

Market Updates

Central Bank Digital Currencies: On the rise

Overview: Central banks and regulators are exploring the potential of Central Bank Digital Currencies (CBDCs) and their implications for the future of the payments and financial services ecosystem for commercial and retail users alike. Increasing efforts can be mainly identified in Asia, where the People's Bank of China (PBoC) is moving rapidly with the legitimisation of the first major CBDC. In addition, efforts can also be seen in the European Union (EU) where the European Central Bank (ECB) is increasingly contemplating a digital euro in light of rising use cases and a digitally progressive Asia. The Bahamas, Japan, Estonia, Spain, Australia and Canada have also joined the race for CBDCs with pilots and research initiatives, while PayPal announced that its customers will be able to transact in virtual currencies. The decentralised finance (DeFi) space records all-time high numbers, as new novel forms of attack decentralised protocols emerge.

The case for a digital euro: In Europe, [a speech by the president of the European Central Bank](#) (ECB) Christine Lagarde at the Deutsche Bundesbank conference on "Payments in a digital world" laid the foundations that support the case for a Digital Euro. Ms Lagarde highlighted the changing consumer sentiment towards digitalisation, e-commerce and electronic payments, further accelerated by the COVID-19 pandemic, along with the rising competition to dominate payments on a global level and Europe's disadvantaged position in the race as the major trends in global payments.

The pros and cons: The [workshop on CBDCs](#) by the Blockchain Observatory and Forum of the European Union (EUBOF) further explored the factors that necessitate the issuance of a digital euro and its likely effects. Specifically, the expert panel consisting of speakers from central banks (the European Central Bank (ECB), the Bank of Japan, the Bank of Canada), as well as the business sector (Libra, BOSCH, ENGIE and MAKER Foundation), theorised the potential benefits of a digital euro for financial services, the industry and society overall, and highlighted potential concerns and perils that could follow its issuance.

Main benefits of a digital euro

-  Supporting digitalization in the European economy
-  Response to a declining use of cash as a means of payment
-  Tackling sovereignty concerns related to foreign CBDC or private digital means of payment in the euro area

A critical analysis: As more than [80% of central banks are engaged in CBDC work](#), the COVID-19 pandemic has accelerated the trend in digital payments and e-commerce, digital currencies such as Bitcoin and Ether are maturing and exhibiting novel features, private tech giants such as Facebook are working on privately-issued global monies, and foreign jurisdictions are at the latter stages of the issuance of a CBDC to facilitate a digital-world economy. Europe is feeling the pressure to keep up, or, in certain cases, catch up. This is especially evident as the discussion for a digital euro has largely shifted from a wholesale CBDC reserved for

use by commercial banks to a more innovative and impactful retail CBDC that can serve the needs of the private sector, households, businesses and end consumers.

A digital euro could support digitalisation, industry 4.0, accommodate for the declining use of cash, facilitate an even faster and more secure network of payments, financial services and e-commerce, and even serve as an on-ramp for private initiatives in the space. At the same time, it could cement Europe and the euro's leading position in the global economy and constitute a decisive response to foreign and private initiatives that pose sovereignty concerns. However, despite its transformative potential, the implications of a digital euro for monetary policy and the role of commercial banks are not yet fully realised. They largely depend on the digital euro's characteristics, novelty and specifics of its design. Significant work is required to ensure that a digital euro does not disrupt financial activity, diminish the role of current financial service providers, dominate the payments solution market, or adversely affect monetary policy and tools.

As the ECB is intensifying work on a digital euro, even issuing a [comprehensive report](#) and feasibility study, [it invites](#) public authorities, financial institutions and society at large to submit their own views and opinions before any final assessments on the issuance and characteristics of a digital euro are made.

