SEBA BANK

March 2021

Decentralised Exchanges
Trustless and Secure

The Bridge

Redefining Finance for the New Economy

Table of Contents

Authors

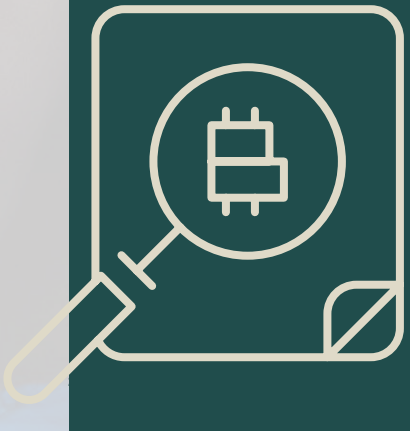
Yves Longchamp
Head of Research
SEBA Bank AG

Kunal Goel
Research Analyst
B&B Analytics Private Limited

Saurabh Deshpande
Research Analyst
B&B Analytics Private Limited

Contact

research@seba.swiss



Executive summary

Centralised Exchanges have played a pivotal role in the crypto asset ecosystem, acting as fiat ramps, custodians, exchange, market makers and VCs, thereby consolidating a lot of power and responsibility. On several occasions, however, they have lost investor money through hacks or fraud. Algorithmic smart contract-based decentralised exchanges offer a non-custodial solution, providing liquidity and value exchange without compromising the sacred tenet “not your key, not your cryptocurrency”.

In this issue of the Bridge, we cover how decentralised exchanges began, how modern DEXes work and the value they add to the crypto-sphere by enabling trustless and secure exchange of crypto assets.

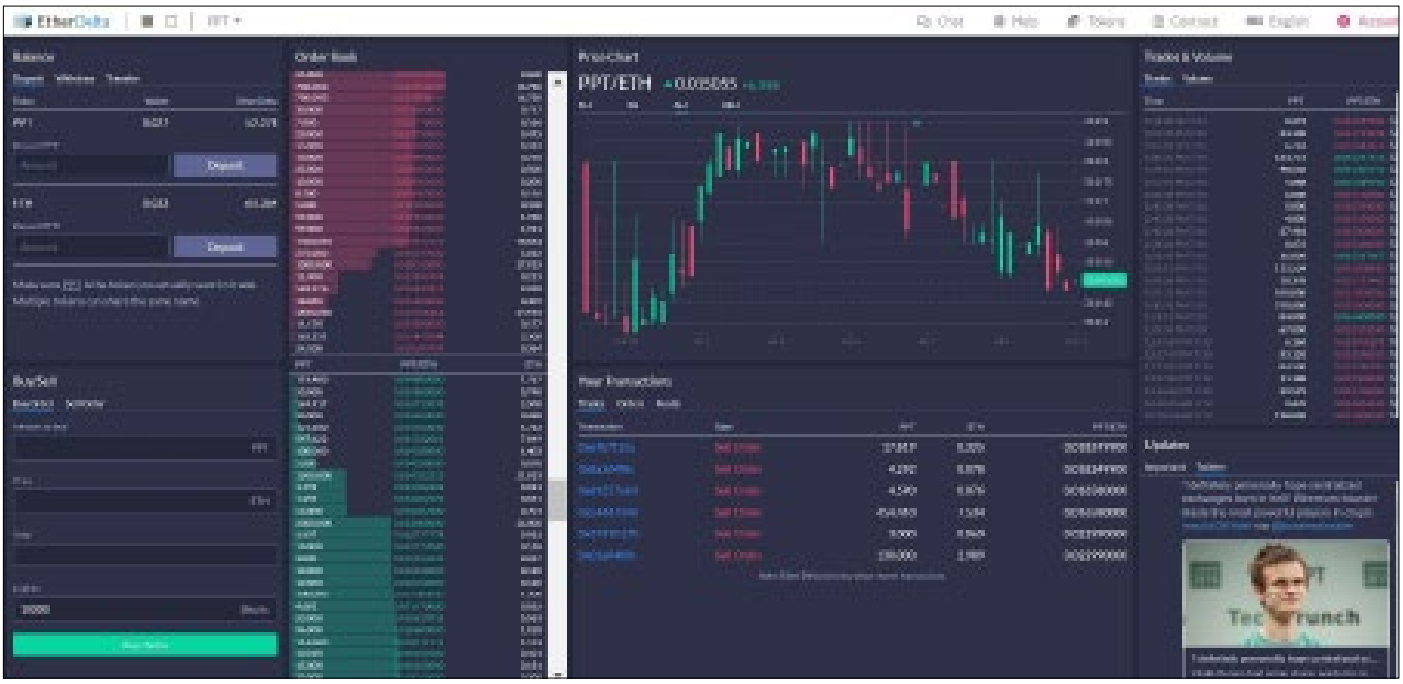
1.
Centralised and decentralised exchanges

