Regulatory Updates

According to [recent reports](), countries representing over 90 % of the worlds GDP are actively engaged in some form of Central Bank Digital Currency (CBDC) work. While the interest of central banks in the issuance of their own digital currencies is not new, [raging global competition]() in the field, and the emergence of a common supportive narrative for CBDCs has accelerated developments.

In terms of competition, most CBDC projects fall under the research or the early development phases. Leaving the US further behind, China and the EU have moved forward with pilots, and the Caribbean region concentrates all live CBDC deployments which can be found in the Bahamas, Saint Kitts and Nevis, Antigua and Barbuda, Saint Lucia, and Grenada. Jamaica too recently announced a plan of a CBDC pilot within August. With regard to the common narrative, CBDCs are increasingly and unanimously positioned as a privacy-respecting and environmentally sustainable alternative to stablecoins and cryptocurrencies, which can also further the financial sovereignty of the issuing area.

As an increasing number of projects move towards research pilot implementations, research is gradually shifting beyond the design space and options for CBDCs. The first quantitative studies aimed at measuring the tangible impact of CBDCs for money or credit creation and interbank procedures are starting to surface. As are experiments that go beyond payments and involve the settlement of other financial instruments or are related to identities.

Europe

On 14 July, the Governing Council of the European Central Bank (ECB) [announced plans]() to move forward with a 2-year project exploring the issuance of a digital euro, Europe's version of a CBDC. The ECB's decision to pursue a digital euro is especially seminal due to the size and influence of the European economy, the potential impact of a digital euro in the development of other CBDCs, and the shift in the power dynamics of the global race for the digital markets of the future. In the latter, Europe has emerged as the definitive runner-up to China, leaving the US further behind.

The ECB's announcement was preceded by an extensive report outlining the desirable characteristics of a digital euro, the launch of a public request for consultation to identify specific areas that might require special attention, and even experiments that yielded "encouraging results". Notably, all bets are off in the matter of the design specifics and distribution of a digital euro, meaning that its effects for the wider banking sector, end-consumers, and even the changes to the regulatory landscape are still uncertain. Europe's decision to commence a 2-year investigation period is to provide answers to the questions above. This approach is not unique and has yielded valuable insights when adopted by various countries such as Sweden.

Despite its as of now ambiguity in terms of design, distribution, and impact, the digital euro seems firmly positioned as a privacy-conscious alternative to private digital currencies, and a tool for strengthening the financial sovereignty of the Euro Area. As noted, this falls in line with how the global CBDC landscape is expanding. In the ECB's relevant public consultation, respect for privacy overwhelmingly emerged as the most important point of special interest. In a recent report by the ECB, economists Massimo Ferrari and Arnaud

Mehl highlight how money issued by "foreign tech giants" can threaten financial stability and how the digital euro can serve as an alternative. Along the same line, Fabio Panetta, executive board member of the ECB stated that, unlike private companies, the ECB has no commercial interest in monetising the data of users. Mr Panetta also provided specific examples of how the ECB is working towards a privacy-respecting euro, by testing offline payments for small transactions where identities are only revealed to the parties enmeshed in the exchange.

As highlighted, beyond the implications of the digital euro for the financial sovereignty of Europe, and the privacy of its citizens, applications that fall outside the realm of regular money are also explored. Indicatively, in late June, the Bank of France in collaboration with the popular Swiss cryptocurrency Bank announced the successful completion of a CBDC experiment, which involved the settlement and delivery of listed securities on TARGET2-Securities in exchange for CBDC. This test was part of a larger initiative launched last year by the Bank of France, that aims to explore interbank integration of CBDCs. This successful test is one of the many similar experiments conducted by banks in Europe and comes at a time where alternative applications for CBDCs beyond payments are starting to be explored. In a press release, the innovation Hub of the Bank of International Settlements announced that it will join the efforts of France and Switzerland by collaborating in a cross-border CBDC experiment to "investigate the potential benefits and challenges of wCBDC in settling cross-border payments and digital financial instruments."

China

In China, pilots of the country's CBDC, the digital yuan (also known as DCEP) are expanding. According to an official announcement, the Beijing subway will start accepting DCEP for its transport services, following the example of another province, Suzhou. Beijing has emerged as one of the epicentres of China's DCEP pilots and is home to more than 3 000 special ATMs that allow for deposits and withdrawals in the country's CBDC.

