There is a revolution in financial services: It's called fintech and it has zero to do with cryptocurrency and blockchain.

It's based on AI, machine learning, Internet of Things and big data. It's revolutionizing payment system, insurance, credit allocation, capital market functions, and asset management.

Take, for example, payment systems: There [are] already plenty of digital payment systems — that do billions of transactions a day, and are used by billions of people around the world — that are not based on blockchain. In China, you have AliPay and WeChat Pay; in India, you have all these UPI systems; in Africa, you have M-Pesa; in the United States, you have Venmo, PayPal, Square — and so on, and so on. These are useful transactions.

With these models, you can do millions of transactions — and there are billions of transactions done by billions of people today. They are digital payment systems based on [the] traditional financial institution and fintech. They have nothing to do with blockchain. We don't need blockchain, we don't need crypto to [democratize] finance.

There is already a revolution: there's going to be much

more competition, there'll be much more access. If you are a poor farmer in Kenya today, you are using M-Pesa. On your little smartphone, you can make transactions, you can borrow and lend, you can buy and sell your goods and services, you have a whole slew of financial services without the brick-and-mortar bank. And all these things are available to billions of poor people in Africa. What [do] they have to do with blockchain or crypto? Nothing, zero. So, there is a revolution and it has nothing to do with blockchain.

CR: THE ENTIRE PHILOSOPHY OF THE INDUSTRY WAS TO CREATE A TRANSPARENT SYSTEM AND CREATE A NEW WORLD FROM A FINANCIAL SYSTEM THAT YOU CAN TRUST, A FINANCIAL SYSTEM THAT THINKS ABOUT A USER, A CLIENT. SO YOU THINK IT FAILED TO DO WHAT IT WAS SUPPOSED TO DO?

NR: Of course, it completely failed: After 10 years, there is no killer app; the crypto assets are going bust; they've lost 99 percent of their value; all these experiments have led not a single corporation or single financial institution using this technology; and there is no reason why they want to use this technology. And why would you want [to]?

Why would I want to trust somebody in Russia or China to verify my transactions? It's not safe. Why would I want to do it? There are central banks, there are corporations, there are institutions that have been existing forever that are based on trust — on the reputation. And I know what I'm dealing with.

MASS ADOPTION

I'd rather have those institutions verify my transaction rather than somebody in China who can manipulate everything I am doing. Why should I trust somebody while I don't even know what the name is, who they are, what they do.

CR: SO, YOU WOULD RATHER TRUST A BANK? HOW CAN YOU BE SURE THAT YOUR MONEY IS SAFE?

NR: We have security laws. If a bank manipulates, there've been hundreds of billions of dollars in fines on the banks and their misbehavior — people ended up in jail. There are lots of problems with the traditional financial system: Blockchain and cryptocurrency do not resolve this problem. Fintech resolves it, but fintech has nothing to do with blockchain or cryptocurrencies.

I'm the first one who criticized the financial system, I've been writing about financial crises, I've been criticizing [the] banking system. I don't believe that crypto or blockchain resolves any, any of the problems of our existing financial system, [and they] don't resolve anything.

It's just something for a bunch of self-serving people speaking about decentralization, speaking about freedom, speaking about [the] democratization of finance — and there is no democratization of finance, there is no more access to financial services through crypto or blockchain.



I may be right or may be wrong, but crypto could go to the moon to go to zero; I'm not going to make a penny out of it. I'm an intellectual. I'm an academic. I have no conflicts of interest.

My only thing is my own academic reputation. If I'm proven wrong, my reputation is going to be negatively affected. But I'm not going to make a penny. And therefore, I'm not going to take a position one way or another because if I take a position, I have a financial interest to talk down or up a particular cryptocurrency; and that's not my interest.

I'm an intellectual and I'm not going to make money — one way or another — out of it. ⚡

There are other alternatives that exist out there, like M-Pesa, that are giving power and giving democratization of finance to billions of people in Africa. Those things have nothing to do with blockchain. I believe in those things.

I don't believe in blockchain.

CR: I SEE YOUR POINT OF VIEW, BUT JUST TO BE CLEAR, THE BANKING SYSTEM HAS BEEN AROUND FOR CENTURIES, RIGHT? SO, MAYBE YOU SHOULD GIVE THE CRYPTO INDUSTRY AND BLOCKCHAIN INDUSTRIES A TRY?

NR: No. I'm not giving it a try. I'm gonna give a try to financial innovation that changes the financial system.

All those things [mentioned above] — they are revolutionizing finance, they are leading to competition, they are forcing the banking system to innovate or not survive, and they are changing the world. But they have nothing to do with blockchain. Why should I give the benefit of the doubt to something that has not provided any application which is used by anybody. I don't believe in it and the proof is in the pudding.

CR: MY LAST QUESTION IS, HAVE YOU EVER TRIED TRADING CRYPTOCURRENCY?

NR: I haven't tried it. Some people say, "Oh, you are critical of crypto because you are shorting Bitcoin or cryptocurrencies." I have zero position — I have no long position, no short position.



MITHRIL

A decentralized social media platform that rewards all content creators.

Mithril founder, Jeffrey Huang, is a Taiwanese-American music, entertainment, and technology industry leader based out of Taipei, Taiwan. Jeff has always taken an interest in new technologies as an early adopter. His most recent project, 17 Media, is the number 1 live-streaming app in developed Asia. As a content creator all his life, he believes that all content creators, amateur or professional, should benefit from their work.

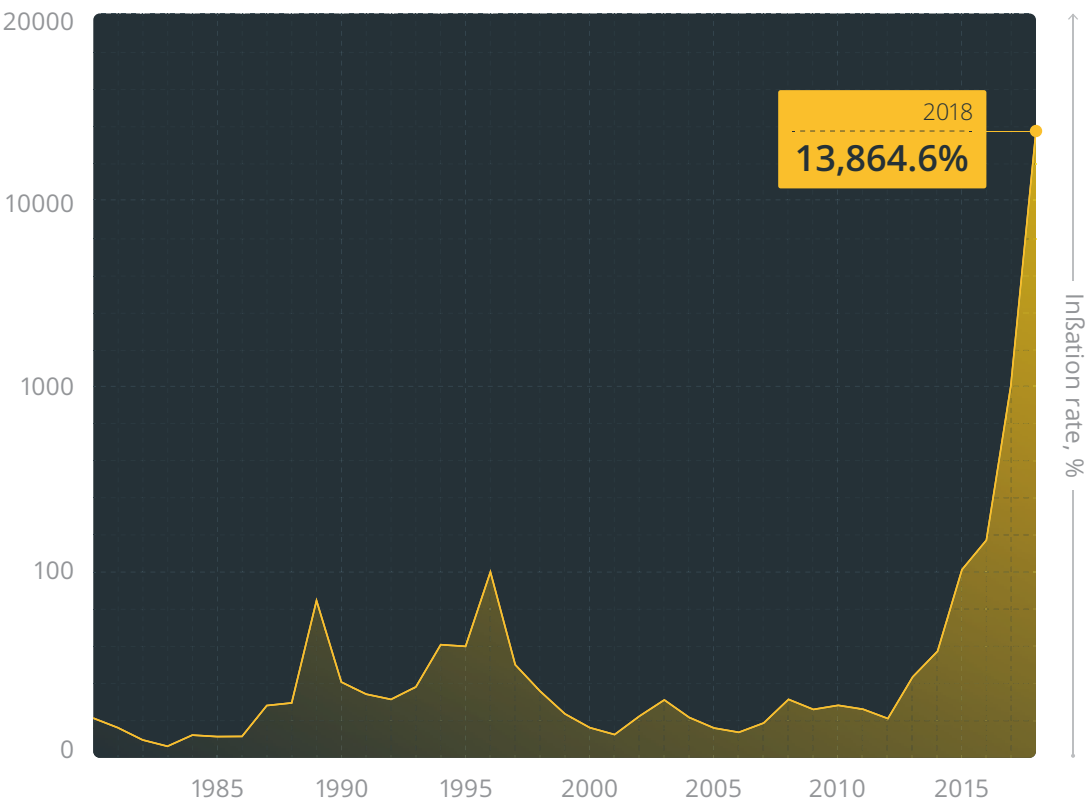
To realize this future, Mithril is establishing an integrated ecosystem starting with social media content and using MITH tokens as rewards. MITH tokens can be acquired through social mining across accepted social networks, and can be spent in the Mithril Merchant Network, which includes online applications and brick-and-mortar retailers.

HOW VENEZUELA BECAME ONE OF THE BIGGEST MARKETS FOR CRYPTO IN THE WORLD

Venezuela has been living with hyperinflation since at least 2014. Its national currency — the Venezuelan bolívar — hit an official inflation rate of 57.3 percent in February 2014, while independent currency analysts were reporting that, by that September, the real inflation rate had already topped 100 percent. In other words, the bolívar (VEF) was depreciating rapidly in value, and ordinary Venezuelans needed something to fill the void it had left as a one-time viable means of exchange.

By definition, hyperinflation is a state in which, as described by the International Accounting Standards Board, "the general population prefers to keep its wealth in non-monetary assets or in a relatively stable foreign currency." However, due to capital controls that had been in place since 2003, Venezuelans were restricted in their ability to obtain U.S. dollars or any other foreign currency. They had no freely accessible outlet for their devalued VEF, with the Venezuelan economy expected to contract in 2015 by 1 percent, according to the IMF.

VENEZUELA INFLATION RATE



It was into this economic quagmire that Bitcoin and altcoins (particularly Dash) entered, providing struggling Venezuelans with stores of value and mediums of exchange they could rely upon more than the nosediving bolívar. Ever since 2014 and the onset of hyperinflation, they've seen marked increases in ownership and trading, with impressive rises being witnessed in the past few months, as Venezuelan inflation topped an eye-watering 46,000 percent and as the IMF predicted an inflation rate of 1,000,000 percent by the end of 2018.

However, as the following will show, the meteoric rise of crypto in Venezuela doesn't simply result from the desire to avoid the worst effects of hyperinflation. It also stems from the proactive attempts certain cryptocurrencies have made to establish themselves within Venezuela, as well as from a desire among the population to resist and circumvent an authoritarian government, which has used capital controls as one way of starving likely opponents of funding.

Bitcoin growth

As an indication of the extent to which crypto usage has grown in Venezuela, it's worth looking at the trading charts provided by the Coin Dance website for the LocalBitcoins exchange, which enables peer-to-peer trades between any two parties anywhere in the world.

In November 2013, around the time Venezuela had an official — i.e., massaged — inflation rate of 'just' 43 percent, a grand total of two Bitcoin were traded for VEF

on the LocalBitcoins exchange. This modest volume, however, quickly rose almost as soon as the country firmly entered hyperinflation territory, with the peak for 2014 being the 64 Bitcoin traded in December, at a time when the BTC value had sunk to as low as \$311 — after having stood at around \$932 at the beginning of the year. It was at this time that inflation was at 63 percent, according to the government, and given that the country had been caught in hyperinflation for well over a year, many groups and individuals were beginning to recognize the vital role crypto could play in giving Venezuelans a lifeline.

One Venezuelan Bitcoin trader told Reuters in October of that year:

"Even though Bitcoin is volatile, it's still safer than the national currency."

While Gerardo Mogollon, a business professor at the University of Tachira, told the news agency:

"I'm teaching people to use Bitcoin to bypass the exchange controls."

2015 was an even better year for Bitcoin, despite — or rather because of — it being a worse year for VEF and for Venezuelans. Annual inflation reached as high as 335 percent in June 2015, according to currency economist Steve Hanke, while 319 Bitcoin were traded on LocalBitcoins for VEF in the month of February alone. This figure excludes volumes on Venezuelan exchanges such as Surbitcoin, which in 2015, was reported by Bitcoin Venezuela as being the "second largest in transaction volume in Latin America after Brazil." It also pales in comparison to the number of Bitcoin traded over the entire year, which — at 2059 — was 983 percent bigger than 2014's total (190) and was worth around \$1,281,223 (based on a crude average annual price for Bitcoin of \$622).

told the Guardian in August 2017. Meanwhile, the percentage of children suffering from acute malnourishment sneaked from eight percent in the previous October to 12 percent that July. "They are getting younger, and the cases more serious," explained Susana Raffalli, the leader of a Caritas project aimed at combating youth malnutrition in the country.

With most Venezuelans going to bed on an empty stomach, the need to source alternative currencies was acutely felt by the population, not least because the national poverty rate had climbed

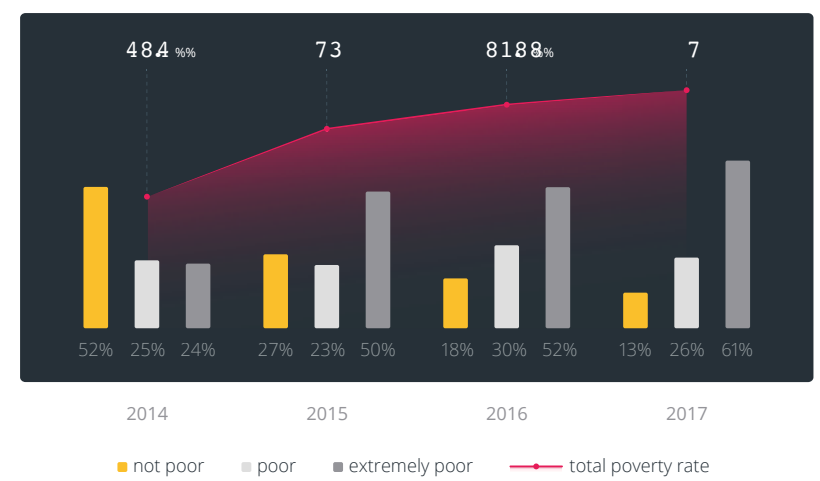


In 2016, the total number of Bitcoin traded via LocalBitcoins was 8624, a 318.8 percent increase over the previous year that coincided with Venezuela's annual inflation rate reaching as high as 500 percent. In 2017, the total number of BTC traded on LocalBitcoins rose again, ramping up to 21,556 — a 150 percent increase over 2016's total. Given that Bitcoin itself became more expensive in 2017 — rising to \$19,000 in December — this expansion offers a stark indication of just how sought-after Bitcoin and crypto had become, as inflation surged to yet another peak of 1,369 percent, according to figures released by the opposition-led Venezuelan parliament.

Because of Venezuela's economic misery, many locals had begun finding it difficult even to secure enough food to eat, as the wages they were paid (in VEF) increasingly dwindled in value. "It's like an obstacle course. You have to find money to buy food, a place to buy it and then get there in time," one Venezuelan

from 48 percent in 2014 to 82 percent in 2016, and then 87 percent in 2017. And it's likely to climb yet again this year, given the quintuple-digit inflation currently in motion — something which has unsurprisingly kept the Bitcoin-buying rate noticeably high.

POVERTY IN VENEZUELA



According to Coin Dance, 14,886 Bitcoin have been purchased with VEF on LocalBitcoins between the beginning of 2018 and Aug. 18. This is almost 1,000 fewer than the 15,868 BTC purchased over the same period last year, yet there has been a distinct upswing in trade volumes over the past month — just as the country's economic crisis has reached a new fever pitch, after the government devalued the bolívar by 95 percent in August. Already, before figures for the final week of August are even available, the total number of Bitcoin traded on LocalBitcoins has reached 2,532, in contrast to the 1,558 traded for all of August in 2017.

