|  | <!DOCTYPE html> |
| --- | --- |
|  | <html> |
|  | <head> |
|  | <title>Cryptocurrency Policy Briefing</title> |
|  | <link rel="stylesheet" type="text/css" href="[CommentsStylesheet.css](http://k-band.us/CommentsStylesheet.css)"> |
|  |  |
|  | <meta charset="utf-8"> |
|  | <meta name="viewport" content="width=device-width, initial-scale=1.0"> |
|  |  |
|  | <meta name="keywords" content="blockchain, cryptocurrency, policy, regulatory"> |
|  | <meta name="description" content="xxx" /> |
|  | </head> |
|  |  |
|  | <body> |
|  | <header></header> |
|  |  |
|  | <main> |
|  | <article> |
|  |  |
|  | <h3 id="title"><i>Blockchain Threat Tracker 2018</i></h3> |
|  | <p id="author">Lauren Saine, Clashbit ~ lauren.saine@gmail.com</p><br> |
|  | <p id="author">(See <a href="[CryptoAgencies](http://k-band.us/CryptoAgencies)">Regulatory Agencies Reference Document</a>)</p> |
|  |  |
|  | <ul style="margin-bottom: 10px;"> |
|  |  |
|  | <li><a href="[#June5](http://k-band.us/CryptoThreatTracker#June5)">6.05 &nbsp; What about Network Layer 1?</a></li> |
|  | <li><a href="[#May28](http://k-band.us/CryptoThreatTracker#May28)">5.28 &nbsp; New FinCEN rules require identification of beneficial owners</a></li> |
|  | <li><a href="[#May18](http://k-band.us/CryptoThreatTracker#May18)">5.18 &nbsp; If anyone still thinks bitcoin is anonymous and fungible... </a></li> |
|  | <li><a href="[#April24](http://k-band.us/CryptoThreatTracker#April24)">4.24 &nbsp; Case against Coinbase for allowing money-laundering moves ahead</a></li> |
|  | <li><a href="[#April20](http://k-band.us/CryptoThreatTracker#April20)">4.20 &nbsp; New blockchain surveillance tools are scraping the web</a></li> |
|  | <li><a href="[#March26](http://k-band.us/CryptoThreatTracker#March26)">3.26 &nbsp; U.S. asserts jurisdiction over data held outside the country</a></li> |
|  | <li><a href="[#March21](http://k-band.us/CryptoThreatTracker#March21)">3.21 &nbsp; The NSA is tracking token users</a></li> |
|  | <li><a href="[#March20](http://k-band.us/CryptoThreatTracker#March20)">3.20 &nbsp; Section 702 v. Section 230</a></li> |
|  | <li><a href="[#February15](http://k-band.us/CryptoThreatTracker#February15)">2.15 &nbsp; The IRS is tracking crypto transactions</a></li> |
|  | </ul> |
|  | <br> |
|  |  |
|  |  |
|  | <p id="June5" class="heading">6.05 &nbsp; What about Network Layer 1?</p> |
|  |  |
|  | <p>Public blockchains, regardless of how decentralized or how masked, rely on the physical layer of the telecommunications infrastructure--the cables and poles and airwaves that envelop the globe. The physical layer, or <a href="<https://en.wikipedia.org/wiki/OSI_model>"> Layer 1</a> of the internet, is <a href="<http://drpeering.net/FAQ/Who-are-the-Tier-1-ISPs.php>"> privately-owned</a> and easily controlled by state actors. This represents a vulnerability of public blockchains that may not be solvable by new technologies alone.</p> |
|  |  |
|  | <p>State actors are continuing to develop their own physical infrastructure, which makes control seamless, obviating the need to go through telecom multinationals. For example, the <a href="<https://bitcoinmagazine.com/articles/quantum-blockchain-time-machine-could-keep-future-blockchains-secure/>"> Chinese government</a> is developing quantum key distribution satellites and a fiber link stretching over 2,000 km from Beijing to Shanghai. </p> |
|  |  |
|  | <p>Blockchain-related businesses can of course also be <a href="<http://fortune.com/2018/05/10/blockchain-law/>"> controlled</a> through their users, owners, miners, or any other entity reachable by <a href="<https://www.rogerebert.com/reviews/men-with-guns-1998>">law enforcement</a>. Chillingly, the Chinese government’s recent <a href="<http://xxzx.miit.gov.cn/InfoAction!showDetail.action?sectionId=M002&info.infoId=1026>"> white paper</a> asserts that ‘[Blockchain technology has] become an important support for the <a href="<http://thehill.com/opinion/technology/386524-the-west-could-be-closer-to-chinas-system-of-social-credit-scoring-than>"> social credit system</a>.” [Google translate] </p> |
