Is Bitcoin a Safe Haven for Your Money?

By Jackson Dumont

In the summer of 2019, the 10-year minus 3-month yield curve inverted (https://markets.businessinsider.com/news/stocks/yield-curve-inversion-explained-what-it-is-what-it-means-2019-8-1028482016) for the first time in 13 years. During the time of the inversion, Bitcoin’s price hit all-time highs for the year. The previous inversion in 2006 was followed shortly thereafter by the global economic crisis of 2008.


Throughout the Iran-U.S. conflict, Bitcoin’s price spiked upward by 21%, from just below $7,000 to nearly $8,500.

The foreshadowing of another global economic crisis and the threat of further international conflict has given rise to an important question: is Bitcoin a safe haven asset?

To investigate this narrative, we sought the opinion of world-renowned economist Campbell Harvey, who is best known for theorizing yield curve inversions as accurate signals of oncoming economic downturns. Harvey is the Edward E. clutch Professor of International Business at Duke University, where he has been teaching a course on fixed income derivatives since 1980.

In his 1981 book, “Haven from Inflation: The Case for Hedging Against Inflation Risk” (https://www.cambridge.org/core/books/haven-from-inflation-the-case-for-hedging-against-inflation-risk), Harvey described how inflation-protected bonds could be used to hedge against future inflation risk.

In a 2012 interview with Cointelegraph (https://coingecko.com/news/bitcoin-a-safe-haven), Harvey elaborated on the role of cryptocurrencies in the global economy, stating: "I think it’s really important that we understand the role of cryptocurrencies and other digital assets in the global economy. They are becoming a very significant part of the financial system, and we need to understand how they work and how they fit into the broader picture of the global economy."

In this interview, Harvey also expresses a vision of the future in which digital tokens could undermine the global dominance of fiat currencies.

https://coingecko.com/news/is-bitcoin-a-safe-haven-for-your-money
By Rachel Wolfson  

CipherTrace Urges Crypto Companies to Prepare for Anti-Money Laundering Compliance
For better or for worse, the cryptocurrency space is coming of age. Since Bitcoins rise to mainstream prominence in 2015, there has been increasing recognition of digital assets from government agencies around the world. In turn, new regulations are being imposed to control the way cryptocurrency companies operate and do business globally.

Most recently, the Financial Action Task Force issued new guidelines (https://coingecko.com/news/fatf-aml-regulation-can-the-crypto-industry-adapt-to-the-travel-rule) on how digital assets should be regulated. In order to raise awareness around these requirements, the blockchain security company CipherTrace hosted a conference and hackathon this week in San Francisco dedicated entirely to discussions on the FATF guidelines, also known as the “travel rule.”

The travel rule requires regulators and Virtual Asset Service Providers, such as exchanges from various countries worldwide, to collect and share personal data during transactions. Much like the guidelines followed by traditional banks under the United States Bank Secrecy Act (https://coingecko.com/news/anti-money-laundering-laws-apply-to-crypto-too-says-fincen-chief), the travel rule being enforced for crypto firms follow the same requirements as money transmitters do to record identifying information on all parties in fund transfers made between financial institutions.

Yet, unlike traditional financial firms, many cryptocurrency exchanges do not capture personally identifiable information by default. Complying with the travel rule will therefore require significant shifts for businesses operating in the crypto space.

“The new regulations coming from FATF will ultimately change the way crypto companies operate, requiring them to track not only their own customers’ transactions, but also where their customers are sending money to,” Dave Jeavons, CEO of CipherTrace, told Cointelegraph.

One of the main goals of the CipherTrace conference was to gather regulators, banks, crypto companies and programmers together to make sense of the new guidelines, and then build a solution that would allow organizations to easily comply with the FATF rules.

“There are broad implications around privacy, identification of customers, how data works across various blockchains and privacy coins,” said Jeavons. “We need to come up with solutions to ensure that companies can easily comply with these regulations, which is what we aim to achieve here.”

Companies must act now

Prior to working on a compliance solution at the hackathon, a number of panels highlighted the themes and main challenges surrounding the FATF regulations. While these rules are not yet legally binding — as the FATF said in a public statement (http://www.fatf-gafi.org/publications/fatf-recommendations/documents/public-statement-virtual-assets.html) in June that countries have until June 2020 to adopt the guidelines — a broad theme at the CipherTrace conference was that action must be taken immediately. The G20 (https://coingecko.com/tags/g20) stated that it already uses the recommendations for anti-money laundering (https://coingecko.com/tags/aml) regulation of cryptocurrencies, so crypto companies that fail to comply with the new regulations are likely to face penalties.

“The consequences for non-compliance could range from a slap on the wrist, to going to jail if a company violates the Bank Secrecy Act,” Carol Van Cleef, CEO of blockchain consulting firm Luminous Group, warned on stage during the legal requirements panel. “No matter how big or small a company is, each has obligations to fulfill under the law.”

