SEBA BANK

November 2021

Scalability

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

Contact

research@seba.swiss

Executive summary

Blockchains hold the promise for money for the internet, world computer, the future of finance, the metaverse and more. However, because of their decentralised architecture, they are struggling to support even a fraction of the user base of the older centralised systems. Scaling solutions can help blockchains achieve their lofty goals. In this edition of the Bridge, we cover the need for scalability, the various scaling solutions available and the trade-offs they make.

The blockchain trilemma states that a perfectly decentralised, secured, and scalable system cannot exist, and trade-offs must be made between these three desirable traits. Scalability, the capacity to process a large number of transactions, is perhaps the greatest challenge for broader blockchain adoption.

In this edition of The Bridge, we present various scalability solutions and their attempt to solve the trilemma.

1. Introduction

In the interplay between the blockchain trilemma, chains can usually achieve two of the three. For a given security level, scalability is inversely proportional to decentralisation. Hence, a blockchain must make trade-offs. We invite readers not familiar with the blockchain trilemma to read our earlier publication on the topic, "The Bridge – The Blockchain Trilemma".

Scalability refers to a blockchain system's ability to support growth in terms of users and transactions without compromising performance. In most current blockchains, as the number of transactions increases, the network gets clogged with pending transactions forcing users to pay higher than usual fees to get their transactions included. Scalability is important as it allows for cheap fees and unlocking of new use-cases, finally helping onboard new users.

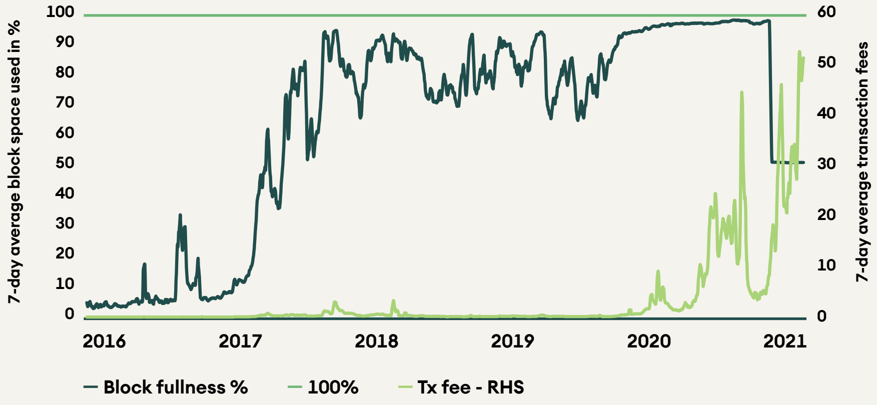
Table 1: Cheap fees allow for the unlocking of new use-cases

Cost per transaction	Use-case
USD 1,000	Large-scale institutional use only
USD 10	Some financial use for middle-to-wealthy individuals
USD 0.1 to USD 1	Financial use for more people and non-financial apps like identity become viable. On-chain privacy becomes viable
USD 0.01 – USD 0.1	Micropayments and more non-financial apps like data management become viable
<USD 0.01	"Why not put everything on the blockchain?"

Source: SEBA Bank, Vitalik Buterin

These issues are most prominent on older generation blockchains like Ethereum and Bitcoin. Figures 1 and 2 show the mean price of transaction fees of Bitcoin and Ethereum in USD and their capacity utilisation. Note that Ethereum's capacity utilisation has dropped to about 50% recently – the target level – as illustrated in figure 1 because of the implementation of EIP-1559. Post EIP-1559, whenever block space utilisation is above 50%, fees increase and vice versa.

