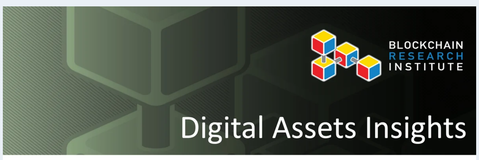

Hi there,

Welcome to Digital Assets Insights, a weekly collection of news, analysis and commentary. Some of this content also appears in *Digital Asset Digest*, a publication of Ninepoint Digital Asset Group. We hope you find this content valuable. Please direct any comments or questions to douglas@blockchainresearchinstitute.org.

Follow us on our other platforms

For more information about digital assets, please see our research papers Digital Asset Revolution, Token Taxonomy: The Need for Open-Source Standards Around Digital Assets, and A Taxonomy of Digital Assets.

You might also find our latest book "Digital Asset Revolution" interesting.

For more information on The BRI's new Web3 program please contact us by clicking here, or send us a note at info@blockchainresearchinstitute.org

News

Beijing Releases Web3 White Paper – Is China Changing its Tune on Web3?

The Beijing Municipal Science and Technology Commission and the Zhongguancun Science and Technology Park Management Committee recently unveiled the "Beijing Internet 3.0 Innovation and Development White Paper" at a forum on May 27th. Classified as "an inevitable trend in the future development of the Internet industry," the report explores what web3 could mean for Beijing and for the economy as a whole.

The white paper classifies the United States as the current Web3 industry leader globally, and stating that Beijing wants to be "an innovational highland with international influence." Apparently, thirty state and local departments have introduced initiatives to promote the development of Beijing as a global hub.

On this week's DeFi Decoded, Andrew and Alex discuss the broader implications of what this means for China's place in the Web3 world and whether this 'thawing' will last. This information came from a translation of the paper.

From the Mainland to Hong Kong…Huobi Starts Offering Spot Trading Under New Licensing Regime

Cryptocurrency exchange Huobi HK has officially begun offering digital asset spot trading for retail and institutional clients in Hong Kong following their application to the Hong Kong Securities and Futures Commission. To ensure compliance and adherence to anti-money laundering regulations, Huobi HK will work closely with auditors. The move comes after Hong Kong implemented a crypto licensing regime to safeguard retail investors while fostering innovation. Hong Kong feels a need to reestablish itself as a hub for Web3 following a lockdown-induced exodus.

Circle's Stablecoin Eurotrip

Following the inaugural Euro Coin launch on the Ethereum blockchain in June 2022, stablecoin issuer Circle has deployed EUROC on the Avalanche blockchain, aiming to enhance payment and financial services efficiency. EUROC is a regulated stablecoin backed by euro reserves held in US-regulated financial institutions. The move is part of Circle's multi-chain strategy, increasing EUROC's liquidity and enabling users to transact in euros alongside USD Coin (USDC). Circle's VP of Product, Joao Reginatto, emphasized the improved accessibility to the euro for all while providing a more cost-effective experience for developers and users. The addition of EUROC on Avalanche aligns with the growing demand for multi-currency and cross-border decentralized finance.

From Canvas to Coins: Binance Introduces NFT-Backed Borrowing

Binance has ventured into the NFT lending sector with the introduction of a new feature on its NFT marketplace. Users can now borrow cryptocurrencies by using their non-fungible tokens (NFTs) as collateral. Initially, the feature will support Ethereum borrowing against "blue chip" NFTs like the Bored Ape Yacht Club (BAYC), Mutant Ape Yacht Club (MAYC), Azuki, and Doodles collections. Binance NFT's website states that the current interest rate on NFT loans is 3.36% per annum, and the loan-to-value ratio ranges from 40% to 60%. Notably, there are no gas fees or Ethereum transaction charges involved. This move follows the recent launch of Blend, an NFT lending protocol by the giant Blur.

Driving into the Digital Age: F1 Debuts NFT Tickets with Loyalty Perks at Monaco Grand Prix

Platinum Group, the prominent F1 ticket provider, has introduced non-fungible token (NFT) race tickets in collaboration with blockchain infrastructure company Elemint and Web3 agency Bary. These NFT tickets, starting with the Monaco Grand Prix, will be minted on Ethereum sidechain Polygon. Besides granting access to the race, the NFTs will offer additional benefits such as hospitality privileges and future race discounts, encouraging collectors to remain loyal. The seamless onboarding process ensures that users without Web3 knowledge can easily purchase the NFT tickets. This move towards blockchain technology in event ticketing is expected to extend beyond Formula 1 into the broader world of sports and entertainment.