Practical deployments of a CBDC – the cases of China and the Bahamas: While in Europe the issuance of a CBDC remains up for debate, in other areas of the world pilots and successful implementations of a state-backed digital currency are starting to emerge. China is spearheading efforts by implementing one of the biggest real-world CBDC trials. The Chinese government in Shenzhen carried out a lottery, or *airdrop*, to give away ¥10 million, worth approximately €1.3 million that consumers can spend at over 3 000 appointed merchants in the area. Out of 2 million applicants, 50, 000 won. At the same time, according to Fan Yi Fei, the Deputy Governor of the PBoC, ¥2 billion (€260 million) worth of transactions have been processed as part of the country's CBDC pilot, and the authority plans to test its digital yuan during the 2022 Winter Olympics of Beijing. ([source1](#), [source2](#)). On the opposite side of the world, the Central bank of Bahamas deployed the sand dollar, its national digital currency. According to the authority, the new state-backed digital currency aims “to advance more inclusive access to regulated payments and other financial services for under-served communities and socio-economic groups” and will be accepted “at any merchant with a Central Bank approved [mobile] e-Wallet.” ([source](#))

Blockchain and CBDC around the world: Over the past months, central banks from East and South East Asia are moving forward with practical implementations, pilots and collaborations on state-backed digital currencies. They have emerged as more open and advanced than the reactive position adopted by the ECB. The Bank of Japan (BOJ) announced a three-stage testing of a retail CBDC, with the latter stage involving the private sector, namely businesses and consumers, with a focus on examining the safety and feasibility of digital currency payments compared to cash ([source](#)). Besides the BOJ and PBoC, CBDC exploration has been peaking over the past months in Asia, with the Bank of Thailand announcing the development of a prototype CBDC ([source](#)), and the Monetary Authority of Singapore (MAS) announcing a cooperation with the PBoC on a new digital currency ([source](#)).

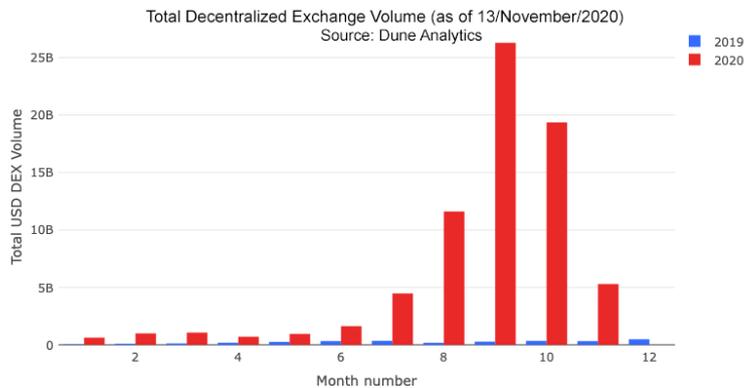
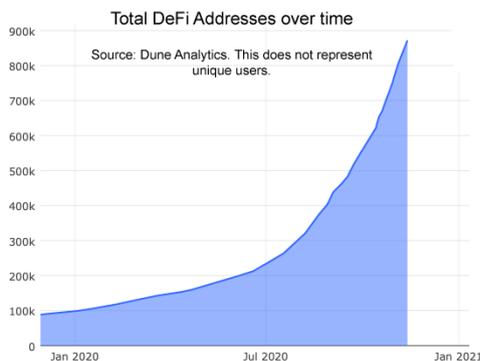
In Europe, Estonia, often described as a “digital nation”, launched a research project for a potential CBDC through its central bank. The Bank of Estonia, in collaboration with technology companies Guardtime and The SW7 Group, will examine whether the existing KSI distributed ledger deployment, a technology that shares many characteristics with blockchains and used in the country's e-governance public services, is suitable for the deployment of a digital currency. ([source](#)). In a strategic plan outlining its priorities over the next five years, The Bank of Spain, the central bank of Spain, highlights CBDC research as a priority under the theme of “New Technologies and Information Sources”, citing that it will explore its design and implications for the financial system and the economy as a whole. The effect of negative interest rates on banks and COVID-related market stress will be also explored. ([source](#))

The Reserve Bank of Australia, in partnership with Commonwealth Bank, the National Australia Bank, Perpetual and ConsenSys, announced an exploratory project for an Ethereum-based proof of concept for a CBDC. The project is set to complete in late 2020, with the first findings being published in the first half of next year. ([source](#)). In South America, Nicolás Maduro, president of Venezuela, as part of the country’s set of strategies to stimulate the national economy, announced a [new decentralised stock exchange](#) built on Ethereum. Traders are able to buy and trade tokenised versions of traditional, real and financial assets such as derivatives, commodities, real estate, stocks and bonds.