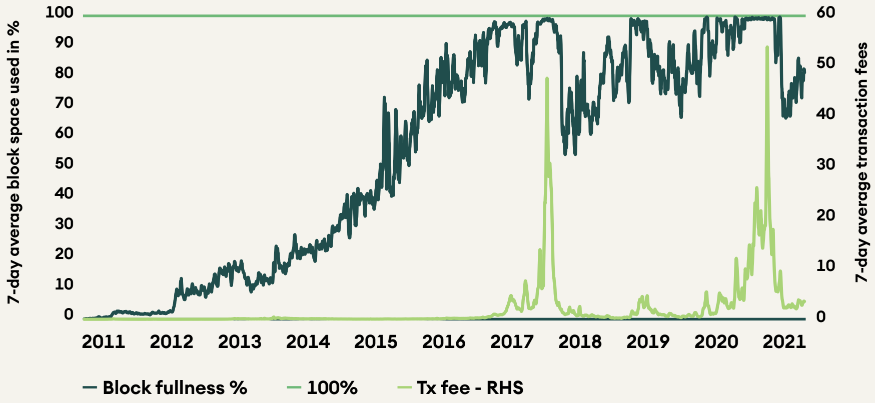
Figure 1: Ethereum mean transaction fee (in USD) and block utilisation



Source: SEBA Bank, Coin Metrics

Regarding Bitcoin, the link between capacity constraint – lack of scalability – and the fee is direct. When the system is in high demand, congestion occurs and fees spike.

Figure 2: Bitcoin mean transaction fee (in USD) and block utilisation



Source: SEBA Bank, Coin Metrics

When the system is in high demand, congestion occurs and fees spike.aCompared to traditional financial solutions, the ratio of transaction speed to cost is unfavourable on older blockchain networks. Visa's payment processors execute around 1,700 transactions per second (TPS) and can scale up to 65,000 TPS. For comparison, a blockchain like Ethereum can process only 15 TPS. Because of this limitation, contenders such as Binance Smart Chain, Solana, Polkadot have emerged to provide higher TPS, often at the cost of higher centralisation. Table 1 shows the TPS comparison of various blockchains platforms versus VISA and PayPal.

Table 2: TPS of Blockchain platforms vs VISA and PayPal

Network	TPS (Transactions Per Second)
Bitcoin	7
Ethereum	15
PayPal	193
Cardano	300
Polkadot	1,000
Stellar	1,000
Avalanche	4,500
Solana	50,000
VISA	65,000

Source: SEBA Bank

While talking about the problem of scalability, Elon Musk tweeted about Dogecoin, quoting, “Ideally, Doge speeds up block time 10X, increases block size 10X & drops fees 100X. Then it wins hands down.” As enticing as it sounds, there is a price for it.

Can we do what Elon proposes?

One of the core tenets of blockchain is to minimise trust, as the saying often goes – “Don’t trust, verify”. A blockchain should strive to provide minimum hindrance if a user wishes to run a node and “verify” the blockchain themselves. This helps maximise decentralisation and allows the blockchain to remain censorship-resistant, providing security against attacks. Bitcoin overcame the ban on Chinese miners because it was decentralised enough to keep the network running even as the most significant contributor fell off.

To maximise decentralisation and trustlessness, a blockchain should be light enough to run on average consumer-grade hardware. The requirements for Bitcoin and Ethereum nodes are barely low enough to allow for consumer laptops to run them. For a higher throughput chain like Solana, the requirements are higher and only dedicated institutional validators can verify transactions. If we implement Elon’s proposal, it will 10x the requirement from nodes, killing decentralisation and making the chain prone to censorship. Hence, there is a need to explore alternate solutions for scalability. To illustrate this path, we will take Ethereum as an example and understand how these solutions pan out and the trade-offs while selecting these alternatives.