This could presage an accelerated rise as Venezuela sees out the rest of the year. Either way, trade volumes are high, and Bitcoin's reputation as an alternative to the bolívar is firmly cemented in the eyes of many Venezuelans. "Luckily, I've always been a fan of Bitcoin and the blockchain technology," wrote one Venezuelan Bitcoin user in a Reddit AMA from July:

"I spend my spare time teaching people how to change their bolivares to crypto so the inflation doesn't wreck their money. So far, I've helped many [businesses][...] i.e, restaurant owners who try to sell dishes every day and the next when they're trying to buy some meat there's no profit (sometimes they can't even afford it), because inflation hits us so hard. Right now the inflation is 1.000.000 percent++. I'm looking forward to a plan [to] help people get food through crypto [...] I'm pretty much focused on training on Bitcoin use and saving [whomever] I can from hyperinflation, I believe Bitcoin is the solution!"

Dash

This linear picture of Bitcoin's rise is, however, complicated by three simple facts: a) it's not the only cryptocurrency available to Venezuelans, b) its growth was hindered by a government crackdown on Bitcoin mining between March 2016 and January 2018, and c) it has suffered (particularly in 2017) from relatively high transaction fees and confirmation times. As a result, Venezuelans have increasingly dabbled in other coins as their economic crisis has unfolded, including Ethereum and Zcash.

However, it's Dash that's leading the charge as the most popular altcoin — and possibly the most popular cryptocurrency.

In August 2016, Dash was added as a tradable cryptocurrency to the Caracas-based Cryptobuyer exchange, which was reporting "soaring demand" for cryptocurrencies at the time. "Our partnership with Dash is valuable," explained Cryptobuyer CEO Jorge Farias in a press release, "especially for customers using unstable fiat currencies, and the perfect example can be found in Venezuela right now. Alternatives for accessing money without traditional banks are gaining traction fast, and we are incredibly confident that Dash will flourish in this economy."

Unfortunately, it's difficult to find websites that offer specific volume data on the DASH/VEF market, so there's no objective and publicly available reading of just how quickly Dash usage has expanded since the end of 2016, or of how it compares to Bitcoin volume. Nonetheless, the indications that are available suggest that it has become enviably popular since 2016, with the Dash Core Group announcing on Aug. 22 that Venezuela was the cryptocurrency's second biggest market, after the United States.

Only 20 %of Paraguay's forest remains.
We need you to prevent further deforestation!

In the next year the goal is to plant 10 million trees on 12 700 hectares or more.

When you invest 23 US-Dollar s, a tree is planted, plus you get 70 TreeCoins.

After 4 years, half of the planted trees are cut down.

40% of the profit will be paid out to investors as a dividend.

The rest will be reinvested in further forestation and in the purchase of 20% of additional fallow land. This way, new trees will be planted on the cut down area plus on the newly bought land.



And as Dash Core's CEO, Ryan Taylor, told Cointelegraph, this success is once again partly a result of Venezuela's economic and monetary difficulties:

"We've found that regions of high inflation rates and industries in which cash handling or credit card chargeback rates are high have been most excited to adopt the technology. For us, we focus on those segments in which cryptocurrency can offer the most benefit, and that's one of the reasons growth in acceptance is so high."

In fact, Dash's superiority over Bitcoin, in terms of transaction fees and confirmation times, is such that the cryptocurrency is now reportedly the most popular in Venezuela among merchants — or at least this is what Dash claimed in a July article, without providing comparative figures. At the very least, Ryan Taylor states that over 800 merchants in Venezuela now accept Dash, and while there isn't an authoritative source for the number of merchants now accepting Bitcoin, Coinmap currently lists a little over 160 merchants in the country that accept BTC (as reported to the website by users, so the actual number may be slightly larger).

Ryan Taylor explains Dash's greater popularity in terms of its greater cost-effectiveness in relation to Bitcoin:

"From the perspective of merchants and businesses, Bitcoin has many uses, including as a means of payment [for] online purchases and for transferring money cross-border at low cost. However, Bitcoin transactions are not instant, which means they are not useful for live transactions such as at a register or for online transactions that customers wouldn't want to wait [for] — such as a digital media purchase. Bitcoin is also too expensive for micro transactions."

Yet, what's interesting about Dash's rise to prominence isn't simply that it has benefitted from user friendliness and from rampant hyperinflation, but that it has made a concerted effort to drive and encourage its adoption throughout Venezuela. Distinguishing it from other coins, 10 percent of its block rewards go to a treasury fund that allocates finances to projects voted for by Dash master nodes. As a result, the Dash Core Group has been able to invest around \$1 million of such funding to promote and raise awareness of Dash in Venezuela, with this funding going toward such things as billboard ads and sales representatives. For example, Dash Caracas — the self-proclaimed first Dash community in Venezuela — began running educational conferences in September 2017, which now accommodate around a thousand attendees. Its leader Eugenia Alcalá Sucre said last September:

"We had a team receiving the attendees and giving them a folder with sheets to take notes, a pen, [instructions] to set up their Dash Wallets and paper wallets with \$10 in Dash. Then they got into the hall, where they watched a welcome video, where they also got instructions for their wallets (phone and paper)."

Such evangelism is clearly having an effect on Dash adoption rates, and it's also something that Bitcoin advocates have been doing in Venezuela, even if Bitcoin's lack of a "Core Group" and a treasury has resulted in its propagation being less unified or organized.



Petro and the government

And funnily enough, cryptocurrencies in Venezuela haven't been boosted solely by crypto groups, but also by the Venezuelan government itself — despite the hard line it had initially taken on Bitcoin miners. Given the economic meltdown the nation was going through, and given that cryptocurrency had already enjoyed such an impressive ascendancy in the preceding months and years, the government announced in early December 2017 that it would issue its own oil-backed cryptocurrency, the Petro. While the Petro has been dissected and denounced by crypto experts and the Venezuelan

opposition alike, it has at least had the inadvertent effect of providing a more favorable environment for non-centralized coins to flourish.

To begin with, its creation resulted in the Venezuelan government declaring in January that crypto mining was "perfectly legal," despite having prosecuted miners for over a year prior to that. From that point onward, those "people who have been victims of seizures and arrests in previous years will have charges dismissed," according to the nation's new cryptocurrency superintendent, Carlos Vargas. And since then,

MASS ADOPTION

cryptocurrency mining appears to have continued increasing its popularity, with a May Bloomberg article's headline — perhaps not without some exaggeration — reading, "There's a Crypto-Mining Machine in Every Home in Caracas."

And as the government prepared for the Petro's ICO and eventual release into circulation, it launched free cryptocurrency lessons for the Venezuelan population. Beginning from the end of February, Venezuelans were able to register at the Granja Laboratorio Petro in Caracas for a course that would, according to instructors, cost them between \$500 and \$800 anywhere else in the world and that would instruct them on how to "buy, sell and mine digital currencies." One teacher of the course, Carmen Salvador, told a local news outlet that the course was intended to reach the widest possible audience:

"Many of our young people here find it impossible to have this amount of resources, [but] the Venezuelan state is guaranteeing that all can participate through these plans."

There are no statistics available on the number of enrollments in this course, but in view of how popular cryptocurrency had already become among Venezuelans, it's reasonable to assume that signup was relatively high. So, even if the government may have continued to put up some resistance toward cryptocurrencies that weren't the Petro (e.g., closing two crypto exchanges in April, although apparently more for disseminating 'false information' about the VEF exchange rate than for permitting trades in crypto), its desire to cultivate a favorable social attitude toward the Petro most likely had the collateral effect of increasing the profile of Bitcoin, Dash, Zcash and Ethereum even further.

And on the subject of inadvertent effects, there's a direct — though unquantifiable — link between the Venezuelan government's authoritarian tendencies and the attraction cryptocurrency holds for many locals. For one, the imposition of capital controls in 2003 was in part a move by then-President Hugo Chávez to cut off potential funding from any of his opponents who might be tempted to organize a repeat of the attempted coup d'état of 2002, or a repeat of the anti-government strike that precipitated it. As he declared during a televised address announcing the controls, "Not one dollar for coup-mongers."

Venezuelan business leaders were quick to denounce the controls, with the then-leader of the Federation of Chambers of Industry & Commerce, Carlos Fernández, telling that the "exchange control is an instrument of repression. When he says that they will not give dollars to businesses that participated in the strike, this signifies that 80 percent of the companies would not receive dollars."

In the face of such an "instrument of repression," those Venezuelans wanting to resist or subvert the political order had to find an alternative monetary framework for surviving, and as all of the foregoing implies, they found cryptocurrency. Caracas-based programmer John Villar told Reuters in late 2014:

"Bitcoin is a way of rebelling against the system."

That said, there's no indication that cryptocurrency is being used to fund actual opposition groups, while Villar went on to tell Business Insider in December 2017 that cryptocurrency in Venezuela "is not a matter of politics. This is a matter of survival." However, when Bitcoin is being accepted by Venezuelan businesses (and even being used to pay employees in a few cases), and when business has often been 'the opposition' in Venezuela in recent years, there's undoubtedly an underlying political edge to their use of crypto.

The future

As the situation in Venezuela worsens, with President Maduro's approval rating continuing its plunge from 55 percent in 2013 to around 20 percent today, it's only likely that more businesses and individuals will turn to cryptocurrency. Since the beginning of this year, there has already been a 344.6 percent rise in the number of Bitcoin traded for Venezuelan bolívars on the LocalBitcoins exchange, a percentage made even more impressive by the fact that it disregards other exchanges and other cryptocurrencies — such as Dash. Seeing as how the recent devaluation of the bolívar is unlikely to make a positive difference in Venezuela's economic situation, it's highly probable that this situation will deteriorate further, leaving people with even fewer options for survival. In turn, cryptocurrencies will be traded even more heavily.

Although it's likely that much of the Venezuelan trade in cryptocurrencies up until now has come from the country's middle classes — i.e., the 60 percent of the population with internet access, as well as those who know how to mine and program — the near future may see a wider distribution of people involving themselves in crypto. There's little question that Dash-, Bitcoin- and other crypto-evangelists will continue doggedly raising awareness among Venezuelans about the benefits of cryptocurrencies. Their efforts have been highly fruitful so far, providing an important model that they and other currencies can follow if — or when — another nation is unfortunate enough to experience something akin to Venezuela's crisis. And for as long as the Venezuelan government continues to impose capital controls (which have been one of the main factors in hyperinflation, among others), there's nothing to suggest they won't continue bearing fruit in the coming months and years. ⚡

24/7 SUPPORT

SECURITY

BITCOIN

ETHEREUM

FREE TRANSFERS

ERC20

EXCHANGE

WEB WALLET

25+ CURRENCIES

TOP UP PHONE

TRON

DASH

13 LANGUAGES

BITCOIN CASH

ANDROID



FWT LOYALTY

iOS

ZCASH

Freewallet

www.freewallet.org





BUSINESS

WHICH COUNTRIES

ARE BEST TO START BLOCKCHAIN PROJECTS?

Bitcoin's boom has spawned more than just a digital currency revolution. Companies across the globe have explored the potential of blockchain technology in a range of different spheres, including cars, phones, and a multitude of disruptive alternatives in banking, government and as well as shipping.

Also, it is not only the small startups that are trying to push blockchain innovation, but rather conglomerates as big as Amazon, Alibaba and Microsoft. However, these companies are still trying to negotiate an ever-expanding regulatory framework that is growing at different rates across different states.

Many different companies began springing up within the cryptocurrency ecosystem, usually attached to a capital raising ICO, which left many regulators wondering how to control this decentralized, crowd-funded form of capital raising.

From the SEC to the Chinese government's hard clampdown on ICOs to Malta and Switzerland competing to be the premier destination for fintech and

blockchain, different nations have taken widely different views on how to regulate, quash or support blockchain startups.

Thus, because of the global nature of blockchain products, it is unnecessary to worry about a regional customer, but rather it is important for blockchain projects to examine the legislation, the atmosphere and approach from the community, fees, and a myriad of other factors in different countries to see which will aid them in realizing their outcomes.

Cryptocurrency havens

The different approaches by governments and regulators have created what has sometimes been referred to as 'cryptocurrency havens', as nations look to try to attract fintech and blockchain projects to their shores in the hope of using a potential financial revolution to boost their own agendas.

A lot of these havens are being created in smaller nations. Places like Switzerland, Malta and Bermuda are actively adjusting and creating legislation to welcome blockchain projects.

On the flipside, there are countries that are trying to discourage and scare away of as many blockchain projects as they can, and it has been successful in many cases. One of the most notable examples is China, where the ban of ICOs and access to exchanges has forced these startups and digital currency exchanges to go elsewhere.

For example, one of the globe's biggest exchanges, Huobi, which was forced to leave China in September last year because of legislative changes. Since then, the exchange has looked to open offices in a number of other different locations, such as Australia, the United States, Singapore, South Korea, the United Kingdom and others.

While not all of these countries are actively supportive of cryptocurrencies, they are at least tolerant and are looking to set their rules to make it easy for companies to follow the legislation.

Switzerland — Crypto Valley

The U.S. may have Silicon Valley, but Switzerland wants to have the 2.0 version — Crypto Valley — in the small town of Zug. However, even before Zug started turning its full attention to cryptocurrency, Switzerland was working toward becoming a fintech sandbox.

In July last year, Switzerland put in place options for companies that accumulated around \$1 million in third-party funds to test out their innovative financial technology ideas without the usual regulation surrounding finance and digital currency.

They also said that banking licenses would be re-evaluated in order to allow these companies earning less than \$1 million to obtain licenses for depositing and allowing crowdfunding donations to be withdrawn over a period of 60 days rather than the previous seven days.

In the year since Switzerland started making life easier for blockchain and fintech companies, there has been a big boom in these innovative projects.

Stephen Meyer, a legal professional and Ph.D. Candidate in Blockchain & Law living in Zurich Switzerland, has seen both the advantages and disadvantages of launching a blockchain project in the small European nation:

"Switzerland has a very clear regulatory situation based on the Swiss financial authority FINMA's ICO Guidance of February 2018. Also, one of the major benefits is the possibility of receiving an individual pre-ruling by FINMA. Every crypto team can describe its project, send it to FINMA and will usually receive within 4-8 weeks a clear statement whether regulatory provisions are applicable."

"Instead of creating new blockchain-related legislation, which — as with every new legislation — leads to uncertainty regarding the specific application, Switzerland applies the existing regulatory framework, but with a flexible and principle-based approach."

Importance of a regulatory framework

While regulations are often frowned upon by those who have spent some time in the blockchain space, they are a necessary part of the evolution of the technology. Some companies have gone from having free rein — building their company up with no restrictions — only for the legislature to catch up.

However, some companies are appreciative of building their blockchain company in a space that is regulated and has easily defined boundaries to follow.

One of the first countries to begin building a regulatory framework for blockchain projects — and a crypto-friendly framework — was Switzerland.



ICOs are also nothing new in Switzerland, as they have seen the Ethereum Token Generation Event back in 2014 and have been gaining experience ever since.

“FINMA and the tax authorities have longstanding experience with crypto projects since the launch of the Ethereum TGE in 2014. In the meanwhile, they have handled a substantial number of ICO as well as more and more other crypto projects as exchanges and funds. Therefore, as a crypto team, you do not have to explain blockchain technology to these authorities, and they usually are up-do-date,” said Meyer.

Valentin Botteron, Swiss attorney currently visiting scholar at Columbia Law School in New York, completing a Ph.D. in Antitrust as well as research in blockchain and smart contract-related legal matters. He had similarly positive things to say about Switzerland’s approach:

“Switzerland has a very tech-friendly approach on regulating the fintech companies, ICOs and cryptocurrencies. The Government has already stated several times that it aims to make Switzerland a regulatory-friendly place for blockchain companies. Switzerland hosts several blockchain companies and associations who advocates for a healthy regulation of the technology.