In line with the developments above, Li Bo, governor of the People's Bank of China, stated that the Winter Olympics of 2022 could serve as an opportunity for testing DCEP with foreign users. The Governor noted that China's CBDC is to facilitate domestic payments and international trade, and while cross-CBDC functions are explored, the goal is not displacing the US dollar as the world's dominant currency. In response to the plans announced by Governor Bo, three US senators signed a letter in an attempt to prevent US Olympian athletes from using China's CBDC, citing concerns over privacy and tracking by the Chinese Communist Party. The Chinese minister of foreign affairs responded by accusing the US senators of ignorance and politicking.

Rest of the World

While Japan is still figuring out the basic characteristics of a potential digital Yen, such as design and distribution, to counter China's progress, cross-CBDCs compatibility will be an important consideration according to Hideki Murai, head of the Democratic Party of Japan. The Monetary Authority of Singapore is offering cash prices in a global challenge, for retail the CBDC solution that further financial inclusion and promote payment speed and efficiency.

Despite the absence of a formal announcement, Andrew Abir, deputy governor of the Bank of Israel, confirmed that the Bank is moving forward with a pilot for a potential digital shekel. The experiment is to examine whether the benefits of a CBDC outweigh the costs and potential risks. Referring to a potential digital shekel, Mr Abir noted that "What we are talking about is a payment system. Bitcoin is not a payment system, and it is not a currency. In the best situation, it is a financial asset, and in the worst case, it is a pyramid scam."

In Africa, Ghana and Nigeria are rapidly approaching the issuance of digital sovereign money. Ghana is striving to be the first nation in Africa to issue a CBDC with Ernest Addison, governor of the Bank of Ghana stating that the Bank is in the advanced stages of creating a CBDC. Mr Addison also added that CBDCs offer an attractive medium of exchange and store of value, unlike the more volatile cryptocurrencies. In Nigeria, where cryptocurrency transactions are banned, the country's CBDC is aimed to address the issue and to ease foreign remittance restrictions.

Market updates

Following a 60 % price drawdown over the summer months, the latter half of July has seen Bitcoin and other major currencies rebound around 30 %. The blockchain market continues to evolve despite these fluctuations with a significant tempo. So far, in the past month, the industry saw significant investments. For instance:

- Revolut, a popular British banking software that allows users to invest in cryptocurrencies, has raised $800 million in a fresh round of funding. According to CNBC, the latest funding round is led by SoftBank, a Japanese financial powerhouse, and Tiger Global, a US hedge fund, which together own about 5 % of Revolut.
- Crypto Finance AG, a Swiss digital asset business, has been purchased by Deutsche Boerse. The German stock market operator has acquired a two-thirds interest in the digital asset firm, according to a press statement. The acquisition price was in the "modest three-digit CHF million range," according to Deutsche Boerse, however, the financial specifics of the sale have yet to be released. Once all parties have received regulatory approval, the stock purchase transaction will be completed in Q4 2021.
- Solana completes a $314 million raise in a token sale that featured the participation of recognisable crypto investors. Solana is a project that implements the proof of history to enhance the transactions speed/that makes use of the sharding technique for enhancing the transactions speed. The funding will allow the further expansion and development of the network.

Traditional businesses are also trying to expand their influence by implementing blockchain technologies and by cooperating with crypto companies:

- With Visa's acquisition of London-based startup Currencycloud, the borders between established payment networks and fintech are becoming increasingly blurred. Visa announced that it has reached a formal deal to buy Currencycloud, a fintech platform that serves roughly 500 financial and technology clients in over 180 countries. The new purchase will help Visa strengthen its foreign exchange business and broaden its reach to include financial institutions, fintechs, and other partners.
- Mastercard has announced plans to overhaul its crypto card program, allowing traditional banks and crypto businesses to provide cards to their customers for digital asset transactions. The New York-based banking institution has announced new agreements with Circle, Paxos, Evolve Bank & Trust, Metropolitan Commercial Bank, Uphold, BitPay, Apto Payments, i2c Inc., and Galileo Financial Technologies to give its consumers access to cryptocurrencies.
- S&P Dow Jones Indices, the world's largest index provider, has developed a new cryptocurrency index that measures the performance of the larger digital asset sector. At debut, the S&P Cryptocurrency Broad Digital Market Index, or BDM, covers more than 240 digital assets, expanding on the firm's recently introduced crypto benchmarks.
- As the e-commerce giant moves on with its plans to bring its payment systems into the crypto era, Amazon is looking to employ a "digital currency and blockchain product lead."
- Nueva Pescanova Group, a Spanish seafood company, has established a partnership with IBM to use IBM's Food Trust platform, a distributed ledger technology platform for supply chain traceability. The

cooperation is already underway, according to an IBM statement, with Nueva Pescanova using blockchain technology to track shrimp fishing in Argentina and prawn farming in Ecuador.