Other industry news

PayPal enters the race: In a relevant press release, PayPal announced that users will be able to buy, hold, sell and spend digital currencies at over 26 million merchants by early 2021. Dan Shulman, CEO of PayPal, commented on the inevitability and potential of digital currencies: “The shift to digital forms of currencies is inevitable, bringing with it clear advantages in terms of financial inclusion and access; efficiency, speed and resilience of the payments system; and the ability for governments to disburse funds to citizens quickly.” In the same press release, the company recognises the rising trend towards digital payments driven by COVID-19, cites the limited utility of digital assets as one of the reasons for their lack of mainstream popularity and positions PayPal as the facilitator of widespread adoption. ([source](#))

DeFi – all-time highs and novel attacks: As the DeFi space continues to expand rapidly, with [over €10 billion total value locked](#) in smart contracts as of October 2020, and an [all-time high](#) in decentralised exchange volume and unique addresses, novel attacks on decentralised protocols are emerging, too. A theorised “attack” on liquidity dependent protocols was realised in early September, attracting more than €1 billion worth of liquidity from decentralised exchange Uniswap to Sushiswap. The so-called “[Vampire Attack](#)” involved strong incentives in the form of a governance token for providers that migrate liquidity to the new exchange in an attempt to acquire the platform’s liquidity, users and trading volume. Following a series of missteps, and a counter-launch of Uniswap’s own governance token, the “attack” was largely deemed unsuccessful.



Relevant suggested reads: [Geopolitical Ramifications of a Major Digital Currency](#), [Deutsche Bundesbank – On the Future of Money and Payments](#), [ConsenSys Q2-2020 DeFi Report](#), [Digital Money Across Borders: Macro-Financial Implications](#), [Security and convenience of a central bank digital currency](#), [Bank of Russia – A Digital Ruble](#)

Technological Updates & Product Releases

Eth2 Launch – Serenity

Eth2 is a long-planned upgrade to the Ethereum network, engineered to upgrade the scalability and security concerns of the current Ethereum blockchain. Among the cornerstone updates is the energy consumption of transactions, since the biggest smart contract blockchain will migrate from Proof of Work (mining) to Proof of Stake (capital risk). Similarly, Serenity – as officials named the new version – will introduce shard chains, parallel blockchains that sit within Ethereum and take on a portion of the network’s processing work. This means that in Eth2, nodes will be dispersed across a subset of shards, leading to an increase in Ethereum’s transactional capacity.

In Proof of Work (PoW) blockchains, miners use advanced hardware with large computing power to solve complex mathematical puzzles in order to verify new blocks of transactions. This process is energy-intensive, with numerous debates around the environmental sustainability of blockchain networks. Proof of Stake (PoS) is different since validators are selected proportionally to the value of cryptocurrency they lock in the staking contract. Most PoS blockchains introduce slashing to avoid risks related to a network attack, so validators are putting their capital into risk.

Serenity is expecting to facilitate up to 100,000 transactions per second, significantly higher than the 15 transactions that Ethereum blockchain can handle right now. Security and decentralisation are key priorities for this update. The network is architected to be operated by at least 16,384 validators.

Prior to a mainnet release, a series of testnet launches involving Topaz, Medalla, Spadina and Zinken were made available to the tech community. The release will take place in three phases: Phases 0, 1 and 2.