“The parliament is well aware of the phenomenon and urges the government not to miss the opportunity to be amongst the first countries to attract blockchain-related actors. The political stability of Switzerland makes it an ideal place to develop business in general. Besides the economic actors, several scholars conduct research in economics and law about blockchain in Swiss universities.”

With a look at what Switzerland is doing, and then seeing how other nations are trying to replicate and advance it, there is this feeling of competition. As Botteron states, Switzerland’s parliament is pushing the government to be the leader in blockchain growth.

ledger technology (DLT) as of March 12, which included three crypto-positive bills. These include: Malta Digital Innovation Authority (MDIA) Act, Innovative Technology Arrangements and Services (ITAS) Act, and the Virtual Currencies (VC) Act.

The result of these positive pieces of legislation has seen a flood of interest in Malta as a premier destination for blockchain and ICOs.

Other exchanges — including OKEx — have moved there, as well as Polish exchange BitBay. The positive regulations for virtual currencies are clearly being gratefully accepted, but even the smaller blockchain projects are cashing in too.

Jonathan Galea, a graduated lawyer in Malta, president of Bitmalta and managing director at Blockchain Advisory, spoke to Cointelegraph about what makes Malta different from other countries.

“What distinguishes Malta from the rest of other jurisdictions when it comes to blockchain and cryptocurrencies — put simply — is the fact that the government, the opposition and all regulatory authorities are pulling the same rope together, chasing one single vision: making Malta one of the leading countries in the space. That, coupled with the ease of accessibility to top officials in relevant positions that are there to promote and aid business activities rather than to hinder it, makes Malta an attractive destination for all blockchain-related matters.

“Of course, one cannot not mention the regulatory framework that has been devised in the span of less than two years, following various consultations with various important stakeholders in the crypto sphere — both locally and internationally. The creation of the first ad-hoc, comprehensive framework in the world, catering for the legal, technical and financial aspects of blockchain and crypto-related activities, grants absolute legal certainty and peace of mind to those wishing to operate within a completely regulated ecosphere — which, at the same time, promotes rather than restricts business growth.”

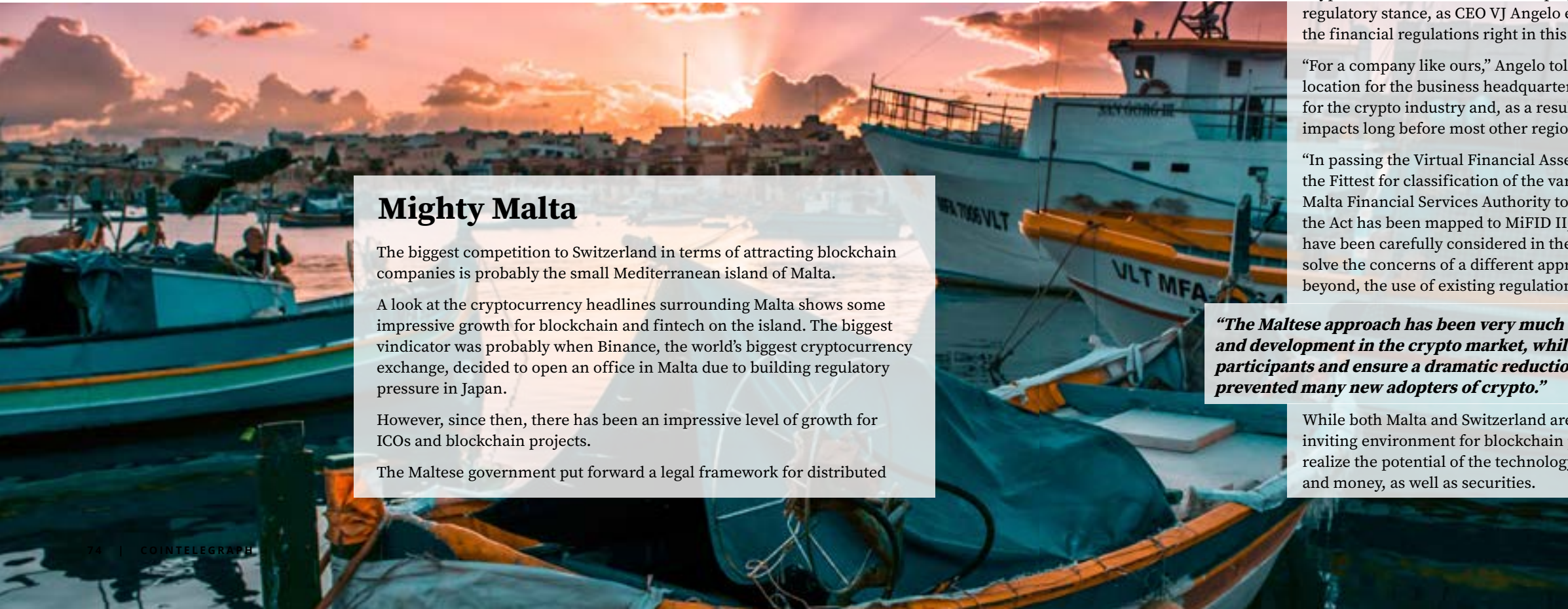
Cryptoindex is such a blockchain project that has benefited from the Maltese regulatory stance, as CEO VJ Angelo explains just why it is important to get the financial regulations right in this space.

“For a company like ours,” Angelo told Cointelegraph. “We chose Malta as its location for the business headquarters because it became an early incubator for the crypto industry and, as a result, has been looking at its long-term impacts long before most other regions.

“In passing the Virtual Financial Assets Act in June of this year and creating the Fittest for classification of the various cryptocurrencies and tokens, the Malta Financial Services Authority took the lead in Europe. A great deal of the Act has been mapped to MiFID II, meaning the Europe-wide regulations have been carefully considered in their new laws. While it does not entirely solve the concerns of a different approach by other regulators in Europe and beyond, the use of existing regulation does mitigate some of the risk.

“The Maltese approach has been very much one of fostering all the opportunities for growth and development in the crypto market, while putting protections in place to cover ICO participants and ensure a dramatic reduction in the stories of fraud and scams that have prevented many new adopters of crypto.”

While both Malta and Switzerland are striving to make the most open and inviting environment for blockchain projects, there are other nations that realize the potential of the technology, but have strict laws governing finance and money, as well as securities.



Mighty Malta

The biggest competition to Switzerland in terms of attracting blockchain companies is probably the small Mediterranean island of Malta.

A look at the cryptocurrency headlines surrounding Malta shows some impressive growth for blockchain and fintech on the island. The biggest vindicator was probably when Binance, the world’s biggest cryptocurrency exchange, decided to open an office in Malta due to building regulatory pressure in Japan.

However, since then, there has been an impressive level of growth for ICOs and blockchain projects.

The Maltese government put forward a legal framework for distributed

Freedom, liberty and securities in the U.S.

The U.S. is a major player in both the cryptocurrency and blockchain ecosystems, with the majority of ICO projects from the last 18 months originating in the U.S. — 16 percent of all global ICOs.

However, the U.S. has been fighting a big battle with ICOs thanks to its Securities Exchange Commission's definition of what a newly founded virtual currency can be classified as.

The SEC, however, found that, in a major precedent-setting decision, that the decentralized autonomous organization (DAO) tokens that were issued in 2016 were securities. This essentially lumped the majority of ICO projects as securities and put them under the scrutiny of the regulator.

But that does not mean that the U.S. is closed off to ICOs and blockchain projects, rather there are some harder hoops to jump through — especially with the division of state and federal law.

Jack Keating, an attorney in New York and a former regulator at the Financial Industry Regulatory Authority (FINRA), spoke to Cointelegraph about the challenges that ICOs and blockchain projects face in the U.S., and particularly in New York State.

There is a path for ICOs to function in a popular ICO country, but the regulatory hoops go against the core values that the crypto community holds dear.

“Another challenge is banking solutions for crypto companies. Similar to how marijuana companies are blackballed by most financial institutions, many U.S. banks have a policy to not open accounts for crypto businesses. Because a bank account offers so many fundamental services to running a company, simply opening a checking account can be extremely difficult. Of late, Metropolitan Commercial Bank has professed its leadership in the space. However, they face heavy scrutiny from U.S. regulators, which challenges their sustainability.”

Keating concluded that it may not be the most welcoming place for blockchain, but the U.S. seems willing to foster the technology, and because of the hunger, it is worth it.

“In my opinion there is a lot of support for crypto and ICOs coming from the government. Whether they see value in it or are willing to foster the technology is hard to say. The lack of an outright ban is encouraging. It's worth the pressure. The U.S. has the best investor base and the best courts in the world.”

“The biggest problem with ICOs is that many of them are being done in clear violation of U.S. securities laws. Whether the issuers are unaware or agnostic to the potential consequences of issues unregistered securities, without a exemption from Section 5 registration. Many ICO issuers have ignored the requirements of the raising capital in the U.S.

“[For] ICOs that do comply with the SEC Rules and U.S. securities laws, investment is often limited to accredited investors. This goes against one of the core tenets of many Bitcoin and blockchain evangelists, that being that this technology can democratize wealth. Unfortunately, when investment is limited to accredited investors, the rich get richer and the non-millionaires are left on the sideline.”

The United Kingdom's definition of an ICO token

With the likes of Switzerland and Malta setting firm and understandable definitions for crypto, ICOs and blockchain, the U.S. — as well as the United Kingdom — have far more ambiguous regulations about different aspects of the ecosystem, as they continue to decide how much, or little, they need to step in.

Romal Almazo, the cryptocurrency lead and principal consultant at CAPCO — a global business and technology consultancy in the U.K. — explained to Cointelegraph how the law is working around cryptocurrencies and ICOs in Great Britain.

“In the U.K., the FCA [Financial Conduct Authority] still does not regard cryptocurrencies to be a currency or a commodity under MiFID II. They do, however, admit that some firms will be regulated where they offer products or service which are caught under existing financial regulations — e.g., Bitcoin futures. Where firms offer ICO tokens, they also concede that some firms might be issuing a regulated security. For a token to be regulated as a security under the U.S. Securities Act of 1933, a firm should look to the ‘Howey test’ and the ‘U.S. Person’ test.

“Looking forward, there are still huge problems on agreeing what crypto assets are and how they behave. Is it an equity, commodity, currency, utility asset or some kind of hybrid? Until this taxonomy becomes clearer and universally agreed upon — which is unlikely in the near-term — competitive advantages between states and jurisdictions will emerge. For example, we are already seeing Malta <...> leading the pack by offering guidance and regulation. They want to create a blockchain island of innovation. The U.K. is still looking promising, but we are still seeing the majority of ICOs in the U.K. set-up through Malta, Gibraltar, Liechtenstein or Switzerland.”

Budding smaller nations

Others — such as Bermuda, Estonia and Liechtenstein — are also doing their best to wrest some crypto authority with their own friendly regulations.

Bermuda has recently — on July 2 — put forward plans to make amendments to the Banking Act in order to establish a new class of banks that offers services to local fintech and blockchain organizations.

Estonia is one of the countries that has actually been trying to make blockchain feel welcome for some time now. The government even went as far as to digitize its services by using blockchain technology. This appreciation of the potential of blockchain has made it easier for startups to build their own innovative projects.

“With most regulators making some form of comment or direction for the present looking to the future of crypto, there are few actually enacting any laws. The crypto market is in the midst of an important transition. The likes of the SEC have made sweeping statements — catching the whole market in a difficult position, as far as the U.S. is concerned. Others merely state they don't currently regulate crypto but will be announcing something soon, like the U.K.'s FCA.”

Still space to pick and choose

It is clear that there is certainly no global standard, which allows companies to pick and choose the places that are most suited for them.

The G20 might be looking to gathering data about cryptocurrencies in order to potentially put forward a united force for regulations, but it sounds like it still has a long way to go — and is not even guaranteed that everyone will agree.

However, what is clear, is that there are countries that are striving to let Blockchain flourish. A few islands, like Malta and Bermuda are changing their legislation to make their country more attractive to fintech companies, and other European Nations, like Switzerland and Estonia believe that they have the right laws to protect against the negatives of crypto while still encouraging its growth.

The UK and the USA have adapted their rules to encompass cryptocurrency into standing legislation, and while it seems quite stringent at the moment, it is a working system. In the end, there is no one place that is offering total freedom for blockchain projects, but along the spectrum, there is a lot of options for innovation. 🚀

HOW BIG FOUR AUDITORS DELVE INTO BLOCKCHAIN:

PwC, Deloitte, EY and KPMG Approaches Compared

PricewaterhouseCoopers (PwC), Deloitte, Ernst & Young (EY) and KPMG, better known as the “Big Four” auditors, all have established solid long-term blockchain roadmaps to remain relevant in the cryptocurrency and blockchain space.

The four professional services conglomerates, which combined employ over a million individuals, have different roadmaps and perception of the future of the blockchain industry. Deloitte for instance, the biggest auditor out of the four with an annual revenue of around \$43.2 billion, has stated that the blockchain sector is close to seeing a breakthrough with the technology.

“Ultimately, [blockchain is] more of a business model enabler than a technology...for legacy organizations...we’re starting to see a change in approach toward blockchain. Executives in these organizations are moving away from the pure platform view of ‘What is it?...let’s find a use case’ toward development of more sensible, pragmatic business ecosystem disruption.”

- Deloitte’s 2018 blockchain survey, published August 27

In contrast, PwC, which has been directly involved in the cryptocurrency market through its investment in VeChain (VET) since May 4, a China-based Internet-of-Things (IoT) blockchain network, expressed its concerns over the uncertainty in blockchain regulation.

PwC blockchain head Steve Davies explained that a large number of conglomerates and startups are exploring ways to integrate the blockchain at a commercial level. But, regardless of the increase in demand for the blockchain, regulatory hurdles in integrating the decentralized technology has limited companies from utilizing the blockchain to process information:

“Businesses tell us that they don’t want to be left behind by blockchain, even if at this early stage of its development, concerns on trust and regulation remain. Blockchain by its very definition should engender trust. But in reality, companies confront trust issues at nearly every turn.”

Generally, the Big Four have reaffirmed in recent reports that the interest in blockchain technology is rising rapidly, especially amongst high profile conglomerates such as Microsoft, IBM, JPMorgan, and Goldman Sachs.

However, many experts including US Securities and Exchange Commission (SEC) commissioner Hester Peirce believe that over-regulation in an industry that is still at its infancy could limit a wide range of developments, ultimately damaging the growth of the crypto and blockchain space.

During a speech delivered on September 12, commissioner Peirce said:

“The Commission should not default to a demand that the crypto markets be subject to comprehensive government regulation as a precondition to allowing products linked to those markets to be traded in markets that we regulate.”

While the Big Four acknowledge the lack of regulatory certainty in the space, the four conglomerates have made significant efforts in understanding the market to assist large corporations to integrate the emerging technology.



PwC: investment in VeChain, 1,000 staff in the blockchain, targeting the Swiss banking space

Despite its concerns in regard to regulatory uncertainty in the market, PwC has been the most active professional services conglomerate in the crypto and blockchain space.

Most recently, PwC announced that through a program called “Digital Accelerators Program,” more than 1,000 employees of the company will be trained in the area of blockchain and cryptocurrency.