- Customers who want to use their cryptocurrency to buy goods at H-E-B stores in Texas may soon be allowed to do so. According to the Houston Chronicle, Coin Cloud, a crypto ATM company, is planning to deploy machines at 29 H-E-B stores in the Houston region.
- A private secondary school near the Nigerian city of Kano has declared that it would accept cryptocurrency payments for school fees, despite the country's central bank prohibiting financial institutions from providing services to cryptocurrency exchanges.
- Issuing, storing, and circulating health certificates is an emerging blockchain use case especially during the COVID pandemic. In this fashion, the airline ticket distribution company, Amadeus, has placed its faith in IBM's Digital Health Pass. The integration of the blockchain platform will help in streamlining the validation process by minimising the bureaucracy and accelerate the check-in procedure
- Allianz, the insurance company, has adopted blockchain to build a platform that streamlines international motor insurance claims.

Moreover, the crypto ATM industry also continues to expand with rapidly. According to ATM radar, this year, the number of crypto ATMs deployed worldwide rose by more than 70 % to 24 030. The 10 037 machines installed in 2021 have already surpassed the 7 620 introduced in 2020 with five months left in the year. The world's largest Bitcoin ATM operator has announced that it would expand into Circle K stores across the United States and Canada. As part of the new collaboration, Bitcoin Depot said today that more than 700 of its Bitcoin ATM machines have already been placed in Circle K convenience shops in 30 states. The expansion, according to the crypto ATM distributor, may give financial access tools to underprivileged regions and draw more individuals to the crypto ecosystem.

On the other side, traditional banking systems also continue to implement cryptocurrencies.

- According to The Korean Economic Daily, Woori Financial Group, the group's banking subsidiary, has become the latest major South Korean financial institution to announce the implementation of digital asset custody services. The group is collaborating with Coinplug, a Bitcoin-based fintech business, to launch D-Custody, a joint venture for digital asset custody. Coinplug will be the largest stakeholder in D-Custody, followed by Woori Bank.
- As the Ukrainian government moves forward with cryptocurrency legislation, a prominent local e-bank is planning to offer a debit card that would allow users to trade Bitcoin (BTC). Monobank, a Ukrainian online banking application, has completed a trial integration with a cryptocurrency trading platform, according to Monobank co-founder Oleg Gorokhovsky. According to the CEO, the new connection would allow Monobank customers to purchase and sell Bitcoin using a debit card.

The sports industry is also gaining traction with the adoption of blockchain technology. The activity is primarily connected with football and motorsports:

- Arsenal F.C., a Premier League mainstay, is releasing a new fan token in collaboration with Socios, offering its followers the power to influence club decisions and access team-related information.
- The Turkish Union of Clubs, Turkey's major soccer league, has collaborated with fan interaction platform Socios.com to encourage innovation in the country's soccer scene.
- Portugal's national football squad will be available to local supporters in the coming days. The digital assets, like previously tokenised sports teams, are minted on the Chiliz blockchain and allow token holders to vote in polls and earn VIP benefits.
- Fantasy soccer game based on blockchain Sorare has established a licensing agreement with a national sports organisation to create nonfungible tokens of its athletes. The France Football

Federation, or FFF, is one of [120+ clubs](#) and teams who are introducing their own line of nonfungible tokens for players.

- The South American Football Federation (known as "CONMEBOL") has announced a collaboration with Ethernity Chain to mint NFTs. The NFT will be modeled after the trophy awarded to the victor of Copa America, South America's premier continental competition.
- Cryptocurrency exchange Crypto.com has [announced](#) that it would collaborate with Formula 1 this year in its racing series. Formula 1 said that Crypto.com will be the new worldwide and inaugural partner for its 2021 Sprint series, which will begin on 17 July. The exchange will become the racing series' official cryptocurrency and nonfungible token, or NFT, partner as part of the arrangement, which CNBC [claims](#) is worth $100 million.
- Landon Cassill, a NASCAR Xfinity Series racing car driver, will get a portion of his pay in Bitcoin and Litecoin as part of a [partnership](#) with crypto broker Voyager.