|  |  |
|  | <p>Note: I have not been able to determine what methods Papua New Guinea used to <a href="<https://gizmodo.com/papua-new-guinea-to-shut-down-facebook-for-a-month-mig-1826382068>"> shut down</a> Facebook.</p> |
|  |  |
|  | <p id="link"><a href="[#title](http://k-band.us/CryptoThreatTracker#title)">&uarr;</a></p> |
|  |  |
|  |  |
|  | <p id="May28" class="heading">5.28 &nbsp; New FinCEN rules require identification of beneficial owners</p> |
|  |  |
|  |  |
|  | <p>FinCEN <a href="<https://www.fincen.gov/news/news-releases/fincen-reminds-financial-institutions-cdd-rule-becomes-effective-today>"> announced</a> May 11 that covered financial institutions must verify the identities of natural persons who are the beneficial owners of accounts held by legal entities. The new <a href="<https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf>">CDD Rule</a> amends FinCEN's Bank Secrecy Act rules, to "prevent criminals and terrorists from misusing companies to disguise their illicit activities and launder their ill-gotten gains." Covered institutions include U.S. banks, mutual funds brokers or securities dealers, futures merchants, and commodities brokers.</p> |
|  |  |
|  | <p>In related moves, South Korea is now requiring crypto traders to open <a href=[”https://qz.com/1186324/south-korea-is-making-real-name-cryptocurrency-trading-mandatory-by-january-30/”](http://k-band.us/%E2%80%9Dhttps://qz.com/1186324/south-korea-is-making-real-name-cryptocurrency-trading-mandatory-by-january-30/%E2%80%9D)> “real name” accounts</a> at the same banks as their exchanges in order to deposit money to trade cryptocurrencies. And the Japanese Financial Security Agency (FSA) <a href="<https://www.coindesk.com/japan-wake-call-get-ready-defend-privacy-coins/>"> has banned</a> all cryptocurrencies that provide a degree of anonymity...In response, Japanese exchanges are pulling four major privacy coins—monero (XMR), dash, Augur's reputation (REP), and zcash (ZEC)—from their platforms.</p> |
|  |  |
|  |  |
|  | <p id="link"><a href="[#title](http://k-band.us/CryptoThreatTracker#title)">&uarr;</a></p> |
|  |  |
|  |  |
|  | <p id="May18" class="heading">5.18 &nbsp; If anyone still thinks bitcoin is anonymous and fungible... </p> |
|  |  |
|  | <p>DMG is <a href="<https://themerkle.com/dmg-blockchain-solutions-addresses-aml-risk-through-bitscore-api/>">pitching </a>a surveillance tool for trading platforms to use on their own users. <a href="<https://dmgblockchain.com/BitScore/>"> BitScore</a> uses AI and machine learning to track cryptocurrency, detecting hops between transactions to determine the origin of funds, and using a weighting function to identify suspicious transactions. DMG says "understanding the provenance of source and destination addresses is imperative...for regulatory compliance.” </p> |
|  |  |
|  | <p>Meanwhile, Chainalysis continues its march to become the NSA of crypto. U.S. federal agency <a href="<https://diar.co/volume-2-issue-14/#1>">customers</a> now include the SEC and CFTC as well as ICE, IRS, FBI, DEA, and <a href="<https://www.fiscal.treasury.gov/>">BFS</a>. Chainalysis is a member of the benignly-named <a href=[:http://blockchainalliance.org/”](http://k-band.us/:http://blockchainalliance.org/%E2%80%9D)> Blockchain Alliance </a> a “public-private forum” to assist law enforcement and regulatory agencies.</p> |
|  |  |
|  | <p>Another member of the Alliance, CipherTrace, claims it can trace the provenance of each bitcoin involved in a transaction and determine if it came from a money-laundering site like BitBlender, a dark web marketplace like DreamMarket, or from digital wallets belonging to known criminals; it can also enable exchanges to monitor "exits" when users exchange their funds into dollars.</p> |