Over the next two years, Sarah McEneaney, digital talent leader at PwC and head of Digital Accelerators, stated that to meet the increasing demand for blockchain by its clients and competitors, the firm decided to engage in a major initiative to solidify its position at the forefront of blockchain development:

“It just seems table stakes at this point that people should have more technology skills. It’s needed for us to remain competitive and to be responsive for what our clients are also going through...our clients are looking for us to do things more digitally and control the cost of what we’re doing.”

As a professional services conglomerate, the core business model of PwC revolves around its auditing and consulting services that are provided to high profile corporations in major industries like finance, technology and manufacturing.

Hence, in her statement, McEneaney acknowledged that a large portion of its client base that is composed of large-scale corporations have started to demonstrate big interest and demand for the technology.

It is possible that PwC criticized the over-regulation of the blockchain space in its recently published study because its clients and large corporations in various industries are unable to integrate blockchain technology at a meaningful capacity to demonstrate the potential of the technology.

Still, Pierre-Edouard Wahl, the head of blockchain digital services at PwC Switzerland, told Cointelegraph in an exclusive interview that the corporation is targeting the Swiss banking and finance sector with blockchain-based products.

In July 2018, SIX, the main stock exchange of Switzerland, announced that it will launch a fully regulated cryptocurrency exchange by 2019. The public release of the finalized plan of SIX was met with optimism in the global cryptocurrency market, as it was the first announcement of a major stock exchange to be directly involved in the asset class. In the following month, ICE / NYSE, Starbucks, and Microsoft launched a regulated cryptocurrency trading platform Bakkt.

According to McEneaney, blockchain technology could negatively impact the current business model of major banks and financial institutions in the short-term, as it eliminates third-party service providers and mediators in the process of settling payments.

In the long-term, however, McEneaney stated that blockchain will enable banks, as institutions, to adopt the technology. This is similar to how Ripple has convinced banks like BBVA and Banco Santander to utilize the blockchain in processing cross-border payments, the technology may improve the existing solutions of banks.

“I actually think it will be an enabler. Yes, it might hurt their existing business, but that is often the case with the new technologies: It’s either you adopt them and you think differently about how those technologies are going to actually offer new solutions — as well as improve the existing solutions — or then you just look at the improvements, and we are all racing to the bottom, because there are less and less margins for everyone.”

PwC invested in VeChain, a major cryptocurrency with a market valuation of \$711 million in May with the vision of utilizing the IoT-focused blockchain to enable the existing infrastructures of large-scale partner conglomerates of PwC.

Raymund Chao, PwC Asia Pacific and Greater China Chairman, said at the time:

“We are glad to establish a deeper relationship with VeChain, which aims to build a trusted and distributed business ecosystem to help address long-standing challenges in supply chain management, food trust and anti-counterfeiting areas. VeChain’s mission aligns with PwC’s purpose of solving important problems and building trust in society.”



Deloitte: focusing on the technical development and implementation of blockchain technology

Since 2016, Deloitte has been fairly active in the blockchain and cryptocurrency space, leading various initiatives to promote the usage of blockchain technology.

Two years ago, the auditor deployed one of the first Bitcoin ATMs in Toronto, Canada, to demonstrate the possibility of exchanging crypto-to-fiat with ease, without the necessity of strict Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures.

Since then, Deloitte has taken a comprehensive approach towards blockchain development and integration, by creating a division within the conglomerate called “Deloitte Blockchain Lab” that is wholly dedicated to blockchain research and development.

Through its blockchain lab, Deloitte has worked with its partner companies to identify major obstacles firms face in adopting the technology and establish ways to leverage the technology to improve the existing infrastructure of corporations.

PwC and Deloitte have offered contrasting reports on the current state of the blockchain space. On August 28, in a survey report entitled “2018 global blockchain survey Breaking blockchain open” Deloitte stated that blockchain technology is getting closer to a breakout moment. Meanwhile, in a study entitled “Regulatory uncertainty and trust are barriers to blockchain adoption amongst businesses” released on the same day on August 28, PwC noted that regulatory uncertainty still remains as a main obstacle in blockchain development.

Deloitte identified scalability as the main problem of the blockchain, rather than regulatory uncertainty in the market, a viewpoint that has also been shared by different experts in the industry.

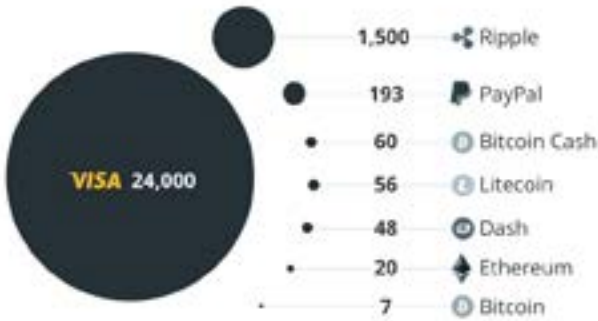
Public blockchain networks need a lot of development work to handle the infrastructure of large conglomerates. Bitcoin is processing around 7 transactions per second while Ethereum has been doing around 20. In contrast, Uber processes 12 transactions/sec, Paypal settles hundreds of transactions/sec, Visa processes 24,000 transactions/sec and IoT networks process hundreds of thousands of transactions/sec.

As such, in order for a major supply chain, distributor or an insurance company to adopt blockchain, it will have to process at least tens of thousands of transactions per second.

“One major reason: As a means of processing transactions, blockchain-based systems are comparatively slow. Blockchain’s sluggish transaction speed is a major concern for enterprises that depend on high-performance legacy transaction processing systems. A lack of standards and interoperability between various blockchain platforms and solutions is another challenge.”

- Deloitte study “Blockchain and the five vectors of progress”

AVERAGE NUMBER OF TRANSACTIONS PER SECOND





Ernst & Young (EY): Building tools to help companies identify risks in the blockchain

In contrast to PwC and Deloitte, EY has focused most its efforts on legitimizing the blockchain, by identifying risks in using blockchain-based platforms and crypto-related models, like initial coin offerings (ICO).

In April 2018, the firm released EY Blockchain Analyzer, a technology “that is designed to facilitate EY audit teams in gathering an organization’s entire transaction data from multiple blockchain ledgers.”

Similar to block explorers including Blockchain.info and Etherscan, EY Blockchain Analyzer is able to extract data from the blockchain to assist companies to audit various types of information processed on the network.

Paul Brody, EY Global Innovation Blockchain Leader, stated that every large-scale conglomerate that attempts to integrate the blockchain as a main component of its infrastructure needs necessary tools to test blockchain-based smart contracts and business contracts, and without established auditing tools, it is difficult to convince corporations to adopt blockchain technology at a big scale:

“Understanding exchanges and cryptocurrencies is the first step in our ability to develop tools to test various blockchain-based business contracts. These technologies lay the foundation for automated audit tests of blockchain assets, liabilities, equities and smart contracts. EY Blockchain Analyzer will be utilized by the auditor to analyze transactions on a blockchain and help provide insight to the finance function.”

The company has also acknowledged developers and builders in the cryptocurrency market, by awarding entrepreneurs in the cryptocurrency sector with the EY Entrepreneur of the Year awards.

Thus, in 2017, Bitcoin ATM manufacturer that deployed more than 180 cryptocurrency ATMs in the US were selected as the finalists by the EY Entrepreneur of the Year awards.

In the months to come, EY is expected to continue its work as a risk identifier in the blockchain and cryptocurrency space, developing various tools to render the experience of using the blockchain seamless for companies.

Most recently, EY started to analyze the public cryptocurrency exchange market, identifying risks involved in ICOs and the vulnerability of token sales to hacking attempts. Over the years, many ICOs lost funds in security breaches, the recent case happened in July, when KickICO lost more than \$8 million in a hacking attack.



KPMG: auditing, taxing and analyzing blockchain integration

KPMG also announced new leadership in its U.S. Blockchain initiatives to drive and expand the firm's blockchain strategy into tax, audit, advisory, and industries. In the months to come, the conglomerate emphasized that with the appointment of Arun Ghosh as the firm's U.S. Blockchain leader, and David Jarczyk and Erich Braun as the U.S. Blockchain Tax and Audit leaders, it will work with partner companies to create comprehensive blockchain strategies and guidance.

The decision of KPMG to pivot its blockchain business to risk assessment and audit comes after the release of its report called “The Pulse of Fintech,” which revealed that the first half of 2018 has exceeded the total investment in blockchain technology made in 2017.

Overall, all Big Four companies have recognized the growing demand for the blockchain and crypto. Interestingly, the four conglomerates are taking different approaches to facilitate the rapidly increasing interest in the blockchain space. PwC is taking a more aggressive approach to directly integrate the blockchain into existing infrastructures of conglomerates and Deloitte is focused on improving the technical aspects of the blockchain. In contrast, KPMG and EY have allocated most of their resources to analyze risk in implementing the technology and creating tools that can ease the process of using the blockchain.

It is positive that conglomerates have identified regulatory and technical risks that come with the blockchain, which will help companies understand the potential of the blockchain in a more realistic manner. Still, as Deloitte and PwC firmly stated, it is important for major markets like the US and Japan to provide regulatory certainty in the development of blockchain technology to increase. ⚡



A BRIEF HISTORY OF BITCOIN

While it may seem like Bitcoin has become entrenched in many lives as an absolute can't-live-without, since it was first whispered around the cryptography tables it has been just 10 years.



TOP PEOPLE IN BLOCKCHAIN

top.cointelegraph.com



Co-founder of Ethereum
Vitalik Buterin

@VitalikButerin

The genius behind the world's second most valuable cryptocurrency t Ethereum – first learned about cryptocurrencies from his father. Af Bitcoin Magazine in 2011, Buterin spent two years learning Blockcha potential, and the applications it had to offer. The Ethereum white published in late 2013. Buterin currently serves as the Chief Scien Foundation and leads Ethereum’s research team, which maintains the technology of the cryptocurrency and works on future versions of th protocol.



Bitcoin Evangelist & Author of 'Mastering Bitcoin'
Andreas M. Antonopoulos

@aantonop

One of the world’s greatest advocates of Bitcoin, Blockchain techno principles of decentralization, Antonopoulos is a security and dist expert, a widely published author of books, articles, and blog post cryptocurrencies, a frequent speaker at technology and security con worldwide, a coder, and an entrepreneur. Antonopoulos offers strate to a small number of cryptocurrency companies, as well as offering testimony as an expert in the security, technical details and use o



Creator of Litecoin
Charlie Lee

@SatoshiLite

Primarily known in the crypto world as the creator of Litecoin, Lee adopters of Bitcoin – entered the crypto sphere by getting into Bit sees Litecoin as the cryptocurrency best suited for smaller, lightw like online retail shopping, while Bitcoin is the currency for more transactions like international payments.



Creator & Designer of Bit Gold
Nick Szabo
@NickSzabo4

A major influencer in Bitcoin, Szabo’s expertise with cryptocurrency started back in 1998 with the creation of the BitGold proposal, the predecessor of Bitcoin. People have speculated that Szabo is Satoshi Nakamoto, the anonymous creator of Bitcoin, although Szabo has repeatedly denied the claim. Szabo is still considered the ‘smart contracts,’ a term usually associated with Ethereum, and he continues to contribute his technical knowledge and commentary in the crypto industry.



President & CEO of The Tapscott Group, Inc.
Don Tapscott
@dtapscott

Tapscott has become an increasingly well-known figure in the cryptocurrency industry, having been one of the foremost the impact of technology for decades. He is also one of the influential living theorists about business and society. Identified as the most influential management thinker in the Thinkers50 and Forbes. He is the author or co-author of 1 books about new technologies and new media in business ar including ‘Wikinomics’ (2006) and ‘The Digital Economy’ (Blockchain Revolution’ (2014)), has made him one of the n Blockchain governance references and proponents.



Co-founder & CEO of Coinbase
Brian Armstrong
@brian_armstrong

As an early investor in Bitcoin, Pierce is a venture cap entrepreneur with an extensive track record of founding, advising and investing in disruptive businesses. He pioneered the market currency in games, and was one of the largest investors in the Bitcoin crowdsale. Pierce has invested in over 30 companies in the Bitcoin ecosystem, participated in over 100 projects, and helped raise over 1 million US for companies he was involved in. Pierce has also been a guest lecturer at the Milken Global Conference, Singularity University, Stanford University, the University of Southern California, and the University of California, Los Angeles.



Founder & CEO of ShapeShift.io
Erik Voorhees
@ErikVoorhees

Before he became an entrepreneur, Voorhees was a blogger libertarian ideas, authoring long thoughts about the natu and politics and the role of cryptocurrencies in this bal industry and mainstream media. Active in the industry aln base, Voorhees’s greatest claim to fame is arguably his project – the crypto exchange platform ShapeShift – and t Bitcoin gambling game SatoshiDice.



Co-founder of Blockchain Capital
Brock Pierce
@brockpierce

As an early investor in Bitcoin, Pierce is a venture capitalist and entrepreneur with an extensive track record of founding, advising and investing in disruptive businesses. He pioneered the market currency in games, and was one of the largest investors in the Bitcoin crowdsale. Pierce has invested in over 30 companies in the Bitcoin ecosystem, participated in over 100 projects, and helped raise over \$200 million US for companies he was involved in. Pierce has also been a guest lecturer at the Milken Global Conference, Singularity University, Stanford University, the University of Southern California, and the University of California, Los Angeles.



Cc-founder & CEO of CivicKey
Vinny Lingham
@VinnyLingham

Lingham’s journey in Blockchain began with his startup Gy and offering Amazon purchases using Bitcoin. He is a prominent commentator on Bitcoin and Blockchain, and is the recipie numerous awards, including Top Young ICT Entrepreneur in (2006) and Top 500 CEO’s in the World by Richtopia (2015) previously a finalist for Men’s Health Best Man (2009) and Personality of the Year in South Africa (2008). He is als the world’s great advisors.



Founder & CEO of Digital Currency Group
Barry Silbert
@barrysilbert

Known as a founder of The Digital Currency Group, Silbert is a crypto investor and a well-known proponent of the rival Ethereum chain, Ethereum Classic. He is a frequent speaker at conferences on the topic of trading illiquid assets and has appeared in many leading publications, including The Wall Street Journal, Financial Times, New York Times, USA Today, BusinessWeek, Forbes, Fortune, and many others. In 2013, he started as an angel investor in Bitcoin companies, and he currently is one of the most influential figures and newsmakers in the crypto world industries.



Host of "Unchained" and "Unconfirmed" podcasts
Laura Shin
@laurashin

Shin is best known for her work as senior editor of Forbe cryptocurrency and Blockchain coverage. She is also the h publication’s Blockchain-focused podcast – Unchained – ar the Forbes e-book, “The Millennial Game Plan: Career And Success In Today’s World” (2014). Her active p the crypto industry and her expert knowledges in this spk one of the most influential persons in the crypto world.



Co-founder & CEO of the Blockchain Research Institute

Alex Tapscott

@alexapscott

Tapscott is a prominent writer, speaker, investor and advisor interested in emerging new technologies, such as Blockchain and cryptocurrencies, and their influence on business, society, and government. He is the co-author of the critically acclaimed #1 non-fiction best-seller, “Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money Business and the World” (2014), which has been translated into over 15 languages. Tapscott co-convened a meeting of Blockchain stakeholders to discuss the Blockchain ecosystem and by the worldwide community. currently sits on the Advisory Board to Elections Canada. Tapscott has become a leading voice on cryptocurrency and Blockchain technologies.