Bitcoin started in 2010 as the first crypto asset, and the only way to acquire it initially was through mining or transacting with a miner. Mt. Gox, launched in July 2010, soon became the leading exchange to buy and sell bitcoins for US dollars. Enthusiasts did not have to mine or barter with miners to acquire bitcoin anymore. As the crypto universe grew and more assets populated the space, exchanges became increasingly pivotal as facilitators of transactions between crypto assets and against fiat. Today, about 300 exchanges support more than 8,000 crypto assets and 35,000 fiat and crypto pairs. New tokens are launched and listed every day, and exchanges play a crucial role in promoting the token and its price discovery.

Mt. Gox infamously filed for bankruptcy in 2014, losing its customers 650,000 BTC, valued more than USD 450 m at the time and USD 32 bn today. This served as a landmark case for the crypto world for two reasons - a black swan event would not mean there will be an extra-blockchain event to compensate the affected parties, and secondly, it exposed a vulnerability in the ecosystem where although the blockchain is impenetrable, the participants and custodians are not. Crypto asset exchanges provide services greater than those of exchanges in traditional finance, acting as brokers, market makers, custodians, investors and of course, the exchange platform. They hold and control an immense amount of value with little regulatory oversight and are prime targets for hacks and frauds. It was the Mt. Gox scandal that gave rise to the idea that if you are not the sole owner of the private keys to your wallet, it is not your crypto asset; in other words, “not your key, not your cryptocurrency”.

However, there was no clean solution available, with P2P having its flaws. Centralised exchanges (CEX) that replaced Mt. Gox, like Bitfinex, Poloniex, Kraken and Bittrex, remained central to the crypto world even while some suffered their own non-fatal breaches. The possibility of a non-custodial trustless exchange grew with developments on Ethereum and utilising the power of its smart contracts. During the Initial Coin Offering boom in 2017, with the launch of hundreds of new projects, the market need for a decentralised exchange (DEX) for free and permissionless listing also grew. Etherdelta, the first DEX (see picture 1), allowed the trustless transfer of crypto assets using Ethereum’s smart contracts and tried to fill this market need.

Picture 1: EtherDelta was the first DEX that allowed permissionless listing and trading of assets on the Ethereum blockchain



Source: EtherDelta Twitter

However, Etherdelta's UX was slow and clunky, with investors first needing to transfer assets to the exchange contract and all orders, fills, and cancellations being settled on the blockchain. There was also limited liquidity. Subsequently, there were attempts by the teams at 0x, Bancor and Kyber Network; however, no solution was elegant enough to gain serious traction. Relay by 0x had similar problems to Etherdelta with slow order flow and low liquidity, Bancor and KyberSwap needed central approval for listing and transacting, and because of lack of traction, they had high spreads. There was also the problem of needing a CEX to move value between crypto asset and fiat as they only allowed for transfer between assets on the Ethereum blockchain.