Commentary

An Interesting Question about the Quantum Threat

By Douglas Heintzman
Chief Catalyst
Blockchain Research institute

On a recent episode of our W3B Talks podcast, I was talking to Pierre-Luc Dallaire-Demers, the founder, and CEO of the Pauli Group. His company is researching the impact of quantum computing on the cryptography that protects blockchain and many digital assets. As most of you know, much of the world's encryption, including that which secures most blockchains is based on asymmetric keys that use prime number factorization. This encryption scheme is very good, and it would take even the most powerful supercomputers in the world, millions of years to crack today's encryption.

The problem is that prime number factorization is something that quantum computers are very good at. A commercial scale quantum computer could break that same encryption in a matter of hours or minutes.

We've known about this problem for a long time and mathematicians and computer scientists have been busy working on quantum safe encryption for many years. The National Institute of Standards and Technology (NIST) has published the first four quantum-safe algorithms based on structure lattice and hash functions. We are on track to have access to quantum-safe cryptography before the quantum threat arrives in force. That's the good news. The bad news is twofold. The first problem is that is quantum safe cryptography isn't as computationally efficient, so we will have to incur marginally greater transaction costs and slower transaction speeds, the second problem is that that the quantum threat has already arrived.

The issue is that it is possible to harvest encrypted data today and decrypt it when a sufficiently powerful and economical quantum computer arrives on the scene. I'm very familiar with the "harvest now - decrypt later" problem. I co-wrote a paper for the ACM Queue journal on the topic a couple of years ago. The mitigating strategy is to inventory your data and determine the monetary, reputational, and regulatory value of the data and then calculate how quickly that value degrades over time. You then need to quantum safe encrypt the data that is valuable, restricted and that has a long shelf life.

The questions that Pierre-Luc asked me was: "What happens when someone uses a quantum computer to attack Satoshi Nakamoto's wallets?" I had never thought about this before. The wallets, after all, can be easily harvested by anyone. Satoshi owns about 1,100,000 bitcoins. At today's exchange rate that is worth about 39.1B USD. At bitcoin's price maximum Satochi's wallets held roughly $75.6B USD worth of bitcoin.

Those numbers are a pretty good incentive to mount an attack. The inevitability of such an attack would surely motivate Satoshi, assuming that he/she/they are alive and still have the keys, to move those bitcoins to quantum safe wallets before they are stolen or even exchange them for some other sort of currency. I struggle to imagine what the phycological effect a theft of that nature and magnitude, or even just a legitimate wallet transfer by Satoshi, would have on the Bitcoin market. Food for thought.

Thankfully quantum safe is major design consideration for CBDCs and other long lived digital assets classes that the designers of those systems are actively working on. I'm confident that we will figure it out, but there will surely be some interesting bumps along the road.

Podcasts

You can find "**W3B Talks**", our podcast series on Web3 and its impact on business and society here. You can also find it on your favourite podcasting platforms such as Spotify, Amazon Music, Google Podcasts, and Apple Podcast.

Recent episodes include:

- Post Quantum Cryptography for Blockchains with Pierre-Luc Dallaire-Demers
- Web3 and Gen Z with Rishab Chakraborty
- LACChain: Enterprise Blockchain in Latin America with Ilan Melendez
- Web 3 and Real Estate with Sanjay Raghavan
- The Circular Economy and ReFi with Tian Zhao

Check out the latest episode of Defi Decoded with Alex Tapscott and Andrew Young: Unpacking Beijing's Web3 White Paper, Circle's Euro Coin, and Crypto's Course

You can see other episodes on Youtube here.

About the Blockchain Research Institute

Navigate, accelerate, and lead the blockchain revolution.

The Blockchain Research Institute is a global think-tank exploring the promise of Web3 and blockchain technology for business, government, and society. Our syndicated program is funded by an international community of member organizations, including enterprises, governments, and technology start-ups from around the world.

We're always looking for new organizations to collaborate with, through a number of initiatives.

- BRI Member Program
- BRI Global Partnership Program
- Web3 and Blockchain World Conference

For all inquires, please email douglas@blockchainresearchinstitute.org