Bitcoin Angel Investor & Bitcoin Evangelist

Roger Ver

@rogerkver

Ver is famous for being one of the first investors in the Blockchain industry, financing the growth of many of its biggest names. He is a popular news and wallet resource Bitcoin.com, and became a proponent of Bitcoin Cash in 2017. Ver is a legend in the Bitcoin community, named as the “Bitcoin Jesus” for his tireless the virtual currency and for his investments in numerous startups. He called himself self-educated enthusiast who free time on studying economics and moral philosophy.



Co-founder & Director of Bitmain Technologies, Ltd.

Jihan Wu

@JihanWu

Wu is a Chinese entrepreneur, financial analyst, and Bitcoin evangelist. He is a major proponent of Bitcoin Cash, having previously supported Bitcoin network scaling solutions such as Bitcoin Unlimited. He believes that Bitcoin and Blockchain technologies are now significantly changing modern world and people’s way of life. Wuis claimed to be one of the most controversial names in crypto industry meanwhile he is the most influential proponent of cryptocurrencies and Blockchain technologies worldwide.



Co-founder of Netscape Communications & Co-founder of LoudCloud

Marc Andreessen

@pmarca

Andreessen is a co-founder of Silicon Valley venture capital firm Andreessen Horowitz, contributing funding to multiple Blockchain industry startups since 2013. He has a background in revolutionary technology, co-creating Mosaic and Netscape, two of the Internet’s first browsers. Andreessen is the recipient of numerous awards related to the Internet Industry, including Vanity Fair’s 2011 New Establishment List, CNET’s 2011 most influential investors list, the 2012 Forbes Midas List of Tech’s Top Investors, and was one of five Internet and Web pioneers awarded the inaugural Queen Elizabeth Prize for Engineering in 2013. He was also named in the 2012 Time100, an annual list of the 100 most influential people in the world assembled by Time Magazine.



Chief Scientist at Bitcoin Foundation & Lead Developer of Bitcoin Core

Gavin Andresen

@gavinandresen

Andresen (formerly known as Gavin Bell) is a well-known figure in the Bitcoin community. A brilliant software engineer, he previously was the co-author of the Bitcoin whitepaper. He is the current Chief Scientist of the Bitcoin Foundation, a Core developer. His technical involvement with Bitcoin started when he discovered Bitcoin, quickly recognising the importance of it. Andresen acts as arbiter and architect for the Bitcoin and helps coordinate improvements to the core Bitcoin software and the worldwide community.



Co-founder & President of Blockstream

Adam Back

@adam3us

Back is a cryptographer and one of the founding fathers of cryptocurrencies, developing Hashcash in 1997. He has been a reference source in Bitcoin development, going on to co-found Blockchain tech company Blockstream in 2014. Back’s work in the Bitcoin community, named as the “Bitcoin Jesus” for his tireless the virtual currency and for his investments in numerous startups. He called himself self-educated enthusiast who free time on studying economics and moral philosophy.



President of Crypto Valley Association & Founder of Bussmann Advisory

Oliver T. Bussmann

@obussmann

Bussmann is a globally recognized technology thought leader of large-scale transformation at multinational organizations. He is the recipient of numerous awards, named COO/CTO of the year by Financial Times, Wall Street Journal, European CIO of the Year by INSEAD/CIO Magazine, and received the Elite 8 Award, which is given to the most in technology working in capital markets by Wall Street & Magazine, and has twice been included on the Financial Times’ list of innovators shaping the future of finance.



Editor-in-chief at Adamant Research

Tuur Demeester

@TuurDemeester

Demeester is an independent investor, newsletter writer, commentator. A globally-known entrepreneur and long-time cryptocurrency advocate, Demeester has maintained a heavy presence in Bitcoin and related debate online since 2013. Editor-in-chief at Adamant Research, he is well-known for his financial advice in the Blockchain industry. Before his career as an investment adviser, Demeester was actively involved in sudbury-type schools, a type of schools where students have complete responsibility for their own education, and Austrian economics.




Director of Development at Digital Currency Group

Meltem Demiros

@MeltemDem

Demiros has a diverse background in management consulting, corporate treasury, commodities trading, and supply chain management. Before joining Ethereum, he worked as research staff in the Robotics Lab at Princeton, as well as at Vision Applications, Inc and various other technology. Demiros brings a wide range of international, multi-sector experience into building Digital Currency Group’s global network. Her strategy is to focus on building and supporting Bitcoin and Blockchain companies by leveraging its insights, network, and access to capital.




Co-founder of Coinbase

Fred Ehrsam

@FEhrsam

A former Wall Street trader and writer at the Duke Journal of Economics, Ehrsam shifted his interests into the crypto industry in 2012. He co-founded Coinbase, an online payment system with the mission of making Bitcoin easy to use. Ehrsam has been named in Magazine’s 30 Under 30 Who Are Changing the World (2013) as one of Forbes 30’s 30 Under 30 (2014).




Co-founder & CEO of Bloq

Jeff Garzik

@jgarzik

Garzik is one of the first Bitcoin Core developers. A futurist, and software engineer, he currently serves as the CEO of Blockchain-for-enterprise startup Bloq and remains a vocal community member in the space on social media. He is also an advisor to several Blockchain industry companies, including Chain and BitFury.




Co-founder of Ztadium

Dinis Guarda

@dinisguarda

Guarda is globally-recognized top influencer, digital and cryptocurrency evangelist. A futurist, and software engineer, he currently serves as the CEO of Blockchain-for-enterprise startup Bloq and remains a vocal community member in the space on social media. He is also an advisor to several Blockchain industry companies, including Chain and BitFury.



Founder & Executive Chairman of Moven

Brett King

@BretKing

King is a bestselling author, an award winning speaker, and banking revolution advocate. He created the popular radio show Breaking Banks in 2013. After the show gained international attention, King launched smart banking app Moven, which has received almost \$50 million US in venture funding. King’s primary interest is in how modern technologies are disrupting business, changing behavior and influencing society.



Founder & CEO of ConsenSys

Joseph Lubin

@ethereumjoseph

Lubin is a worldwide famous distributed database entrepreneur. Before joining Ethereum, he worked as research staff in the Robotics Lab at Princeton, as well as at Vision Applications, Inc and various other technology. Demiros brings a wide range of international, multi-sector experience into building Digital Currency Group’s global network. Her strategy is to focus on building and supporting Bitcoin and Blockchain companies by leveraging its insights, network, and access to capital.




Co-founder & CEO of Chain

Adam Ludwin

@adamludwin

Ludwin rose to fame in 2016 when his startup Chain secured Visa and other major financial institutions, bringing ‘true’ blockchain to an important area of the mainstream economy. Chain continues to grow, while Ludwin has become a vocal online presence on Blockchain and cryptocurrency.



Owner, Editor & Publisher of the Digital Banking Report

Jim Marous

@JimMarous

Marous is an internationally recognized financial industry expert and influencer. Apart from his writing and publishing, he focuses on customer experience, portfolio growth, innovation, marketing strategies, channel shift and digital transformation within the services industry.



Founder & CEO of Galaxy Digital

Michael E. Novogratz

@novogratz

Novogratz was formerly a member of the board of directors of investment group LLC and Chief Investment Officer of the Fortress Investment Group LLC. He joined Fortress in 2002 after spending at Goldman Sachs, where he was elected partner in 1998. Novogratz serves as the Chairman of the Board of the Beat the Street Foundation, a non-profit organization which builds wrestling programs in New York City public schools, and is also the Honorary Chairman of the U.S. Foundation.




Co-director of CryptoCurrencies & Contracts (IC3)

Emin Gün Sirer

@el3ct4xor

Sirer is the creator of the first cryptocurrency to use a proof-of-work consensus, The Karma System. A major figure in both Bitcoin and Blockchain academic research, he has contributed his expertise to multiple projects, including Ethereum smart contracts and computer networking.



Venture Partner for Blockchain Capital LLC

Jim my Song

@jim my song

Song has contributed technical innovations to various Blockchain-related projects, including the development of Bitcoin integration with open transactions. A revered Bitcoin technologist and commentator, he has authored many influential posts and explained cryptocurrencies’ characteristics and upgrades.




Founder & President of The Digital Chamber of Commerce

Perianne Boring

@PerianneDC

Boring has been a Blockchain commentator and public speaker for several years, becoming a recognized voice in the industry. Founder of Blockchain trade association, the Chamber of D Commerce, in July 2014. She focuses on public policy, specifically centered on US regulation of Blockchain and cryptocurrencies.



Co-founder & CEO of Lightning

Elizabeth Stark

@starkness

Stark is a Blockchain entrepreneur, educator, and open internet advocate. She serves as a mentor with the Thiel Fellowship, has collaborated with companies such as Google and Mozilla, and is an Entrepreneur-in-Residence at Stanford's StartX. Stark previously taught at Stanford and Yale University about the future of the Internet. She is currently a visiting fellow at Yale's Information Society Project. Stark played an instrumental role in the Internet freedom effort that defeated SOPA/PIPA, engaging 18 million people globally.



CTO at R3

Richard G. Brown

@gendal

Brown is a major presence in banking innovation. He worked before becoming CTO of cross-bank ‘distributed ledger technology’ CEV. He also advises a number of cryptocurrency-related consensus firms, including Chromaway, an early developer of the ‘Blockchain 2.0’ platform, and Elliptic identifies illicit activity on the Blockchain.



Founder & CEO of BitFury

Valery Vavilov

@Valeryvavilov

Vavilov’s entrepreneurial experience and passion for Blockchain technology led him to found the BitFury Group in 2011. Vavilov was inspired by Blockchain technology and saw an opportunity to build technological solutions that could improve the lives of people all over the world. He focused first on the hardware solutions that would ensure security and trust in the Blockchain, leading BitFury Group to develop five generations of cutting-edge mining chips and state-of-the-art center designs. Under his leadership, the BitFury Group shifted its focus to provide custom-designed software, consulting, and advanced hardware, all while maintaining its position as a major public Blockchain security and transaction provider.




Founder of Draper Associates & Draper University

Tim Draper

@Tim Draper

Draper is a venture capital investor who has been recognized as a leading supporter of entrepreneurship with numerous awards and honors. He was listed as one of the most outstanding Harvard graduates on the Forbes Midas List, and in Worth Magazine’s 100 Most Powerful People in Finance. Draper also received the World Entrepreneur Forum’s “Entrepreneur for the World” in 2015.



Co-founder of Eyeka S.A.

Gilles Babinet

@babgi

Babinet is a French entrepreneur who has founded and managed numerous companies, specializing in the digital industry. In June 2012, Gilles was appointed French digital champion in 2012 by Fleur Pellerin, French minister of digital technologies. He worked with Neelie Kroes, European Commissioner in charge of digital technologies, as a follow up of his former position as president of the French National Digital Council.



CEO of Ripple

Brad K Garlinghouse

@bgarlinghouse

Prior to Ripple, Garlinghouse served as the CEO of file cloud service Hightail. He was also the President of Consumer Affairs at AOL from 2009 to 2012 and held various positions at Yahoo from 2009 to 2009, including Senior Vice President. He is an active member of the industry.




CEO of Mattereum

Vinay Gupta

@vashless

Gupta is a materials scientist and a senior scientist at the National Energy Harvesting department of the National Physical Laboratory, India. Gupta has co-founded and serves as Chairman at TripFactor, an online travel agency. He also serves as Director at Flight Raja Travels Private Limited. His award list includes the NASI-Scopus Award for young scientists in 2008, the National Academy of Sciences, India and Elsevier (2011), the Swarup Bhatnagar Prize—one of the highest Indian science awards in 2013, and The Council of Scientific and Industrial Research (2017).



General Manager at IBM Blockchain

Marie Wiecek

@mwiecek

Wiecek has been working for IBM for over 30 years, experiencing a variety of technical and executive roles in IBM’s hardware and services divisions. She is passionate about innovation and building new businesses. Wiecek is currently General Manager of IBM Blockchain where she is focused on driving ecosystem growth around the Hyperledger Project and other open Blockchain fabric and solutions that transform enterprise processes and transactions.



Founding & Executive Director of the Bitcoin Foundation

Jon Matonis

@jonmatonis

Matonis is an e-money researcher and crypto economist focused on expanding the circulation of non-political digital currencies. He has included senior influential posts at Sumitomo Bank, Visa, eBay, and Hushmail. He was an Executive Director of the Bitcoin Foundation until December 2014. Matonis also provides e-money consulting services to companies on alternative currency programs, Bitcoin compliance, jurisdiction selection, monetization strategies, risk management, and virtual currency platforms.




Co-founder of Winklevoss Capital Management

Tyler H Winklevoss

@tylerwinklevoss

Winklevoss is an American businessman, an early Bitcoin investor, entrepreneur, and a founder of Winklevoss Capital Management. He founded HarvardConnection (later renamed ConnectU) along with brother Cameron and classmate Divya Narendra. He was one of the great comeback stories in American business. Winklevoss is the co-founder of the Gemini Exchange, a digital currency exchanger that became the world's first licensed Ether exchange.



Founder of Startup Management

William Mougayar

@wmougayar

Mougayar is a leading Blockchain industry analyst who is described as the most sophisticated Blockchain business thinker. He is a Blockchain industry insider whose work has already shaped and influenced the understanding of Blockchain for people around the world, via his position as producer and host of The Token Summit, the first conference to explore the Token-Based Economy. Mougayar is a direct participant in the crypto-technology market, working alongside startups and entrepreneurs in addition to being an investor and advisor for some of the leading organizations in this space.



CEO of Overstock & Co-Chair at EdChoice

Patrick Byrne

@CverstockCEO

Byrne is the founder and CEO at Overstock, the Amazon rival to fame when it chose to accept Bitcoin for payments long before other major corporations. He remains bullish on cryptocurrency, defending Bitcoin against high-profile naysayers such as JPMorgan Chase CEO Jamie Dimon.



Co-founder & President of Unocoin

Sunny Ray

@SunnyStartups

Ray has over 15 years of experience in business development in the robotics and financial industries. He operates beyond the level of pure technology and always considers relevant social, economic, environmental, and political issues in the local and global level. In a 2015 interview, Ray identified India as one of the biggest unbanked populations in the world. After founding Unocoin in India, Ray made the company's mission to improve financial inclusion in the country.