Although this may be the case, John Jeffries, CipherTrace’s chief financial analyst, pointed out that many companies operating in the cryptocurrency sphere have yet to comply with the new regulations.

“Many U.S. exchanges may not yet be compliant, but they should be at this time,” Jeffries said. “Moving forward, when Binance or Coinbase completes a transaction for example, they need to send the sender recipient data at the same time with that transaction. Otherwise, they are not in compliance.”

https://coingecko.com/news/is-bitcoin-a-safe-haven-for-your-money

3/5
Is Bitcoin a Safe Haven for Your Money?

The U.S. Treasury Department’s Financial Crimes Enforcement Network emerging technology policy specialist, Carole House, explained the FATF guidelines during her keynote. She highlighted that the guidelines are designed to curb the use of cryptocurrencies for financial crimes by making crypto transactions more traceable, giving regulators increased visibility into both cross-border and domestic currency transfers.

“Crypto companies need to comply with the virtual currency recommendations by the end of June 2020. We’ve already been involved with a number of people from the Digital Commerce Association to provide commentary around accomplishing this,” House stated.

The regulations are clear — now what?

As the FATF regulations were brought to light, a number of challenges around ensuring compliance followed.

For instance, the question of how the FATF guidelines would relate to privacy coins was a pressing issue. One of the stated goals of privacy coins such as Monero (https://cointelegraph.com/tags/monero) and Zcash (https://cointelegraph.com/tags/zcash) is to ensure that users have anonymized transactions, so it is questionable how these could be compliant with the new regulations.

During the privacy coin panel, Jack Gavigan, head of product and regulatory affairs at Zcash, asked, “Is compliance possible in relation to privacy coins?”

Answering his own question, Gavigan stated his belief that compliance is indeed possible, as a number of privacy coins are already listed in U.S. exchanges regulated by the Financial Crimes Enforcement Network.

Even though this may be the case, understanding how to abide by the FATF regulations in a way that focuses on privacy while maintaining the decentralized ethos of cryptocurrency and blockchain remains a challenge.

Jake Tarrow, a security software developer at CipherTrace, aimed to solve this problem during the hackathon. His team came up with an impressive solution that aims to keep data anonymous when information is being exchanged between Virtual Asset Service Providers.

“if VASP A is trying to send data to VASP B, we need to know how this can be done in a way that none of the information is in the clear,” Tarrow told Cointelegraph.

His solution entailed using a zk-SNARK — short for a “zero-knowledge succinct non-interactive argument of knowledge” — a form of cryptography that allows one party to securely reveal that it possesses a piece of information, without actually exposing the information itself.

“By using zk-SNARKs, VASPs can send this information in a bulletproof way, where no one else can pick that up and pull out their proprietary information,” explained Tarrow.

During the hackathon, developers also worked closely with security software gurus to integrate the Travel Rule Information Sharing Architecture into their systems. CipherTrace announced the release of TRISA (https://bitcoinmagazine.com/articles/ciphertrace-unveils-travel-rule-protocol-for-cryptocurrency-businesses) in September as an open-source, peer-to-peer design for cryptocurrency companies and blockchain projects to comply with the FATF regulations.

TRISA is meant to provide secure, reliable delivery of personally identifiable information, or PII, to the correct VASP, eliminating a huge risk for exchanges. However, sharing PII is prone to spamming, a problem that developers at the CipherTrace hackathon aimed to solve.

“Various backend systems managing PII are vulnerable to spamming, as spammers can get into these systems and start asking people to send PII,” explained Jeffries.

Independent consultant Kenneth Kron and his team won first place in the hackathon for coming up with a solution that introduces PII tokens to prevent spamming in TRISA.

“We want to solve the problem of PII spamming in TRISA by introducing PII tokens and KYC providers who can generate enhanced KYC tokens. If spammers are trying to capture personal information and get a hit, all they get back is a token in this case,” Kron told Cointelegraph.

All the ingredients for a compliance recipe

Overall, the CipherTrace conference and hackathon gathered a unique mix of individuals to discuss the future of cryptocurrency regulations. The discussions throughout the event demonstrated that action must be taken now to ensure that crypto companies are compliant with the FATF regulations by June 2020.

“We gathered many tribes that do not typically interact, enabling experts from government, exchanges and privacy groups to understand each other’s diverse perspectives,” Jeffries told Cointelegraph after the conference. “The conversations instilled a sense of urgency in the community and TRISA, while creating an open-source path to meet these tight regulatory deadlines and defend privacy at the same time.”
<table>
<thead>
<tr>
<th>Title</th>
<th>URL</th>
</tr>
</thead>
</table>

Follow us on

Daily updates

Your Email  Subscribe