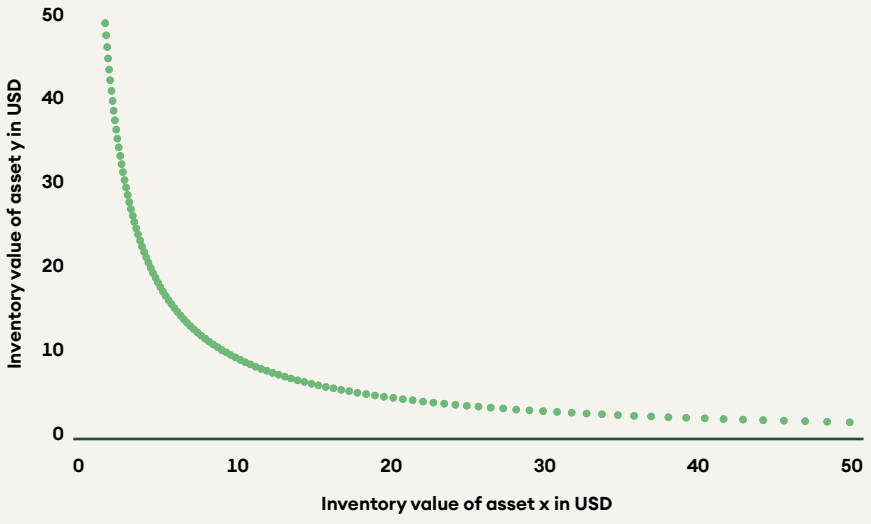
2.
Modern DEXes

Uniswap launched its upgraded version 2 in 2020 and became the first major DEX to provide a serious and decentralised solution to compete with centralised exchanges. It works as an Automated Market Maker (AMM) and has led the DEX space in users and volumes since. Following Uniswap's lead and model, other exchanges have come up offering similar services and filling the gaps in Uniswap's model. The success and popularity of DAI and USD-equivalents like USDT, USDC and wrapped assets like WBTC enabled value transfer between assets on the Ethereum blockchain with fiat and BTC, allowing investors to at least change the risk profile of their portfolio if not exit the space entirely. The assets remain in the users' custody, and any exchange is settled within a single block with traders acting as "takers" to the Liquidity Provider "makers". Please refer to the Digital Investor for more on how the participants' interplay.

We cover the types of modern exchange and the function they serve in a trustless system.

Constant Product AMM

Figure 1: Constant Product Model where the product of inventory levels x*y remains k = 100



Source: SEBA Bank

Popularised by Uniswap, AMMs are the most popular type of DEX. Instead of using order books, assets are priced algorithmically using a constant product formula x*y=k. Liquidity providers (LPs) pool their tokens against which traders can input their trades and earn a fraction of the trade value as fees. The product of the pool of tokens (x*y) must remain the same after the trade (i.e. equal to the constant k), which is why it is called the "constant product formula".

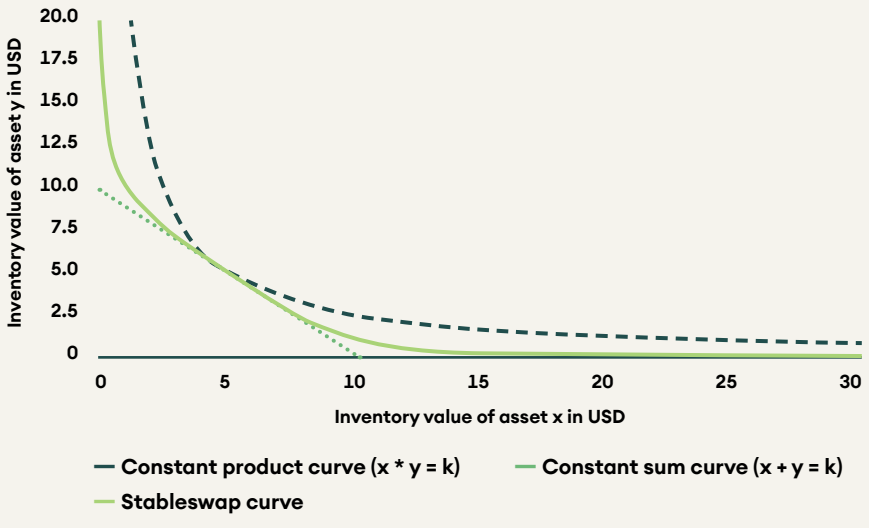
We use an example to illustrate how this works. To trade between ETH and USDC, assume a price ratio of 1 ETH to 2,000 USDC and a pool of 500 ETH and 1,000,000 USDC available in the liquidity pool. Here the k constant product value is 500,000,000. The contract will accept any transactions such that the product x*y remains equal to k, i.e., to buy 10 ETH, ~20,408 USDC will have to be supplied (490 * ~1,020,408 = 500,000,000) with the new price being 1 ETH = ~2,082 USDC. The slippage is directly proportional to the order size and inversely to the size of the liquidity pool.