More people on top.cointelegraph.com



CREATIVE CRYPTO

🔗 thecreativecrypto.com
🔍 hello [at] thecreativecrypto.com
🐦 [at] creative_crypto



THE STATE OF CRYPTO CREATIVITY [2018 Q4 UPDATE]

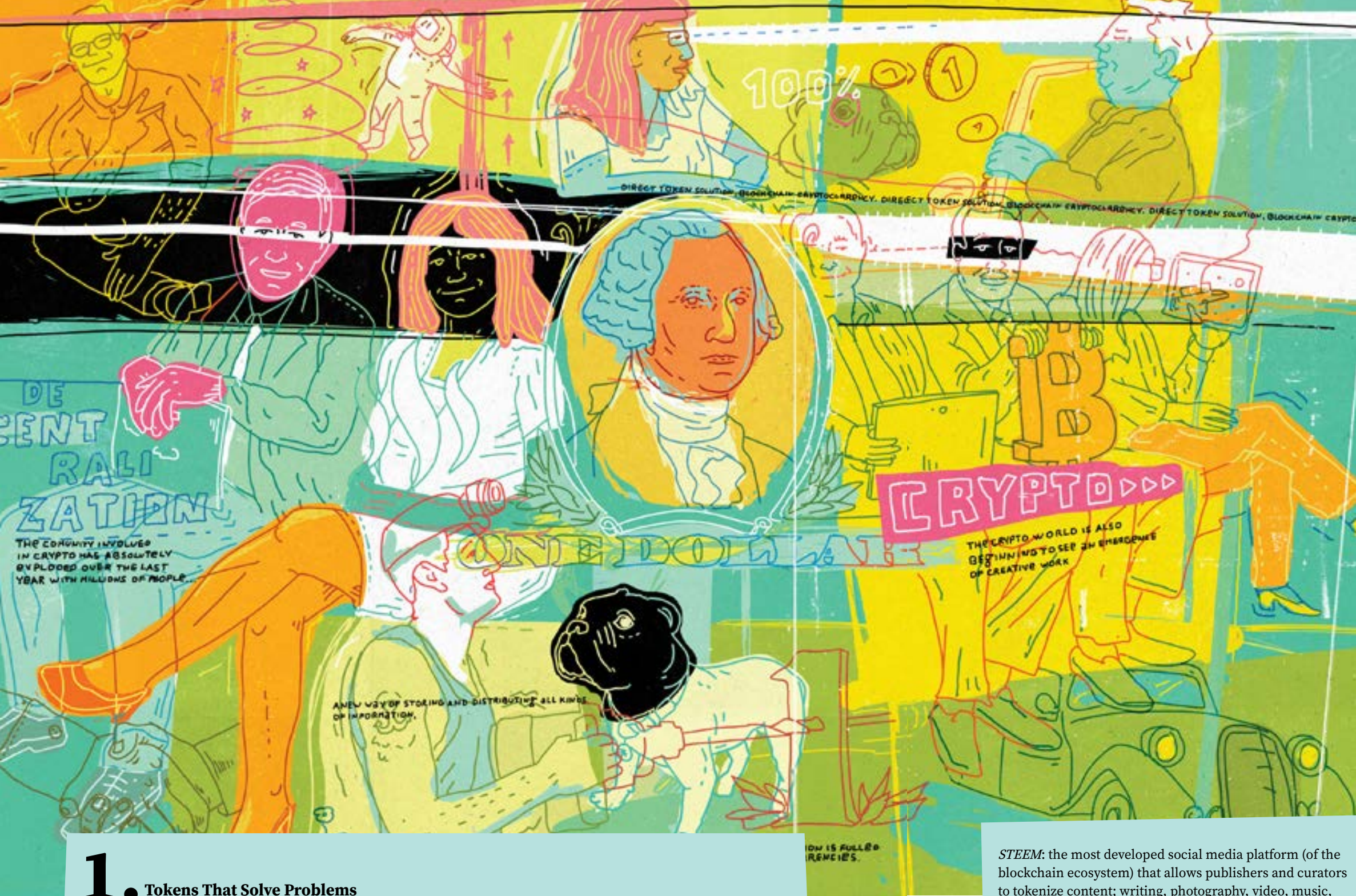
The Creative Crypto is an online magazine dedicated to the growing culture of blockchain - art, design, fashion, architecture, music, entrepreneurship, social impact, and more. The magazine serves as the nexus for activity and information across all crypto-networks and as the foundation for unique design projects borne from creative partnerships. Our mission is to make blockchain culture and its components accessible and appealing to anyone interested in the emerging technology.

WHY IS BLOCKCHAIN IMPORTANT TO CREATIVE PROFESSIONALS?

There are big implications of this new hierarchy of information in blockchain - security, stability, speed, transparency - but the most impactful repercussion of the blockchain ecosystem is its ability to protect, connect, and monetize our creative content. All of it. Imagine getting a micropayment for every Instagram shot, every witty Tweet, every Medium article, every Pinterest sketch, and every digital piece of art you send into the depths of Silicon Valley servers. Think of every aspect of your practice earning you stake in a valued blockchain and global audience. This new normal of open-source information and value is already beginning to kickstart an entirely new economic foundation for creative work.

Off of this premise, we're already beginning to see major projects and practices that creative industry professionals are leveraging to take innovative work to new levels. The following examples represent some of major in-real-life advancements that are actively empowering a once nebulous and underappreciated maker's economy:





1. Tokens That Solve Problems

Let's start at the infrastructural level. Several recent types of blockchains have been designed to focus on internet-era problems and the topics that haunt every creator - copywriting, proof of authorship, verifying authenticity, distribution, and many more - are being solved through immutable blockchain applications. Additionally, with the redistribution of profits typically reserved for a central company, creatives will also have access to new and more equitable crowdfunding tools, rewarded curation, and more effective content sharing. Makers will be able to take full control of and monetize their work through these new cryptocurrencies.

Here are just a few examples of developing blockchains that we'll cover with exclusive articles and interviews on The Creative Crypto —

STEEM: the most developed social media platform (of the blockchain ecosystem) that allows publishers and curators to tokenize content; writing, photography, video, music, and all manner of creative work.

LBRY: A tokenized and decentralized media marketplace, designed to eliminate commercials and central ad-revenue like on the traditional YouTube model.

CREATIVECHAIN: A new model for photo and visual design sharing, creating micro-payments to control Creative Commons licensing.

MUSICOIN: A blockchain and cryptocurrency dedicated to rewarding musical work.

DECENTRALAND: A digital ecosystem that allows the development of 3D objects and programs on their blockchain platform.

PROPS: A media and streaming-centric cryptocurrency designed to nurture more engaged relationships between streamers and fans.

CODEX: A blockchain and platform that secures and supports the provenance of both digital and physical assets.

All of these blockchains set the foundation for the growth of a decentralized ecosystem on top of their dedicated infrastructure. Whether it be music or art or 3D work, these solutions are already allowing new ways of making and rewarding.

2. Creative Communities and Programming

Since the last report on the state of creativity in crypto, we've experienced a monumental uptick in public activities around creative work and action in blockchain. From global exhibitions to industry-specific conferences.

This past spring's Ethereum Summit NYC by ConsenSys was one of the first instances of a major creative push, with a dedicated exhibition incorporating the work of RARE Art Labs and the Codex Protocol. Since then, showings and auctions have become regular occurrences worldwide and critical starting points for new creatives looking to enter the growing market.

Even long-standing 'traditional' institutions like Christie's are moving quickly to stake out blockchain partners to both integrate the technology as well as plug into these new booming markets. The New Art Academy is continuing that momentum of bridging traditional and emerging markets with their recent ArtTech + Blockchain Connect event as well as their upcoming Crypto Art Fair in New York City. Other like-minded organizations such as Mondo NYC are taking up similar trajectories with the music industry.

The impact of this growing environment is not just limited to new companies, apps and physical products. The community involved in crypto has absolutely exploded over the last year with millions of people contributing their time and experience to help make blockchain a unique topic of cultural discussion. We've seen the passionate community form an entire network of social activities including new collectives, educational institutions, hackathons, creative contests, and more types of organizations that help nurture and diversify the reach of blockchain.



3. Cryptocurrency Cultural Work

The crypto world is also beginning to see an emergence of creative work that integrates new functionalities of blockchain into art, design, architecture, and more. These cultural interventions range from Bitcoin eating flowers to a crypto-funded public park.

Though this is a bit of a lesser developed facet of the blockchain space, we're likely to see more efforts in creating cultural programming around the impact of the technology. This past summer, we launched the first in a series of yearly exhibitions titled "The Crypto Renaissance" to showcase tools and use cases of blockchain in the real world. Our friends at #ArtProject are led by Jessica Angel as well to create the Dogethereum Bridge at the upcoming Vancouver Biennial in 2019, an inhabitable installation that will house a variety of artistic crypto projects. At the platform level, Dada's distributed art creation app allows people from all parts of the world to collaborate on custom tokenized pieces.

These types of specialized and targeted activities are aggregating into a larger movement to make blockchain less of a buzzword and more of a relevant resource for anyone.

4. New Marketplaces

With art, it often comes down to the sale of artwork - this factor determines the livelihood of any creative practice. Luckily, this is a domain that many teams have tackled over the last several months to nurture a paradigm of peer-to-peer marketplaces and forums for collecting. It's easier than ever for art appreciators to collect the work of artists they love and even engage with them in a meaningful way, all without the former barriers presented by prohibitive pricing, infrastructural hurdles, and institutional gatekeepers.

Instead of that stodgy older model, one that has boxed out a tremendous amount of global creative energy, we're witnessing a modern renaissance of new creators and new collectors. Platforms like OpenSea, KnownOrigin, RARE Labs, Codex, SuperRare, and Portion, just to name a handful, are some of the premiere services that streamline that connection between maker and buyer. Before, gaining access to gallery-like systems or garnering enough eyeballs to generate a personal market was nearly impossible. Now, injecting one's work into a community of energetic creators is not only simpler, but much more sustainable for creatives. The specific support of digital art through crypto assets and non-fungible token systems is paving a more open economy for art and design.

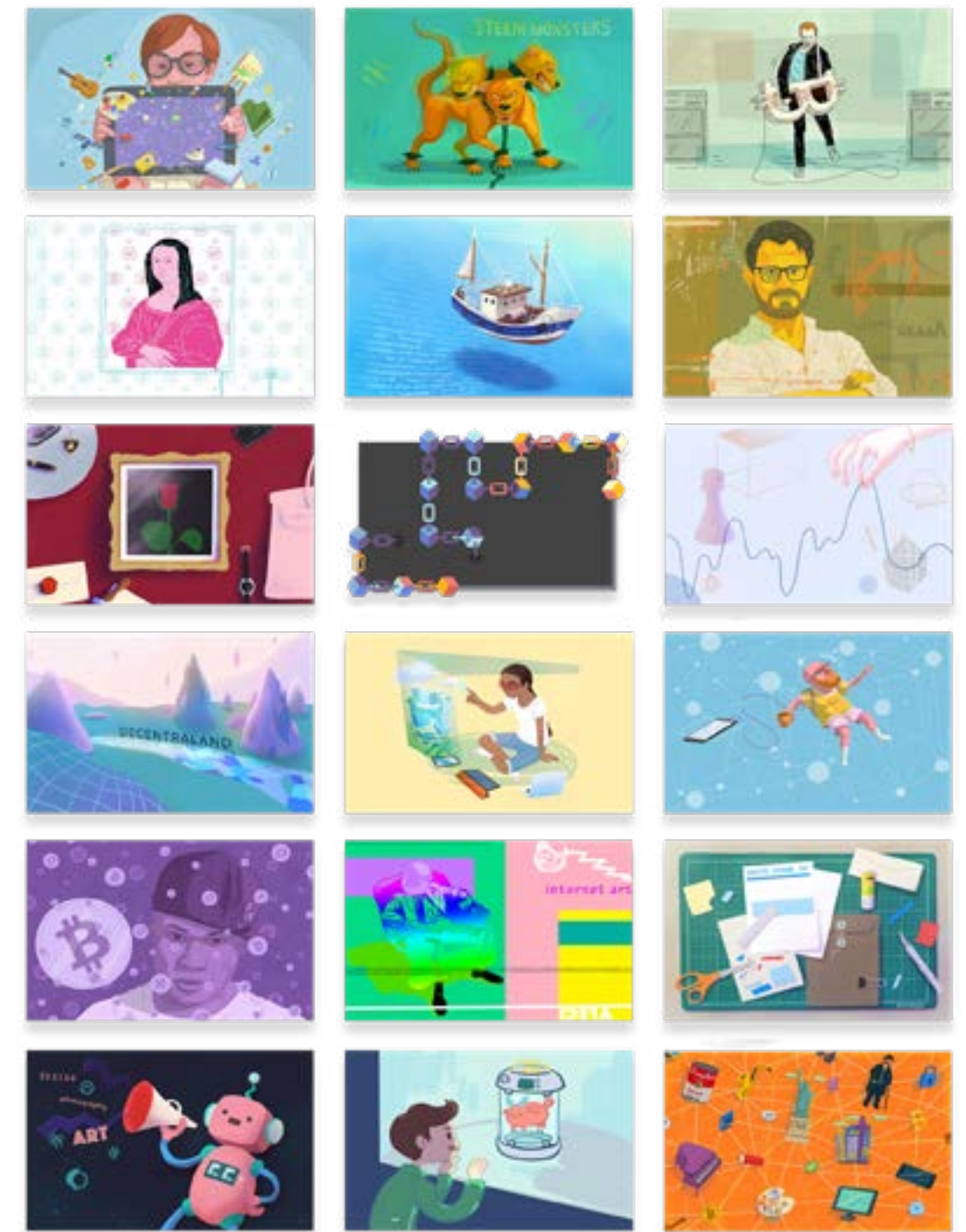




5. Gamifying Adoption

Lastly, the effort to make blockchain more widespread and accessible has been the most persistent thorn in the side of this industry. Educating the public on blockchain has proven to be deeply challenging. Instead of your typical tutorial or course series, industry leaders are crafting trojan horse-like strategies to attract new users without the major turn-off that is blockchain technical jargon. One primary strategy that has emerged is gaming. This specific form of creative engagement allows potentially anyone to use an app built on blockchain without being bogged down by all the burdensome technicalities and alien lingo. Plus, everyone loves games, especially so when you have the ability to earn from them.

The original precedent of CryptoKitties and digital collectibles has since spiraled into a much more diverse roster of gaming options, both existing and upcoming. The Loom Network, a scaling solution for the Ethereum blockchain, is going all-in on its application Zombie Battleground and speaking directly to the need for blockchain gaming's role in ushering in new usership. Axie Infinity, Gods Unchained, and Etheremon are unique versions of this ethic as well, and the daily usage of these products prove the strategic validity as games like Decentraland and CryptoKitties maintain the most transactional volume above most other DApps.