Phase 0 is expected to commence in December 2020. Phase 0 will be an implementation of the Beacon Chain (BC). BC stores and manages the registry of validators, as well as deploys the PoS consensus mechanism. Phase 1, which is expected in 2021, will see the integration of shard chains. The launch will include 64 shards, though the shards will not support smart contracts.

Phase 1.5, which is also expected to take place in 2021, will integrate the current Ethereum mainnet as a shard of the Serenity. Phase 2, which is likely to take place during 2022, will see shards become fully functional and compatible with smart contracts.

Eth2 ROADMAP

Eth2 consists of upgrades to improve the scalability and security of the network. Each milestone is being worked on in parallel, though the dependencies determine the deployment timeline.

1

The BEACHON CHAIN



The Beacon Chain will act as the coordinator of the new system, introducing staking to Ethereum and act as the foundation for future upgrades.

December, 1st 2020

2

SHARDING



Shard Chains will expand Ethereum’s capacity to process more transactions. The shards will be upgraded with new features over time, rolled out across 2 main phases.

Expected: 2021

3

DOCKING



The current mainnet Ethereum will be merged with the new beacon chain as a shard. This will enable staking for the entire network, along with eliminating the energy-intensive PoW mining.

Expected: 2022

Blockchain Interoperability & Cross-Chain Transactions

Connecting multiple distributed ledger technologies with cross-chain bridges has been one of the key advancements in the blockchain ecosystem during Q3 2020. Numerous prominent Layer 1 & Layer 2 blockchains have released bridges that currently mainly serve to make them more accessible to users and assets across different DeFi systems. One of the most characteristic examples is lending Bitcoin for high-yield financial instruments on Ethereum has surpassed \$1 billion on chain management. When we refer to cross-chain transactions, we do not refer to asset transfers via atomic swaps with hash time locked contracts. A relay bridge implements a bi-directional relay of block headers between two blockchain infrastructures. One example is the BTC Relay that implements a unidirectional relay from Bitcoin to Ethereum. The Ethereum Smart Contract computes the difficulty of the submitted Bitcoin headers, a proof of the validity of each header amounts to checking if it resides on the longest chain of submitted headers.

Until today, solutions about the blockchain interoperability problem have been either centralised solutions, atomic swaps, also called the Hashed TimeLock Contracts. Similarly, Atomic Swaps, while they facilitate cross-chain exchange of assets, are not technically interoperable solutions since it is an agreement between two peers on a value transaction that will move across two chains through a time locked contract.

Below is a representation of recent technological approaches in the interoperability domain by different ecosystem actors. The list is not exhaustive, but acts as a reference to timely use cases:

Rainbow Bridge: NEAR’s Rainbow Bridge uses light clients to transfer ERC-20 tokens from Ethereum to NEAR’s PoS blockchain and vice versa. For each chain, the Rainbow protocol deploys a smart contract that implements a light client and relay nodes that regularly sends block headers to the light client. Namely, Ethereum relays (aka ETH-2-NEAR relays) sends every single Ethereum header to the NEAR contract, while the NEAR relays (aka NEAR-2-ETH relays) sends one header every four hours to the Ethereum contract. As a result, both contracts can independently verify the inclusion of any event on the other chain.

XCLAIM: XCLAIM is a framework for trustless, cross-chain exchanges where a smart contract on each chain governs the exchanges between the two chains (e.g. Bitcoin and Ethereum) and punishes malicious parties by seizing their collateral in favour of honest parties. The XCLAIM model consists of three main entities: a client who wishes to move funds from Bitcoin to Ethereum, a vault that locks the Bitcoin funds received from the client, and an Ethereum relay contract known as BTCRelay that stores Bitcoin block headers to allow verification of Simplified Payment Verification proofs.

Waterloo: Kyber’s Waterloo is a cross-chain bridge between Ethereum and EOS. An Ethereum smart contract serves as a light client that only verifies EOS block headers. The consensus protocol of EOS is based on the delegated PoS mechanism, where EOS token holders continuously vote (i.e. delegate) for their favourite block producers. Instead of relaying all EOS block headers, the Waterloo relay only relays the changes in the set of EOS block producers.