This model has worked well for billions of dollars locked by LPs and traded by traders. However, it generates "impermanent loss" for the LPs. Impermanent loss is the fictitious loss suffered by liquidity providers for providing liquidity instead of holding the tokens separately. We continue the above example to illustrate this. For an LP who contributed 10% of the total pool, meaning initial ownership of 50 ETH and 100,000 USDC, the initial net worth is 200,000 USDC at 1 ETH = 2,000 USDC. Post-trade, the LP owned 49 ETH and 102,041 USDC, with a net worth of 204,081 USDC at 1 ETH = ~2,082 USDC. Had the LP held 50 ETH and 100,000 USDC, their net worth would be 204,123 USDC at 1 ETH = ~2,082 USDC. The difference of 42 USDC is known as impermanent loss. This loss goes to zero if the ratio returns to what it was at the time of providing liquidity, giving it the moniker impermanent loss. At this point, the fees earned by the LP would be pure extra profits versus holding the coins separately.

Uniswap is an Ethereum-based exchange, allowing swaps between ERC-20 tokens on the base layer of the Ethereum blockchain. Similar models have been implemented to other platform chains like PancakeSwap for Binance Smart Chain and Raydium for Solana. Newer projects like Loopring AMM allow for swaps on Ethereum layer 2 and Thorchain is building a cross-chain AMM.

Constant Sum Model for Similar Assets

Figure 2: Stableswap curve, constant product curve and constant sum curve



Source: SEBA Bank, Kyber Network DMM paper

The constant product AMM has different relative prices at all inventory levels and, therefore, does not work well for highly correlated assets, like wrapped tokens, synthetic tokens, and stable coins. For this, Curve pioneered a modified constant sum model, which allows for a 1:1 exchange for most inventory levels. As illustrated in figure 2, the modified constant sum model is linear with the same slope for a large part of the curve allowing for a constant exchange rate, while the constant product model has a variable slope and a variable exchange rate at every point. Only at extreme inventory levels is the price is considered de-pegged from the other pool asset, and the price is allowed to change.

The constant sum model allows for large transactions with low slippage in "similar" assets stable coins such as TUSD, USDT, USDC and DAI or wrapped and synthetic tokens such as WBTC, renBTC and sBTC. Since the price typically stays within a range, impermanent loss is not a feature of "stableswaps". LPs earn transaction fees while accepting the risk of a de-pegging of an asset.

NFT Exchanges

Rarible and OpenSea allow for the purchase and sale of art non-fungible tokens or NFTs. Art NFTs are unique tokens that may carry unique qualities and also have an audio/visual output. Bids and asks, therefore, need to be matched 1:1 for NFTs as the tokens are unique. Uniswap-like AMMs can only trade fungible assets as the assets are pooled and priced the same, having no differentiation from one another.

Aggregators

Ethereum has multiple DEXes like Uniswap, Sushiswap, Kyberswap and Curve, with different models, different liquidity depths (defined by the value k) and, consequently, different slippages. With multiple competing exchanges, it becomes difficult for users to find the exchange offering the best price. Aggregators have come up to help the user find the best rate across DEXes. Some of the more popular implementations are 1inch, Metamask, Zerion and 0x. Aggregators automatically find the best price for the users from the underlying DEXes, even splitting the order among the DEXes to ensure the lowest slippage and transaction cost, as seen in picture 2.

Picture 2: Routing provided by 1inch for a 100 ETH to WBTC transaction utilising Uniswap, Sushiswap, Kyber Network and a Private Market Maker

Source: 1inch Exchange

2.
The Case for Decentralised Exchanges

Now that we understand the different types of decentralised exchanges, it is also important to understand the need for them and what makes them better than centralised custodial exchanges.