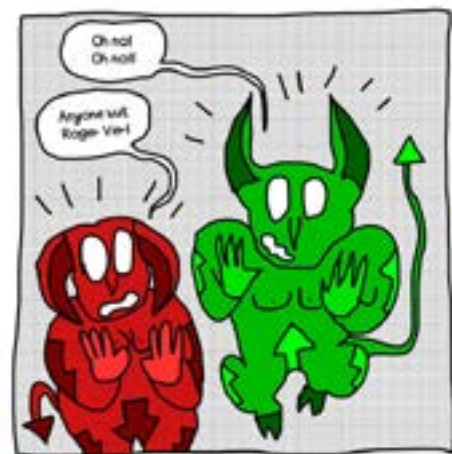
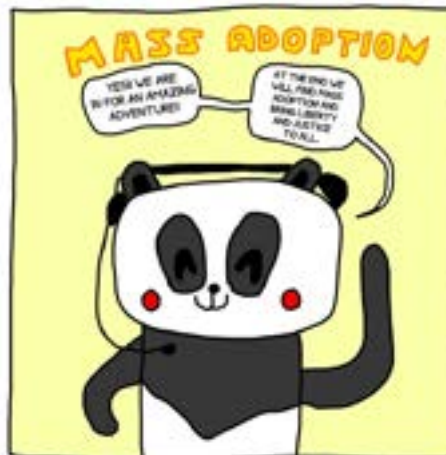
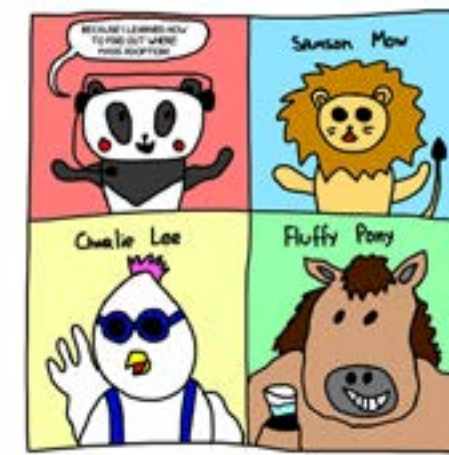
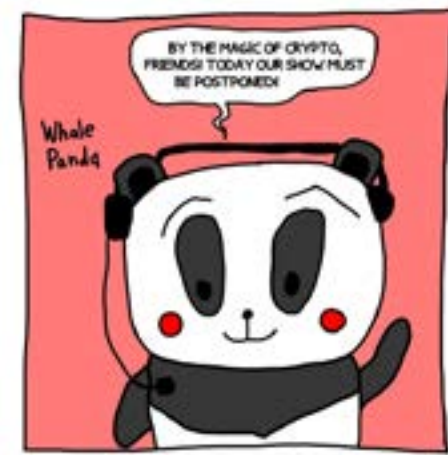
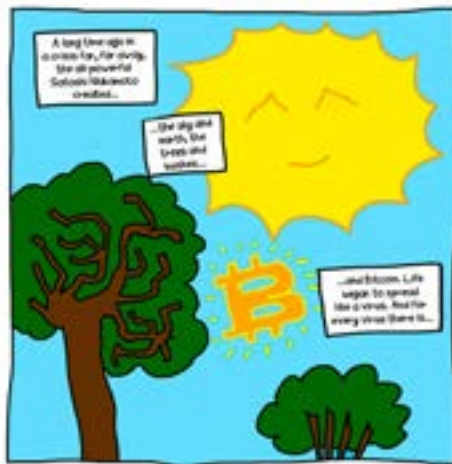


CULTIVATING THE CREATIVE CRYPTO MAGAZINE

It has only been only half a year since providing an initial overview on the creative components of the blockchain industry, and yet it seems the space has already made a generational leap forward. The entrepreneurship and stewarding is far beyond what was originally estimated, and with the sheer number of higher quality solutions appearing on the scene in the last few months, we're more optimistic than ever that blockchain's potential to revolutionize creative industries will become more historical than speculative.

Be sure to follow us at thecreativecrypto.com and on Twitter @creative_crypto for more articles and updates regarding our work.

Illustrations by @zsolt.vidak and @carrotcake





FUTURE



TOM LEE, SPEAKER AT BLOCKSHOW ASIA: 'BITCOIN IS PREPARING TO BREAK OUT'

One of the most anticipated speakers at Blockshow Asia, Mr. Thomas Lee, is a Fundstrat Global Advisors co-founder and a Wall Street analyst with over 25 years of equity research experience. He has consistently been ranked as the top institutional investor every year since 1998. Thomas Lee was one of the first “traditional finance” professionals that was talking about Bitcoin, and he is well-known for his positive attitude towards cryptocurrency.

This year's lineup of speakers at Asia Blockchain Week include Crypto-Congressman and Taiwan Legislator Jason Hsu; CTO at IBM, Former Head of Innovation at Mas, Stanley Yong; Co-founder & Managing Partner at Kenetic, Co-Founder Social Alpha Foundation, Jehan Chu; Co-founder of BTCC and Board Member of the Bitcoin Foundation, Bobby Lee; Partner at DFJDragon Fund/ DraperDragon Fund, Richard Wang; Partner at

Fenbushi Capital, Remington Ong; Blockchain Educator, Founder of Boxmining, Michael Gu; Partner at Sora Ventures, Former Managing Director at JRR Crypto, Vanessa Cao; Partner at Global Blockchain Innovative Capital, named as top 10 most influential crypto funds by 36kr (TechCrunch of China) and ODaily (Chinese Blockchain Media) will be present on the stage, Sinha Lee, and many more leading industry professionals.

Some of his recent quotes are: “Ethereum will rally strongly up to \$ 1,900 by the end of 2019” and “Bitcoin could end the year explosively higher,” referring to an upcoming Bitcoin and cryptocurrency market trend reversal.

The BlockShow team met with Mr. Thomas Lee during BlockShow Americas in Las Vegas to ask him why he believes Bitcoin will have a great next year, and whether he is expecting a financial crisis to happen imminently.

BLOCKSHOW: IN YOUR OPINION, WHAT WILL BE THE MOST PROFITABLE CRYPTOCURRENCY NEXT YEAR? WILL IT BE ONE OF THE WELL KNOWN CURRENCIES OR DO YOU EXPECT SOME NEW PLAYERS TO HAVE CONQUERED THE MARKET?

Mr. Thomas Lee: That is always very challenging to predict but I am sure it will be a token or coin with the best growth in active users. In the past year we saw the best performing cryptocurrencies have had the best growth in active users (e.g. EOS, XLM, BTC and DOGE). I at least expect Bitcoin to be one of the most profitable cryptocurrencies next year.

BLOCKSHOW: WHEN WILL BITCOIN BREAK OUT OF ITS LONG-RUN BEAR TREND?

Mr. Thomas Lee: Bitcoin is preparing to break out. It has found support around the \$6,000 level, which equals the breakeven for mining costs.

BLOCKSHOW: WHAT DO YOU THINK ABOUT THE PREDICTION OF J.P. MORGAN, THAT THE NEXT MAJOR FINANCIAL CRISIS WILL STRIKE THE U.S. ECONOMY BY 2020? IS THAT SOMETHING YOU CAN AGREE WITH?

Mr. Thomas Lee: In my opinion, a financial crisis will be inevitable to take place but the exact timing will quite uncertain. There is a greater leverage today and the global central banks have less “wobble” room because of the current low rates. With that being said, I am not expecting an imminent crisis.

BLOCKSHOW: DO YOU BELIEVE IT WILL BE POSSIBLE, THAT THE ENTIRE ASIAN REGION WILL BECOME CRYPTO-FRIENDLY IN THE FUTURE?

Mr. Thomas Lee: Asia is a region where I expect crypto to flourish. There is a large population of young people and countries are technically savvy. Also, there are already extensive use-cases of digital money and platforms such as WeChat and others.

BLOCKSHOW: HOW DO YOU THINK EVENTS INFLUENCE THE BLOCKCHAIN INDUSTRY?

Mr. Thomas Lee: Blockchain is dependent on community support and conferences and events allow communities to gather.

BLOCKSHOW: WHAT IS YOUR OPINION ON THE U.S. DOLLAR BACKED STABLECOIN USDT? WHAT DO YOU EXPECT?

Mr. Thomas Lee: I am comfortable that USDT is backed by USD and I have confidence in the Tether team.

BLOCKSHOW: WHAT DO YOU EXPECT FROM STABLECOINS?

Mr. Thomas Lee: Stablecoins are a novel idea and I hope they work. ⚡



LIFE'S CODE:

BLOCKCHAIN AND THE FUTURE OF GENOMICS

In an era of hotly contested debates surrounding data ownership, privacy and monetization, one particular piece of data could be said to be the most personal of all: the human genome.

While we are 99.9 percent identical in our genetic makeup across the species, the remaining 0.1 percent contains unique variations in code that are thought to influence our predisposition toward certain diseases and even our temperamental biases — a blueprint for how susceptible we are to everything from heart disease and Alzheimer's to jealousy, recklessness and anxiety.

2018 offered ample examples of how bad actors can wreak havoc with nefarious use of even relatively trivial data. For those concerned to protect this most critical form of identity, blockchain has piqued considerable interest as a powerful alternative to the closed architectures and proprietary exploits of the existing genomics data market — promising in their stead a secure and open protocol for life's code.

Encrypted chains

Sequencing the human genome down to the molecular level of the four 'letters' that bind into the double-stranded

helices of our DNA was first completed in 2003. The project cost \$3.7 billion and 13 years of computing power. Today, it costs \$1,000 per unique genome and takes a matter of days. Estimates are that it will soon cost as little as \$100.

As genomic data-driven drug design and targeted therapies evolve, pharmaceutical and biotech companies' interest is expected to catapult the genomics data market in the coming years, with a forecast to hit \$27.6 billion by 2025.

If the dataset of your Facebook likes and news feed stupefactions has already been recognized as a major, monetizable asset, the value locked up in your genetic code

is increasing exponentially as the revolution in precision medicine and gene editing gathers pace.

Within the past year, unprecedented approvals have been given to new gene therapies in the U.S. One edits cells from a patient's immune system to cure non-Hodgkin lymphoma; another treats a rare, inherited retinal disease that can lead to blindness.

Yet, here's the rub.

Genomics' unparalleled potential to trigger a paradigm shift in modern medicine relies on leveraging vast datasets to

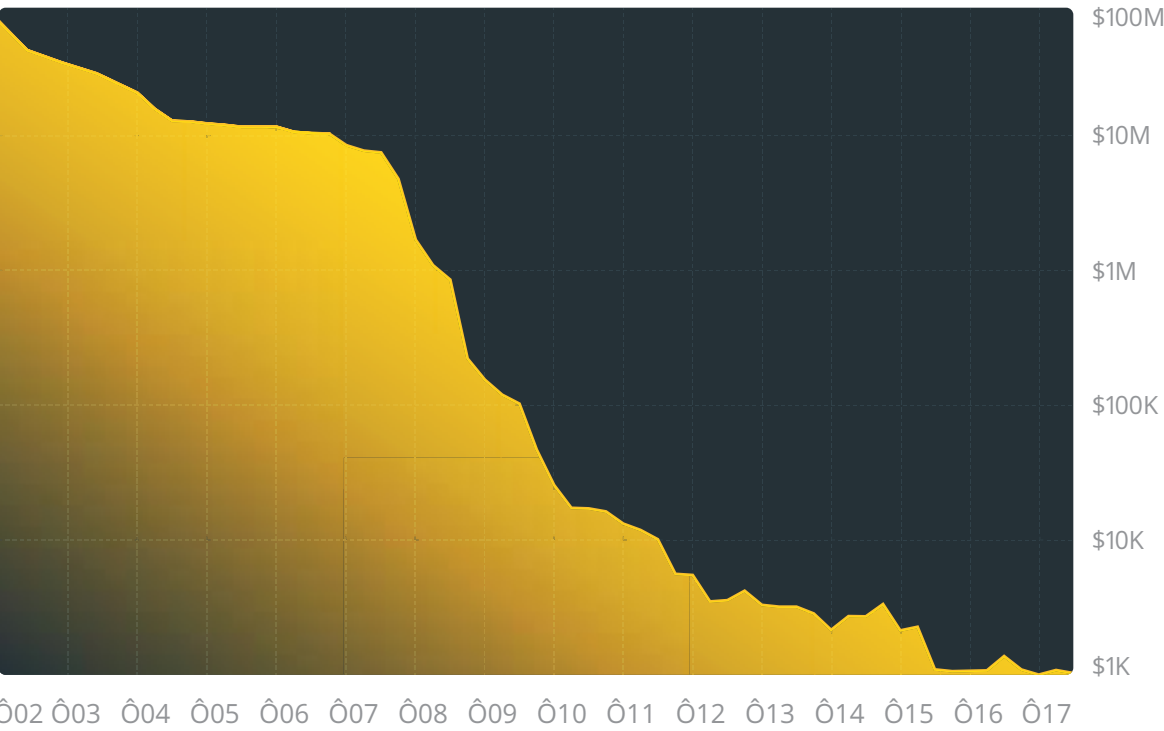
establish correlations between genetic variants and traits.

Generating the explosion of big genomic data that is still needed to decode the 4-bits of the living organism faces hurdles that are not only scientific, but ethical, social and technological.

For many at the edge of this frontier, this is exactly where Nakamoto's fabled 2008 white paper — and the technology that would come to be known as blockchain — comes in.

Cointelegraph spoke with three figures from the blockchain genomics space to find out why.

DNA SEQUENCING COST PER GENOME



Who owns your genome? Resurrecting the wooly mammoth... and blockchain

For Professor George Church, the world-famous maverick geneticist at Harvard, the boundaries between technologies in and out of the lab are porous. Having co-pioneered direct genome sequencing back in 1984, a short digest of his recent ambitions include attempts to resurrect the long-extinct mammoth, create virus-proof cells and even to reverse aging.

He has now placed another bleeding-edge technology at the center of the genomics revolution: blockchain.

Last year, Church — alongside Harvard colleagues Dennis Grishin and Kamal Obbad — co-founded the blockchain startup Nebula

Genomics. Church had been trying for years to accelerate and drive genomic data generation at scale. He had appealed to volunteers to contribute to his nonprofit Personal Genome Project (PGP) — a ‘Wikipedia’ of open-access human genomic data that has aggregated around 10,000 samples so far.

PGP relied on people forfeiting both privacy and ownership in pursuit of advancing science. As Church said in a recent interview, mostly they were either the “particularly altruistic,” or people concerned with accelerating research for a particular disease because of family experiences.

In other cases, as cybersecurity expert DNABits’ Dror Sam Brama told Cointelegraph, it is the patients themselves who generate the data and are “sick enough to throw away any ownership and privacy concerns”:

“The very sick come to the health care system and say, ‘We’ll give you anything you want, take it, we’ll sign any paper, consent. Just heal us, find a cure.’”

The challenge is getting everybody else. While no one knows exactly how many people have had their genomes sequenced to date, some estimates suggest it is around one million.

Startups like Nebula and DNABits propose that a tokenized, blockchain-enabled ecosystem could be the technological tipping point for onboarding the masses.

By allowing people to monetize their genomes and sell access directly to data buyers, Nebula thinks its platform could help drive sequencing costs down “to zero or even offer [people] a net profit.”

While Nebula won’t subsidize whole genome sequencing directly, a blockchain model would allow interested buyers — say, two pharmaceutical companies — to pitch in the cash for someone’s sequence in return for access to their data.

Tokenization opens up the flexibility and granular consent for enabling different scenarios. As Brama suggested, a data owner could be entitled to shares in whichever drug might be developed based on the research that they have enabled or be reimbursed for their medical prescription in crypto tokens. Contracts would be published and hashed, and reference to the individual’s consent recorded on the blockchain.

Genomic dystopias

Driving and accelerating data generation is just one part of the equation.

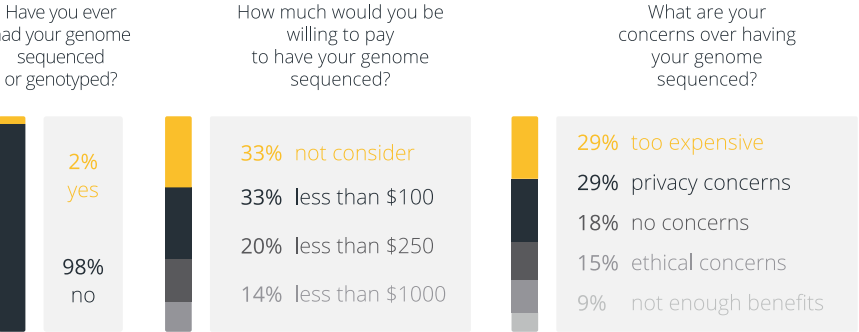
Nebula ran a survey that found that, rather than simply affordability, privacy and ethical concerns eclipsed all other factors when people were asked whether or not they would consider having their genome sequenced. In another study of 13,000 people, 86 percent said they worried about misuse of their genetic data: over half echoed fears about privacy.

These concerns are not simply founded in the dystopian 90s sci-fi of Hollywood — think Gattaca’s biopunk imaginary of a future society in the grips of a neo-eugenics fever.

As Ofer Lidsky — co-founder, CEO and CTO of blockchain genomics startup DNAtix — put it:

“Once your DNA has been compromised, you cannot change it. It’s not like a credit card that you can cancel and receive a new one. Your genetic code is with you for all your life [...]