|  |  |
|  | <p>Coindesk <a href="<https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto/>"> reports</a> that OFAC’s <a href=[”](http://k-band.us/%E2%80%9D) https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq\_compliance.aspx”> Q&A</a> about “virtual currency” now warns that they may list cryptocurrency addresses associated with blocked persons, which means financial institutions would have to screen crypto transactions.</p> |
|  |  |
|  | <p>Even mammoth, shadowy exchange <a href="<https://cointelegraph.com/news/bitfinex-requires-customer-tax-info-which-it-may-exchange-with-govt-tax-authorities>">Bitfinex</a> says it may report personal ID data to US and <a href="<https://www.oecd.org/about/membersandpartners/>">OECD</a>-member tax authorities.</p> |
|  |  |
|  |  |
|  | <p id="link"><a href="[#title](http://k-band.us/CryptoThreatTracker#title)">&uarr;</a></p> |
|  |  |
|  | <p id="April24" class="heading">4.24 &nbsp; Case against Coinbase for allowing money-laundering moves ahead</p> |
|  |  |
|  | <p>The 11th Circuit Court of Appeals has allowed a <a href="<http://media.ca11.uscourts.gov/opinions/unpub/files/201712728.pdf>">case</a> against Coinbase to move forward. The plaintiffs are scammed customers of another exchange claiming Coinbase should have halted suspicious-looking trading by the founder of their exchange. In other private enforcement actions, Kraken was the target of a <a href="<https://news.bitcoin.com/class-action-lawsuit-exchange-kraken/>">lawsuit last year |
|  | </a>claiming it should have halted trading while under a DDOS attack.</p> |
|  |  |
|  | <p id="link"><a href="[#title](http://k-band.us/CryptoThreatTracker#title)">&uarr;</a></p> |
|  |  |
|  |  |
|  | <p id="April20" class="heading">4.20 &nbsp; New blockchain surveillance tools are scraping the web</p> |
|  |  |
|  | <p>Regulator demand for blockchain surveillance tools is increasing, and the private sector is responding. U.S. government contractor Chainalysis recently announced a <a href="<https://techcrunch.com/2018/04/05/benchmark-just-funded-chainalysis-the-crypto-intelligence-company-that-helped-crack-the-mt-gox-case/>">KYT tool,</a> with Series A funding from Benchmark Capital, which links real-time data on the "underlying purpose" of transactions with exchanges’ transaction processing. Until now, Chainalysis software only allowed customers to analyze transactions retroactively, but the KYT tool provides transaction analysis in real time. </p> |
|  |  |
|  | <p>The Merkle <a href=[”https://themerkle.com/bitfury-group-de-anonymizes-over-15-of-the-bitcoin-network-with-new-blockchain-analysis-tool/”](http://k-band.us/%E2%80%9Dhttps://themerkle.com/bitfury-group-de-anonymizes-over-15-of-the-bitcoin-network-with-new-blockchain-analysis-tool/%E2%80%9D)>reports</a> that Bitfury’s <a href=[”https://crystalblockchain.com/”](http://k-band.us/%E2%80%9Dhttps://crystalblockchain.com/%E2%80%9D)> Crystal </a>"blockchain analysis tools successfully de-anonymized millions of transactions and their associated addresses...[using] Bitcoin address clustering, which exposes users by identifying addresses which may be linked to one and the same user...gathering information from nearly 100 different sources.... Twitter and Reddit contain a treasure trove of information when it comes to de-anonymizing Bitcoin users. Close to 16% of the entire Bitcoin blockchain has been identified as a result of the first major test conducted by BitFury Group."</p> |
|  |  |
|  | <p>Legacy players are entering the market as well. Amazon Technologies won a <a href=[”](http://k-band.us/%E2%80%9D) http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=9,947,033.PN.&OS=pn/9,947,033&RS=PN/9,947,033”> |