Not your key, not your cryptocurrency

Those who have been in the crypto asset space long enough and have unfortunately been hit with hacks and breaches of trust learned the hard way the meaning of the phrase “not your key, not your cryptocurrency”. In our opinion, this reason alone is sufficient to support the case for decentralised exchanges. Having control over your assets without a central regulatory authority is one of the fundamental values that brought about bitcoin and the ecosystem. Whether it was Mt. Gox in 2014 losing 650,000 BTC, now worth USD 35 bn or Kucoin in 2020 losing funds worth USD 250 m, or Binance in 2021 removing ETH withdrawals during times of high gas prices, there is always some risk associated with trusting the custody of valuable crypto assets with third-party exchanges.

With every bull run, the value deposited in custodial exchanges skyrockets, and they naturally become high priority candidates for any malicious actors. Unlike traditional assets where a regulator may return funds to an aggrieved party, blockchain technology makes it so that stolen funds are rarely recovered. The only safe way to store funds is with oneself and following the ethos of blockchain, “not your key, not your cryptocurrency”. It only takes one hack or loss of funds to put users off custodial solutions, but perhaps it does take one hack.

However, in 2021, centralised exchanges are no longer completely operating in the wild west and, in the future, will likely come under greater regulatory oversight with a lower risk of loss of funds through insurance. Coinbase will soon be a listed US company and will have public records and regular audits to ensure everything is in order. Kucoin was able to recover the lost funds through insurance, and the users were eventually unaffected.

Disproportionate Influence of Centralised Exchanges

Another core tenet for crypto assets is decentralisation and democratisation of power, and without it, BTC is no different from Libra or USDT. Having funds on custodial exchanges gives them ecosystem-defining power as tokens also get governance votes and allow holders to define the protocol’s direction. In May 2020, Binance was caught in the fork dilemma of STEEM token and flip-flopped on which party to support, having the deciding number of votes. While it finally sided with the majority of the users, the fact that a centralised exchange has such power is already concerning. This is even more concerning for the future of competing protocols, as Binance is one of the largest holders of the DEXes tokens. Relying on the continued benevolence of a centralised exchange is against the ethos of the crypto world.

Democratising Fund Raising and Listing of Assets

With thousands of crypto assets to be excited about and choose from, the utility provided by a trustless exchange has never been more apparent. Whether it is the latest yield aggregator, NFT, oracle, or interoperability project, the first thing the investor wants to know is "when token?" wanting to be the first to invest in it. DEXes provide a solution without expensive listing requirements of centralised exchanges. Not only providing liquidity to a wide variety of coins, but DEXes also allow for new projects to raise funding through an Initial DEX Offering (IDO) where the project team opens a new pair for their token against ETH or a stable coin on a DEX becoming the first LP. The open and vast pool of investors can then come in and collectively help in true price discovery. While we are all in it for the tech, the ability to make quick gains on the newest project does sustain that interest. Ten to hundreds of new currency pairs are opened on Uniswap every day.

With complete freedom and no checks on the team and product authenticity, many fly-by-night projects may be listed on DEXes to dupe investors. There was also a plague of projects being listed with names similar to highly anticipated projects. Uniswap has mitigated this by introducing verified lists of projects and various warnings to inform users if they are about to invest in an unverified product.

Censorship Resistance

Decentralised exchanges live as code on the smart contract. Anyone with access to a wallet can connect to the contract and transact with it without requiring any identification or background checks. There has been no regulation stopping individuals in any jurisdiction from trading on a DEX, and it is unlikely that even if one comes, it will be enforceable and will fully accomplish its goal. For example, the Uniswap smart contract is deployed already and lives on the Ethereum blockchain and is not in control of any single entity. Even if the front-end is taken down, it is possible to interact directly with the blockchain contract.

Programmability

What makes the opportunity in decentralised finance (DeFi) exciting is that it is like a lego box with each protocol providing another opportunity to build on top of it. DeFi is a stack of interrelated contracts with each providing service to another. Liquidity tokens on decentralised exchanges can be used for yield farming (like yearn finance vaults for various curve pools) or staked for "reflexive yield farming", i.e. raising funds by rewarding users who provide liquidity.

Centralised exchanges are also providing saving and staking products to compete with the yields provided by DeFi. However, the products are limited, and the yields are not as high.