Horizon: Harmony’s Horizon Bridge is a gas-efficient, cross-chain bridge protocol to transfer assets from a Byzantine Fault Tolerant (BFT) blockchain to another blockchain (e.g. Ethereum) that supports basic smart contract execution. Horizon consists of a super-light client for BFT chains that allows a client to prove to any external entity that a transaction has been recorded on the BFT chain by providing a cryptographic proof of logarithmic size in the length of the chain.

Cross-chain composability and interoperability is expected to continue advancing, with many new trustless innovations to be created.

Blockchain oracles - Making Sense of Price Oracles in DeFi

A blockchain oracle is any device or entity that connects a deterministic blockchain with off-chain data. These oracles enter every data input through an external transaction. This way, we can be sure that the blockchain

itself contains all of the information required to verify itself. This is why oracles are known as blockchain middleware: they are the bridge between the two worlds.

The need for having oracles is driven by the fact that smart contracts require a secure middleware to connect them to real-world data. This external data will trigger the contract, creating the need for its high reliability. Real-world applications until today were limited, but with the growing popularity of DeFi, oracles are now applicable. It makes a strong case for the adoption and usage of oracle projects, and suggests that price oracles are an integral part of the decentralised financial services infrastructure. The Ethereum ecosystem features mainly four Decentralised oracle projects: Chainlink, Band Protocol, Teller and Nest Protocol.

- Chainlink is the leading decentralised data oracles network. The oracles are secure, resistant to manipulation, and thus reliable. The Chainlink project is at the forefront of decentralised data oracle innovation and constantly introduces new data pairs/services to advance the field. Its value accrual is secured by the fact the node operators must be paid in LINK and that most crypto-based services need reliable/secure data for their smart contracts for effective and stable operation. Chainlink provides feeds for 55 trading pairs, including 30 fiat pairs. At least \$2.5 billion are locked values in crypto assets that are referencing to Chainlink price oracles.
- Band Protocol beyond cryptocurrencies can also connect to trusted data sources such as weather, the lottery, or even the unemployment rate through traditional Web APIs with customised oracle script. BAND is also a cross-chain (compatible with multiple blockchains) decentralised data oracle project that provides and manages real world data to smart contracts.
- Tello takes the old-fashion PoW method combined with the staking concept to maintain data quality. Users can request data by adding the Teller token as a tip.

Ethereum decentralised oracles are likely to fail to update due to the Ethereum network congestions and extreme market conditions, like the one on Black Thursday.

The cross-chain trend is also applicable to the Decentralised Data Oracles industry. For example, Kylin Network is building a cross-chain platform powering the data economy, which aims to be the data infrastructure for DeFi and Web 3.0 powered by Polkadot. The Open API and SDK of Kylin Network offers any applications and blockchains (such as parachains and parathreads) instantaneous but transparent, reliable and valid on-/off-chain market data and social data sources by leveraging the power of Polkadot/Substrate Framework on open networks.

COMPARISON OF DECENTRALIZED ORACLES

		 Chainlink		 tellor	
Data Collection	DPos	Nodes Price Feed	Validated Data Feeders via oracle & arbitration nodes; POS	Quotation Mining	PoW with Medium Selection
Blockchain Integrations	Ethereum, Cosmos, Tron, Harmony	Blockchain-Agnostic	Polkadot, All chains via Bridge-Chaining	Ethereum	Ethereum
Validation or Dispute	Slash	Slash & Reputation Mode	Arbitration & Oracle Node, slashing of failed challenges, reward for validated data	Arbitrage	Slash
Price Feed Threshold	Non Applicable	By pairs	Non Applicable	Minimum Cost of Arbitrage	Non Applicable
Heartbeat	Non Applicable	2 Hours	Relay Chain via Polkadot	Non Applicable	One (1) Block
Key Risk Factors	Price Delay & Price Deviation	Price Delay & Price Deviation	Price Delay & Price Deviation	Price Delay & Price Deviation	Price Delay & Price Deviation
Supported Data	Price Feeds, Weather, Unemployment	Price Feeds	Price Feeds: any feed accessible via OCWs theoretically	Price Feeds	Price Feeds