|  | patent</a> for a process that de-anonymizes “cryptographic tokens” by combining <a href="<https://motherboard.vice.com/en_us/article/d35eax/amazon-bitcoin-patent-data-stream-identify-cryptocurrency-for-law-enforcement-government>">multiple real-time data streams</a>--from online merchant payment transactions, tax filings (which are supposed to be <a href="<https://www.law.cornell.edu/uscode/text/26/6103>">confidential</a>), and other sources--with cryptocurrency transactions. Finally, we have long known that data mining company Palantir counts many <a href=[”https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/”](http://k-band.us/%E2%80%9Dhttps://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/%E2%80%9D)> government clients</a>; Forbes <a href=[”https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/#1cd3ea207785”](http://k-band.us/%E2%80%9Dhttps://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/#1cd3ea207785%E2%80%9D)> reported </a> that the CIA was a seed investor. </p> |
|  |  |
|  | <p id="link"><a href="[#title](http://k-band.us/CryptoThreatTracker#title)">&uarr;</a></p> |
|  |  |
|  |  |
|  | <p id="March26" class="heading">3.26 &nbsp; U.S. asserts jurisdiction over data held outside the country</p> |
|  |  |
|  | <p>The <a style="display:inline" href="<https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes>">Cloud Act,</a> part of the <a style="display:inline" href="<https://regmedia.co.uk/2018/03/23/omnibus.pdf>"> Consolidated Appropriations Act of 2018</a> (page 2201 et seq), allows the U.S. government to seize data on servers outside U.S. territory, if it can find a U.S.-based entity that can access those servers. Conversely, it also allows "qualified" foreign governments to wiretap communications and seize personal data of U.S. citizens on U.S. territory and abroad, obviating the need to use the cumbersome Mutual Legal Assistance Treaty process.</p> |
|  |  |
|  | <p>The Cloud Act allows access to personal data held by communications-service providers for law enforcement purposes; the EU-US<a href="<https://www.privacyshield.gov/welcome>"> Privacy Shield</a> allows access to commercial data by registered private companies (both probably inconformance with the GDPR).</p> |
|  |  |
|  | <p>FinCEN’s existing regulations under Section 314(a) of the Patriot Act allow federal, state, local, and EU law enforcement to demand information from more than 16,000 financial institutions to find accounts and transactions that might be involved in terrorism or money laundering. (This has been used to identify facilitators of high-level political corruption using shell companies, misappropriating state assets, and exploiting the real estate sector.)<p/> |
|  |  |
|  | <p>In other surveillance news, Privacy International <a href=[”https://privacyinternational.org/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20%28200%29\_0.pdf"](http://k-band.us/%E2%80%9Dhttps://privacyinternational.org/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20%28200%29_0.pdf%22)> reports </a> that, from the Joint Defence Facility Pine Gap in Alice Springs, Australia, the US controls a global satellite network which monitors wireless communications under the <a href=[”https://www.lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing”](http://k-band.us/%E2%80%9Dhttps://www.lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing%E2%80%9D)> Five Eyes </a>agreement.</p> |
|  |  |
|  | <p id="link"><a href="[#title](http://k-band.us/CryptoThreatTracker#title)">&uarr;</a></p> |
|  |  |
|  |  |
|  | <p id="March21" class="heading">3.21 &nbsp; The NSA is tracking token users</p> |
|  |  |