3.
Final word

The case for DEXes is the same as the case for bitcoin, being in charge of your funds. There will always be a need to move between assets and increase and decrease risk based on market conditions. Centralised exchanges currently provide this service. But decentralised exchanges will continue to grow as limitations like transaction cost, slippage, order books, margin trading, options and leveraged positions are addressed. There are already upcoming projects or improvements in current projects addressing one or more of these limitations. It is only a matter of time that decentralised exchanges start controlling a higher share of volumes. Even centralised exchanges understand this and are already looking to diversify by offering decentralised solutions like Serum by FTX or Binance Smart Chain by Binance. However, the incumbents with an already established user base will likely capture most of the volumes as we ad-vance. Please refer to the Digital Investor to learn more about the specific DEX projects, what differentiates them and how they accrue value.

Disclaimer

This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head once and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is published solely for information purposes; it is not an advertisement nor is it a solicitation or an offer to buy or sell any financial investment or to participate in any particular investment. strategy. This document is for distribution only under such circumstances as may be permitted by applicable law. It is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction.

No representation or warranty, either express or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document, except with respect to information concerning SEBA. The information is not intended to be a complete statement or summary of the financial investments, markets or developments referred to in the document. SEBA does not undertake to update or keep current the information. Any statements contained in this document attributed to a third party represent SEBA's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.

Any prices stated in this document are for information purposes only and do not represent valuations for individual investments. There is no representation that any transaction can or could have been elected at those prices, and any prices do not necessarily reflect SEBA's internal books and records or theoretical model-based valuations and may be based on certain assumptions. Different assumptions by SEBA or any other source may yield substantially different results.

Nothing in this document constitutes a representation that any investment strategy or investment is suitable or appropriate to an investor's individual circumstances or otherwise constitutes a personal recommendation. Investments involve risks, and investors should exercise prudence and their own judgment in making their investment decisions. Financial investments described in the document may not be eligible for sale in all jurisdictions or to certain categories of investors. Certain services and products are subject to legal restrictions and cannot be offered on an unrestricted basis to certain investors. Recipients are therefore asked to consult the restrictions relating to investments, products or services for further information. Furthermore, recipients may consult their legal/tax advisors should they require any clarifcations. SEBA and any of its directors or employees may be entitled at any time to hold long or short positions in investments, carry out transactions involving relevant investments in the capacity of principal or agent, or provide any other services or have offcers, who serve as directors, either to/for the issuer, the investment itself or to/for any company commercially or financially affliated to such investment.

At any time, investment decisions (including whether to buy, sell or hold investments) made by SEBA and its employees may differ from or be contrary to the opinions expressed in SEBA research publications.

Some investments may not be readily realizable since the market is illiquid and therefore valuing the investment and identifying the risk to which you are exposed may be diffcult to quantify. Investing in digital assets including cryptocurrencies as well as in futures and options is not suitable for every investor as there is a substantial risk of loss, and losses in excess of an initial investment may under certain circumstances occur. The value of any investment or income may go down as well as up, and investors may not get back the full amount invested. Past performance of an investment is no guarantee for its future performance. Additional information will be made available upon request. Some investments may be subject to sudden and large falls in value and on realization you may receive back less than you invested or may be required to pay more. Changes in foreign exchange rates may have an adverse effect on the price, value or income of an investment. Tax treatment depends on the individual circumstances and may be subject to change in the future.

SEBA does not provide legal or tax advice and makes no representations as to the tax treatment of assets or the investment returns thereon both in general or with reference to specifc investor's circumstances and needs. We are of necessity unable to take into account the particular investment objectives, financial situation and needs of individual investors and we would recommend that you take financial and/or tax advice as to the implications (including tax) prior to investing. Neither SEBA nor any of its directors, employees or agents accepts any liability for any loss (including investment loss) or damage arising out of the use of all or any of the Information provided in the document.

This document may not be reproduced or copies circulated without prior authority of SEBA. Unless otherwise agreed in writing SEBA expressly prohibits the distribution and transfer of this document to third parties for any reason. SEBA accepts no liability whatsoever for any claims or lawsuits from any third parties arising from the use or distribution of this document.