Regulatory Updates & Financial Updates

EU

General legal framework changes

European Commission proposes special rules for digital assets

The Markets in Crypto-Assets (MiCA) was adopted by the European Commission on 24 September to ensure EU consumers get access to innovative yet safe cryptocurrency without detriment to market stability. The safety of crypto market participants is its main task, which has to be balanced against the requirements for more innovative investment products, and the regulatory and financial risks associated with the widespread use of insufficiently verified assets such as stable coins. The EU suggested to pay attention to the interaction of the virtual service providers to the European market in order to benefit from its financial services.

The MiCA outlines four main tasks:

- Legalise crypto-assets that have to be covered by EU financial services;
- Provide equal rules for Virtual Assets Service Providers (VASPs) across Europe;
- Change current governmental rules applicable to crypto-assets;
- Guarantee special laws for 'stablecoins', including when these are e-money.

Legalisation of Bitcoin ATM in Germany

ATMs that provide services for digital assets such as Litecoin and Bitcoin now require a license from BaFin, Germany's financial regulator, according to a statement by the authority. Moreover, BaFin mentions that "[p]roprietary trading is a financial service and financial commission business is a banking business, for which prior approval from BaFin is required."

Worldwide

Taxation regulations changes

Israeli regulators suggest tax crypto as a currency, not an asset

Israeli authorities proposed significant changes to the current taxation laws body in order to abolish capital gains from digital assets. Presently, digital assets investors' gains taxed withhold is 25%.

New Zealand releases tax guideline

According to the Inland Revenue Department, New Zealand provided a crypto-asset guideline that clarifies income taxation rules for both entities and individuals.

FinCEN plan to get information about transactions more than \$250

The Financial Crimes Enforcement Network (FinCEN) and the Federal Reserve intend to decrease the \$3,000 threshold to \$250 for international transactions. This means that agencies should get the exchange information of transaction issuers if the amount of the transaction is greater than \$250.

General legal framework changes

US Cyber Digital Task Force presents new crypto guidance

The US attorney provided detailed information about the regulation for digital assets and blockchain technologies, and their possible usage within illicit activities. In addition, it provided a list of tasks and strategies for VASPs.

Cayman Islands propose new regulatory framework for digital assets

Authorities introduced a list of rules in order to provide Anti-Money Laundering and Countering the Financing of Terrorism compliance for VASPs. After the rules entered into force, VASPs have to register with the Cayman Islands Monetary Authority. The next step, approximately in June 2021, will be for VASPs to also comply with licensing requirements.

US SEC provides simplified offering rules for securities

The Securities and Exchange Commission (SEC) voted for adopting changes to certain rules in order to modernise the existing framework and simplify the offering conduction process for companies.

The Bahamas announce the launch of CBDC

The Central Bank of the Bahamas is ready to present the release of its digital currency known as “Project Sand Dollar”. Such a step can make the Bahamas one of the global pioneers in the access to a central bank digital currency.

Peru starts preparing for crypto regulation in the country

A Peruvian regulator authority started to thoroughly research local cryptocurrency exchanges. The insight gained should be key to providing the legal status, functioning and mechanisms of digital assets in the country.

Malaysian Securities Commission reviews existing crypto assets guidelines

The updated guidelines should support the current Securities Commission objectives in providing valuable innovations to the current framework for VASPs, while at the same time lowering risks and protecting the interests of issuers and investors.

China’s central bank proposes regulatory framework for CBDC

The People’s Bank of China prepared a framework with laws to legalise digital yuan and describe the status of other virtual assets.