Technological Trends & Developments

Deep Dive on Ethereum's London Hard Fork

Ethereum's London hard fork has been activated on block 12 965 000 on 4 August introducing the EIP-1559 which is introducing important reforms in the gas fee markets, along with structural changes on how gas fees refund are handled, and the ICE Age schedule. The London upgrade includes five EIPs: EIP-1559: Fee market change for ETH 1.0 chain, EIP-3198: BASEFEE opcode, EIP-3529: Reduction in refunds, EIP-3541: Reject new contracts starting with the 0xEF byte, and EIP-3554: Difficulty Bomb Delay to December 2021.

Understanding Ethereum Improvement Proposal (EIP)- 1559 – one of the most anticipated upgrades

EIP-1559 has evolved into one of the most anticipated upgrades in the history of Ethereum, which introduces a burning function of a significant portion of the transaction fees on the protocol, and inaugurates variable block sizes to improve efficiency. EIP-1559 is introducing a "base fee" in blocks on the network which tracks the gas price that the network will accept from transactions based on demand for blockspace. It constitutes easier for wallets and other users to estimate the expected price for the transaction, rather than predicting and potentially overpaying by depending on historical data. EIP-1559 structures a new transaction type that allows users to define the maximum fee they are willing to pay, along with the maximum they are willing to pay to the miners and receive a refund for the difference between the maximum and the base fee & miner tip. This should help eliminate the number of failed transactions, while users are protected from overpaying for transaction fees. The upgrade is expected to affect negatively Ethereum miners, while constituting the value proposition of Ether more valuable due to elements of scarcity. At the same time, it is optimising the predictability of the network's gas fees. The update is introducing a new base fee model with an additional miner tip, which is replacing the current first-price auction fee mechanism. Given the depth of the EIP-1559 is recommended to review the list of resources, along watching the PEEPanEIP episode about the Ethereum Improvement Proposal.

EIP-3198: BASEFEE opcode

EIP-3198 is adding an opcode, BASEFEE, which returns the value of the base fee for the block it is executed. Small Contracts will access this value on chain, by submitting fraud proofs and creating trustless gas price derivatives. This will enable smart contracts or dApps to get the value of the base fee immediately.

EIP-3529: Reduction in refunds

EIP-3529 removes gas refunds for SELFDESTRUCT and reduces gas refunds for SSTORE. This has been introduced as an incentive for developers to develop applications to use efficiently storage and decrease redundant codes. These operations motivated the creation of gas tokens which served to store gas when the gas price was low, and redeemed when the gas price has been higher. The technique though has proven that results were not those as initially anticipated, and the gas refunded caused multiple unexpected negative outcomes. Those have caused network downside, by exacerbating state size and inefficiently clogging the gas fee usage. The EIP refunds the gas fee when the variable storage is reduced.

EIP-3541: Reject new contracts with the 0xEF byte

The existing smart contracts starting with 0xEF byte will continue to exist, but new contracts will be rejected. EIP-3451 upgrade is necessary because of the implementation of EVM Object Format. The upgrade prevents Ethereum clients from confusion between smart contracts that are not in EVMOF.

EIP-3554: Difficulty Bomb Delay to December 2021

EIP-3554 is introduced to delay the difficulty bomb which is known as the ICE AGE. The ICE AGE mechanism was introduced in Ethereum to freeze mining as the network is transitioning to Proof of Stake. Due to the fact that the PoS transition is not yet ready, the developers are delaying when the difficulty bomb will go off. It happened again three times in the past (Metropolis, Constantinople, and Muir Glacier). The bomb is pushed back to December 2021.