|  | <p>The Intercept <a href="<https://theintercept.com/2018/03/20/the-nsa-worked-to-track-down-bitcoin-users-snowden-documents-reveal/>">reports that </a> the Snowden documents reveal that the NSA has been “tracking down” coin holders on the bitcoin ledger and getting their passwords, internet activity, and MAC addresses. The NSA uses its<a href="<https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/>"> XKeyScore </a> search system and OAKSTAR, a system of covert partnerships with corporate owners of the <a href="<https://arstechnica.com/information-technology/2016/05/how-the-internet-works-submarine-cables-data-centres-last-mile/>"> global internet infrastructure</a>.</p> |
|  |  |
|  | <p>Subprogram MONKEYROCKET taps into unspecified “foreign" fiber cable sites, and forwards that data to the NSA’s technical center in Germany. It's most controversial forms of surveillance, including warrantless bulk monitoring of emails and fiber optic cables from this and other programs, may have been used in court via "<a href="<https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases>">parallel construction</a>."</p> |
|  |  |
|  | <p>We’ve long known that security company RSA incorporated compromised <a href=[”https://www.theregister.co.uk/2018/04/20/rsa\_security\_conference\_insecure\_mobile\_app/](http://k-band.us/%E2%80%9Dhttps://www.theregister.co.uk/2018/04/20/rsa_security_conference_insecure_mobile_app/)> NSA algorithms</a> into its products. Not to crush any remaining illusions, but we now also know that <a href=[”https://freedom.press/search/?query=tor”](http://k-band.us/%E2%80%9Dhttps://freedom.press/search/?query=tor%E2%80%9D)> The Tor Project</a> is largely funded by US government agencies <a href="<https://www.bbg.gov/who-we-are/mission/>"> RFA (BBG)</a>,<a href="<https://www.state.gov/j/drl/>"> DRL (State Department)</a>, and the <a href="ttps://www.nsf.gov/">NSF</a>. See https://www.torproject.org/about/findoc/2015-TorProject-combined-Form990\_PC\_Audit\_Results.pdf. |
|  |  |
|  | <p id="link"><a href="[#title](http://k-band.us/CryptoThreatTracker#title)">&uarr;</a></p> |
|  |  |
|  |  |
|  | <p id="March20" class="heading">3.20 &nbsp; Section 702 v. Section 230</p> |
|  |  |
|  | <p>FISA <a href="<https://www.law.cornell.edu/uscode/text/50/1881a>"> Section 702 </a>, as <a href="<https://www.aclu.org/blog/national-security/privacy-and-surveillance/congress-just-passed-terrible-surveillance-law-now>"> reauthorized, </a>codifies government surveillance <a href="<https://s3.amazonaws.com/demandprogress/reports/FISA_Violations.pdf>"> abuses.</a> It <a href="<https://en.wikipedia.org/wiki/PRISM_(surveillance_program)>">allows the NSA </a>to demand data without a warrant--online content platforms must turn over messages to and from certain identifiers, and ISPs must intercept traffic traversing their cables and servers.</p> |
|  |  |
|  | <p>CDA <a href="<https://www.law.cornell.edu/uscode/text/47/230>"> Section 230 </a>protects online platforms from liability for good faith actions to restrict objectionable material. (<i>April 14 update: </i><a href="<https://www.eff.org/deeplinks/2018/03/how-congress-censored-internet>">SESTA/FOSTA </a>may upend that protection.) </p> |
|  |  |
|  | <p id="link"><a href="[#title](http://k-band.us/CryptoThreatTracker#title)">&uarr;</a></p> |
|  |  |
|  |  |
|  | <p id="February15" class="heading">2.15 &nbsp; The IRS is tracking crypto transactions</p> |
|  |  |
|  | <p><a style="display:inline" href="<https://www.forbes.com/sites/laurashin/2018/02/13/forbes-fintech-50-2018-the-future-of-blockchain-and-crypto/#654003151036>">Laura Shin: </a>Chainalysis, with just $1.6 million in capital invested, already counts the IRS, FBI (and <a href="<https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.4.4&s=FPDSNG.COM&q=VENDOR_FULL_NAME%3A%22CHAINALYSIS+INC.%22+CONTRACTING_AGENCY_NAME%3A%22DRUG+ENFORCEMENT+ADMINISTRATION%22&x=0&y=0>">DEA), </a> and Europol as users of its tools, which allow specific crypto transactions to be traced.</p> |
|  |  |
|  | <p id="link"><a href="[#title](http://k-band.us/CryptoThreatTracker#title)">&uarr;</a></p> |
|  |  |
|  | </article> |
|  | </main> |
|  | </body> |
|  | </html> |