Research will initiate, update and cease coverage solely at the discretion of SEBA. The information contained in this document is based on numerous assumptions. Different assumptions could result in materially different results. SEBA may use research input provided by analysts employed by its affliate B&B Analytics Private Limited, Mumbai. The analyst(s) responsible for the preparation of this document may interact with trading desk personnel, sales personnel and other parties for the purpose of gathering, applying and interpreting market information The compensation of the analyst who prepared this document is determined exclusively by SEBA.

Austria: SEBA is not licensed to conduct banking andfinancial activities in Austria nor is SEBA supervised by the Austrian Financial Market Authority (Finanzmarktaufsicht), to which this document has not been submitted for approval. France: SEBA is not licensed to conduct banking and financial activities in France nor is SEBA supervised by French banking and financial authorities. Italy: SEBA is not licensed to conduct banking and financial activities in Italy nor is SEBA supervised by the Bank of Italy (Banca d'Italia) and the Italian Financial Markets Supervisory Authority (CONSOB - Commissione Nazionale per le Società e la Borsa), to which this document has not been submitted for approval. Germany: SEBA is not licensed to conduct banking and financial activities in Germany nor is SEBA supervised by the German Federal Financial Services Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht), to which this document has not been submitted for approval. Hong-Kong: SEBA is not licensed to conduct banking and financial activities in Hong-Kong nor is SEBA supervised by banking and financial authorities in Hong-Kong, to which this document has not been submitted for approval. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Hong-Kong where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not "professional investors" within the meaning of the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong) and any rules made thereunder (the "SFO"). Netherlands: This publication has been produced by SEBA, which is not authorised to provide regulated services in the Netherlands. Portugal: SEBA is not licensed to conduct banking and financial activities in Portugal nor is SEBA supervised by the Portuguese regulators Bank of Portugal "Banco de Portugal" and Portuguese Securities Exchange Commission "Comissao do Mercado de Valores Mobiliarios". Singapore: SEBA is not licensed to conduct banking and financial activities in Singapore nor is SEBA supervised by banking and financial authorities in Singapore, to which this document has not been submitted for approval. This document was provided to you as a result of a request received by SEBA from you and/or persons entitled to make the request on your behalf. Should you have received the document erroneously, SEBA asks that you kindly destroy/delete it and inform SEBA immediately. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Singapore where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not accredited investors, expert investors or institutional investors as declned in section 4A of the Securities and Futures Act (Cap. 289 of Singapore) ("SFA"). UK: This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head offce and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is for your information only and is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product.

SEBA is not an authorised person for purposes of the Financial Services and Markets Act (FSMA), and accordingly, any information if deemed a financial promotion is provided only to persons in the UK reasonably believed to be of a kind to whom promotions may be communicated by an unauthorised person pursuant to an exemption under the FSMA (Financial Promotion) Order 2005 (the "FPO"). Such persons include: (a) persons having professional experience in matters relating to investments ("Investment Professionals") and (b) high net worth bodies corporate, partnerships, unincorporated associations, trusts, etc. falling within Article 49 of the FPO ("High Net Worth Businesses"). High Net Worth Businesses include: (i) a corporation which has called-up share capital or net assets of at least GBP 5 million or is a member of a group in which includes a company with called-up share capital or net assets of at least GBP 5 million (but where the corporation has more than 20 shareholders or it is a subsidiary of a company with more than 20 shareholders, the GBP 5 million share capital / net assets requirement is reduced to GBP 500,000); (ii) a partnership or unincorporated association with net assets of at least GBP 5 million and (iii) a trustee of a trust which has had gross assets (i.e. total assets held before deduction of any liabilities) of at least GBP 10 million at any time within the year preceding the promotion. Any financial promotion information is available only to such persons, and persons of any other description in the UK may not rely on the information in it. Most of the protections provided by the UK regulatory system, and compensation under the UK Financial Services Compensation Scheme, will not be available.

© SEBA Bank AG, Kolinplatz 15, 6300 Zug. 2021. All rights reserved.

SEBA BANK

SEBA Bank AG
Kolinplatz 15 • 6300 Zug • Switzerland • www.seba.swiss • info@seba.swiss