Ethereum Reorgs

Among the topics that have emerged lately in the Ethereum ecosystem, is the capacity of Ethereum miners to modify the Ethereum client to accept bribes to facilitate short reorgs of the mainnet chain. Such a scenario could constitute the Ethereum network as a Wild West, while decentralised finance applications would be vulnerable. Ethereum Co-Founder Vitalik Buterin and Blockchain researcher Konstantopoulos Georgios have published a post evaluating the possibility of miners performing such reorgs. As a reorg, we refer to events that a block that has been a part of the canonical chain, but it is no longer valid because another block has been validated earlier- most probably due to increasing the fees spent. Finality is a critical concept in a decentralised network since it guarantees that a transaction is economically unsustainably to be reorganised. In the current consensus algorithm of the Ethereum network (Proof of Work), the rule of the longest chain is applicable. Short reorgs are not something strange, since those occur frequently due to the latency. Reorgs that exceed 2-5 blocks indicate a network failure, malicious attack or bugs. Short reorgs will not constitute the network vulnerable, are causing user experience degradation, uncertainty, and increase the chances to 51 % attacks. With the transition to the Proof of Stake algorithms, the researchers suggest that reorg even single-blocks will be extremely difficult because an attacker controlling only a few validators has no way to beat the honest majority of thousands of attesters. The report consults that malicious attackers require to control close to 50 % of all validators. Furthermore, long reorgs are not possible because blocks deeper than 2 epochs are considered finals - and it is impossible to revert them. The key takeaway from the paper is that the most effective prevention to Ethereum reorgs is to speed up the merge processor to even initiate an emergency merge to transition to the Proof of Stake algorithm. As we approach the transition, the risk of a potential reorg-attack is most likely since miners who are currently validating the blocks could be attracted to the idea of accumulating bribes or even stealing funds from decentralised finance protocols, since they are aware that their operations horizon is limited. The article concludes that post-merge to the Proof of Stake algorithm, the risk of reorg will not be considerable because small groups of malicious actors will not be able to reorg blocks.

EY contributes to a zero-knowledge proof layer 2 protocol to address increasing transaction costs on the Ethereum blockchain

EY Blockchain teams have previously contributed ZKP protocol as open-source software, under the name Nightfall since 2019. The EY team has since keep optimising the protocol to provide more efficient transaction handling, leading to reduced gas fees. Nightfall 3 is a layer two scalability protocol on the Ethereum blockchain, which combines zero-knowledge proofs with a new model for handling transaction verification to increase efficiency and lead to reduced transaction fees which are known as optimistic rollups. The protocol is known as ZK-Optimistic Rollup. The new protocol can achieve a cost of approximately 8,200 gas per transaction, while it is preserving privacy. This represents one-eighth of the cost of transacting on the Ethereum mainnet. Nightfall 3 comes provides developers with a standardised application interface that is similar to other token transfer tools. Currently, it supports transferring of ERC20, ERC721, AND ERC1155 token standards under Zero-Knowledge.

Coinbase introduced Solidify- a tool to automatically detect and classify smart contract security risks

Solidify implements security reviews by using a large signature database and a pattern matching engine to detect contract features along with their related risks, standardises and scores smart contract risks, and suggests mitigation strategies. The tool currently has 6 000 unique signatures. The tool currently is supporting only ERC-20 and similar tokens. The code will be open-sourced this year, while further developments will be focusing on improving the accuracy of signature generation and detection logic, and integrating formal verification techniques to reduce the need for manual analysis.

Chainlink Keepers Open Beta Is Live: A Fully Decentralised Service for Smart Contract DevOps

Chainlink announced the open beta phase for Chainlink Keepers in June. Keepers will aid smart contract developers, DAOs, and dApps to automate their smart contracts in a reliable, decentralised, and cost-efficient method. A set of operations that can compute in Keepers are Chainlink Keepers can perform a variety of compute operations, monitoring, and time- and event-based tasks for smart contracts, such as: Execute limit orders on decentralised exchanges b) Mint tokens when reserves increase c) Harvest yield from vaults d) Rebase elastic supply tokens e) Trigger automated trading strategies f) Liquidate undercollateralised loans g) Release locked assets after periods of inactivity h) Top up token balances falling below a minimum threshold.

Ripple announced Federated Sidechains on the XRP Ledger

The Ripple Foundation has announced its vision for the implementation of federated sidechains on the ledger. The foundation was pressured by the growing popularity of smart contracts in DeFi, but a fundamental commitment is on the efficiency of Ripple ledger. In brief, sidechains will operate as their own blockchain while XRP will act as a primary asset. The advantages that federated sidechains bring are horizontal scaling, low risk, low effort, and a long roadmap.