NEBULA’S SURVEY ON GENOME SEQUENCING



Once it’s been compromised, there’s no way back.”

Data is increasingly intercepted, marketized and even weaponized. Sequencing — let alone sharing — your genome is perhaps a step further than many are willing to take, given its singularity, irrevocability and longevity.

DNABits’ Brama gave his cybersecurity take, saying that:

“The consequences are very difficult to imagine, but in a world [in which] people are building carriers like viruses that will spread to cells in the body and edit them — it’s frightening, but in fact, all the building blocks are

already there: genome sequencing, breaches of data, gene editing. People are now working to fix major health conditions using gene editing in vivo. But we should assume that every tool out there will eventually also get into the wrong hands.”

He added, “We’re not talking about taking advantage of someone just for one night with GHB or some other drug” — this would impact the rest of an individual’s life.

This April, on the heels of the Cambridge Analytica scandal,

news broke that police detectives had mined a hobbyists' genealogy database for fragments of individuals' DNA they hoped would help solve a murder case that had gone cold for over thirty years.

Law enforcement faced no resistance in accessing a centralized store of genetic material that had been uploaded by an unwitting public. And while many hailed the arrest of the Golden State Killer through a tangle of DNA, others voiced considerable unease.

This obscurity of access has implications beyond forensics. While Brama's dystopia may be some way off, today there are concerns about genetic discrimination by employers and insurance firms — the latter of which is currently only legally proscribed in a partial way. Grishin echoed this, noting

that in the U.S., “you can be denied life insurance because of your DNA.”

This May, the U.S. Federal Trade Commission opened a probe into popular consumer genetic testing firms — including 23andMe and Ancestry.com — over their policies for handling personal and genetic information, and how they share that data with third parties.

23andMe and Ancestry.com represent a recent phenomenon of so-called direct-to-consumer genetic testing, the popularity of which is estimated to have more than doubled last year.

These firms use a narrower technique called genotyping, which identifies 600,000 positions spaced at approximately regular intervals across the 6.4 billion letters of an entire genome. While limited, it still

reveals inherently personal genetic information.

The highly popular 23andMe home genotyping kit — sunnily packaged as “Welcome to You” — promises to tell people everything from their ancestral makeup to how likely they are to spend their nights in the fretful clutches of insomnia. The kit comes with a price tag as low as \$99.

This July, GlaxoSmithKline (GSK), the world's sixth largest pharmaceutical company, invested \$300 million in a four-year deal to gain access to 23andMe's database, and the testing firm is estimated to have earned \$130 million from selling access to around a million human genotypes, working out at an average price of around \$130. By comparison, Facebook reportedly generates around \$82 in gross revenue from the data of a single active user.

Battle-proof, anonymized blockchain systems for the genomics revolution

In this increasingly opaque genomics data landscape, private firms monetize the genotypic data spawned by their consumers, and sequence data is fragmented across proprietary, centralized silos — whether in the unwieldy legacy systems of health care and research institutions or in the privately-owned troves of biotech firms.

Bringing genomics onto the blockchain would allow for the circulation that is needed to accelerate research, while protecting this uniquely personal information by keeping anonymized identities separate from cryptographic identifiers. Users remain in control of their data and decide exactly who it gets shared with and for which purposes. That access, in turn, would be tracked on an auditable and immutable ledger.



Grishin outlined Nebula's version, which would place asymmetric requirements on different members of the ecosystem. Users would have the option to remain anonymous, but a permissioned blockchain system with verified, validator nodes would require data buyers who use the network to be fully transparent about their identity:

“If someone reaches out to you, it shouldn't be just a cryptographic network ID, but it should say this is John Smith from Johnson & Johnson, who works, say, in oncology.”

Grishin added that Nebula has experimented with both Blockstack and the Ethereum (ETH) blockchain but has since decided to move to an in-house prototype, considering the 15 transactions-per-second capacity of Ethereum to be insufficient for its ecosystem.

DNABits' Brama, also committed to using a permissioned system, proposed using “the simplest and most robust form of blockchain — i.e., a Bitcoin-type network.”

“The more powerful and the more capable engine that you use, the larger the surface attack.”

Lie-proofing the blockchain

23andMe is said to store around five million genotype customer profiles, and rival firm Ancestry.com around 10 million. For each profile, they collect around 300 phenotypic data points — creating surveys that aim to find out how many cigarettes you (think) you've smoked during your lifetime or whether yoga or Prozac was more effective in managing your depression.

A phenotype is the set of observable characteristics of an individual that results from the interaction of his or her genotype with their environment. Generating and sharing access to this data is crucial for decoding the genome through a correlation of variants and traits. But as Grishin notes, being largely self-reported, the quality of much of the existing data is uncertain, and a tokenized genomics faces one hurdle in this respect:

“If people will be able to monetize their personal genomic data, then you can imagine that some people might think, ‘If I claim to have a rare condition, many pharma companies will be interested in buying access to my genome’ — which is just not necessarily true. The value of a genome is kind of difficult to predict and it's not correct to say that if you have something rare, then your genome will be more valuable. In fact many studies need a lot of control samples that are kind of just normal.”

Education can help make people aware that they won't be making any more money by lying and that a middle-of-the-road genome might be just as interesting for a buyer as an unusual one. But Grishin also

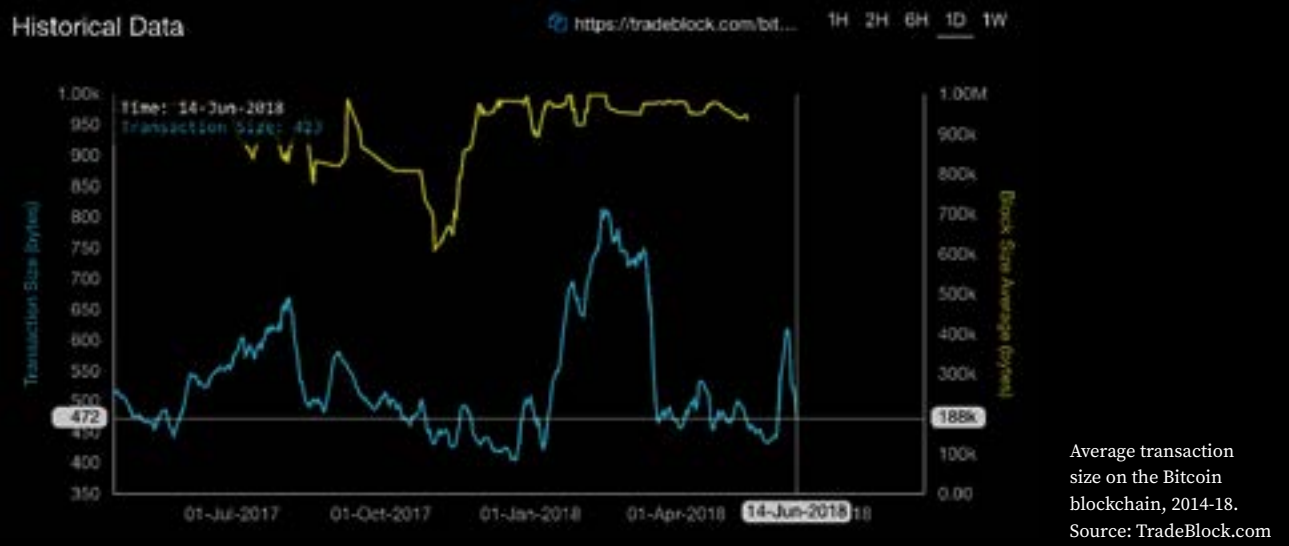
noted that a blockchain system can offer unique mechanisms that deter deception, even where education fails:

“Blockchain can help to create phenotype surveys that detect incorrect responses or identify where an individual participant has tried to lie. And this can be combined with blockchain-enabled escrow systems, where, for example, before you participate in a survey, you have to deposit a small amount of cryptocurrency in an escrow wallet.”

If conflicting responses indicate that someone has tried to lie about their medical condition, then their deposit could be withheld in a way that is much easier to implement within a blockchain system than compared to one using fiat currencies.

2018: Viruses and chromosomes hit the blockchain

In his interview with Cointelegraph, Lidsky proposed that the raw 200 gigabyte dataset is unnecessary for analysts, emphasizing that initial genome sequencing is read multiple times “say 30 or 100 times,” to mitigate inaccuracies. Once it’s combined, he explained, “the size of the sequence is reduced to 1.5 gigabytes.” This still requires significant compression to bring it to the blockchain. As a reference, the average size of a transaction on the Bitcoin (BTC) blockchain was 423 kilobytes, as of mid-June 2018.



In June, DNAtix announced the first transfer of a complete chromosome using blockchain technology — specifically IBM’s Hyperledger fabric. Lidsky told Cointelegraph the firm had succeeded in achieving a 99 percent compression rate for DNA this August.

Nebula, for its part, envisions that even on a blockchain, data transfer is unnecessary and ill-advised, given the unique sensitivity of genomics. It proposes sharing data access instead. The solution would combine blockchain with advanced encryption techniques and distributed computing methods. As Grishin outlined:

“Your data can be analyzed locally on your computer by you just running an app on your data yourself [...] with additional security measures in place — for example, by using homomorphic encryption to share data in an encrypted form.”

Grishin explained that homomorphic techniques encrypt data but ensure that it is not “nonsensical” — creating “transformations that morph the data without disturbing it”:

“The data buyer doesn't get the underlying data itself but computes on its encrypted form to derive results from it. Code is therefore being moved to the data rather than data being moved to researchers.”

Encrypted data can be made available to developers of so-called genomic apps — something that Nebula, DNAtix and many other emerging startups in the field all propose as one means of providing users with an interpretation of their data. They could also provide a further source of monetization for researchers and other third-party developers.

But is ‘outsourcing’ genomic interpretation to an app that simple? The decades-old health care model referred patients to genetic counselors to go over risks and talk through expectations, helping to translate what can be bewildering and often scary results.

Consumer genetic testing firms have already been accused of leaving their clients “with lots of data and few answers.” Beyond satisfying genealogical curiosity and interpreting a range of ‘wellness’ genes, 23andMe can reveal whether you carry a genetic variant that could impact your child’s future health and has — as of 2017 — even been authorized to disclose genetic health risks, including for breast cancer and Parkinson’s.

Blockchain may not fare much better when it comes to leaving individuals in the dark, faced with the blue glow of their computer screens. Nebula and DNAtix are both considering how to integrate genetic counselors into their ecosystems, and Grishin also proposed that users would be able to “opt in” to whether they really want to “know everything,” or only want “actionable” insights — i.e., things that modern medicine can address.

Blockchain and big pharma

Prescription drug sales globally are forecast to hit \$1.2 trillion by 2024. But closing the feedback loop between pharmaceuticals and the millions of people who take their pills each and every day still faces significant hurdles.

Drug development relies on correlating and tracking the life-cycle of medical trials, genetic testing, prescription side effects and longer-term effects relating to lifestyle; tokenization can incentivize individuals and enterprises to share data that is generated across multiple streams. As Brama outlined:

“Lifestyle data comes from wearables, smartphones, smart homes, smart cities, purchasing, commercial interactions, social media, etc. Another is carried by everyone, and that's our genome. The third is clinical and health-condition data generated in the health care system.”

Brama used the analogy of a deck of cards to explain how blockchain could be the key to starting to bring this data into connection, all the while protecting data owners’ anonymity.

An individual can hold an unlimited number of unique addresses in their digital wallet. Going into a pharmacy to purchase a particular drug — say, vitamin C, stamped with a QR code — would generate a transaction for one of these addresses. A visit to a family doctor might generate a further hash for a diagnosis on your electronic medical record (EMR) — say, a runny nose. This transaction goes between the caregiver and another wallet address.

A user might choose to put the correlation between transactions for their different wallets on the blockchain and make it public for people to bid on the underlying data. Or, they might keep the correlation off-chain and send proof only when, say, an insurance firm or research institute advertises to users who have a particular set of transactions:

“You hold the deck. You look at the cards, you decide if you say, if you don't say. And you can put them on the table and let everyone see, or you can indicate privately that you actually have these. It really leaves the choice to you.”

BIO technological frontiers

Professor Church has made an analogy that likely rings bells for anyone plugged into the crypto and blockchain space, saying that “right now, genome sequencing is like the internet back in the late 1980s. It was there, but no one was using it.”

Blockchain and the vanguard of genomic research have perhaps come closer to each other than ever before. Now that the DNA in our cells is understood as a life-long store of information, a new and disruptive technology is needed to securely and flexibly manage the interlocking networks of the body’s code.

The advent of genomics raises questions that cannot be settled by science alone. For all of our interviewees, blockchain could be just the key to creating the equitable and transparent means of ownership and circulation that would ensure these helices of raw biomaterial don’t spiral out of control. ⚡



BLOCKSHOW ASIA 2018 YEARBOOK



Addy Crezee
CEO



Anna Sergius
Deputy Director



Viad Stoiny
Sponsor Relations



Katrin Demi
Sponsor Relations



Shavrat Gas
Event Manager



Victoria Neiman
Project Manager



Aleksandra Miller
Account Manager



Julia Daimio
Agenda&Research Expert



Ksenia Eris
Customer Support



Florence Ibuowo
Olubunmi
Call Center Operator



Stasy Dulcimer
Media Producer



Roma Markiz
Videomaker



Elaine McQueen
Assistant Manager



John Fom
Media Buyer



Lina Freeman
Public Relations Manager



Stefania Rossi
Media Relations



Aleksander Raserei
Artists&Content Manager



Tanya Krum
Social Media Manager



Alex Kotezky
Designer



Antony Watsky
Developer



Daria Blumgart
Email Marketing Expert

Chief designer: Christine Thorpe

Authors: Ted Lins, Andrew Tar, Markus Kasanmascheff, Kirill Bryanov, Chrisjan Pauw, Stephen O'Neal, Nikolai Kuznetsov, Veronika Rinecker

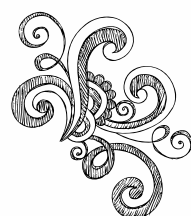
Copyright © 2018, Cointelegraph. All rights reserved.

CAUTION. ADVICE. RESEARCH.: Articles and advertisements in Cointelegraph are purely for information purposes and represent neither endorsement nor recommendation of such companies by the Publisher, Editor, and their agents.

While reasonable care is taken to ensure the accuracy of information in Cointelegraph magazine at the time of preparing for the press, no responsibility can be taken for any error that may have crept up inadvertently, or consequences of action based on any material contained herein. The views expressed in Cointelegraph do not necessarily reflect those of the Publisher or the Editor. We welcome unsolicited material for consideration, however, Cointelegraph accepts no responsibility for them.

Readers are recommended to make appropriate inquiries and take appropriate advice before sending their money, incurring any expense or entering into a binding commitment in relation to an advertisement. Cointelegraph magazine shall not be liable to any person for loss or damage incurred as a result of their accepting or offering to accept an invitation contained in any advertisement published in Cointelegraph.

Cointelegraph magazine was published under Cointelegraph franchise. Learn more: cointelegraph.com/franchise



We pick the best from
the web version of Cointelegraph
and give it a new life on paper.

USA

ASIA

EUROPE



Worldwide distribution
www.cointelegraph.com/magazine



BLOCK SHOW

P O W E R E D B Y



COINTELEGRAPH

The Future of Money

Cointelegraph
BlockShow Edition
November, 2018
Not for Sale