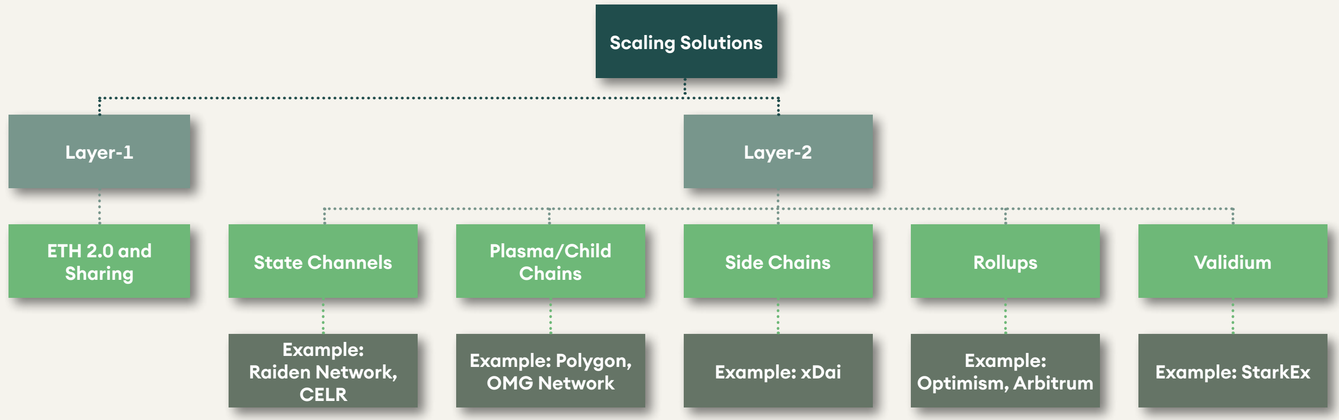
2.
Are there any solutions?

Fortunately, several different scaling solutions are emerging. Some are already live, in different stages of rollouts, while others are still under development. Each of these solutions provides unique trade-offs and can be fundamentally categorised as follows:

1. Layer-1 or on-chain solutions: These solutions keep all the transactions on the main chain itself.
2. Layer-2 or off-chain solutions: These solutions adopt an off-chain mechanism where transactions and computations occur outside the main chain.

To better understand the difference between layer-1 and layer-2 solutions, imagine a road known for traffic jams. The layer-1 solution is to upgrade the road, reduce intersections, widen lanes to “process” more cars. The layer-2 solution is to create a second road or a public transport infrastructure like a bus or metro service to reduce congestion.

Figure 3: A selection of promising scaling solutions



Source: SEBA Bank AG

3.
Layer-1 solutions

To illustrate the layer-1 scalability solutions, we present the case of Ethereum, which has started its upgrade to ETH 2.0. For readers interested in this matter, we recommend reading the two Digital Investors we wrote on this topic – "Ethereum 2.0" and "Phase 0".

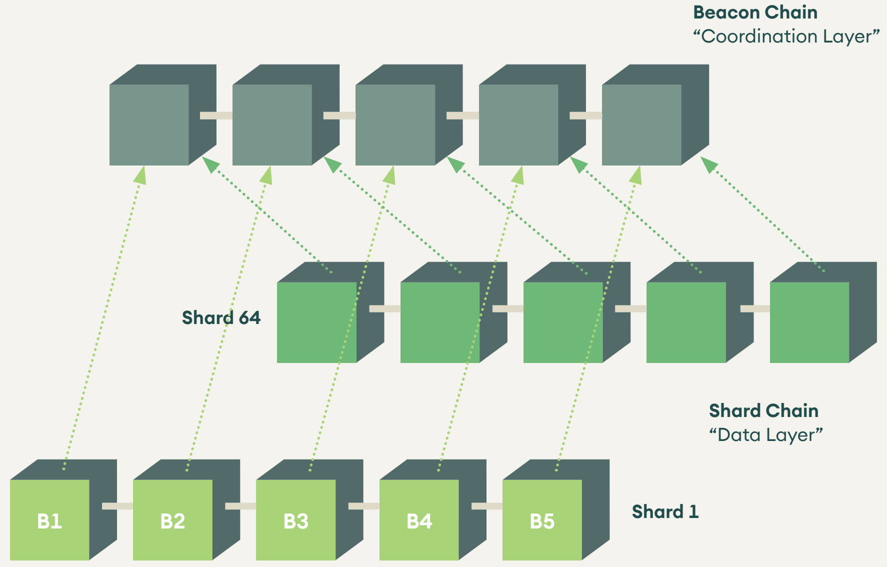
The primary reason to move to ETH 2.0 is to increase the throughput of Ethereum to help it process more transactions and compete with newer layer-1 solutions. TPS should increase from ~15 today to ~100,000 once fully implemented along with rollups. This will be a significant improvement allowing more use-cases and lower transaction costs.

To achieve such speed, the Ethereum architecture will be "sharded". Sharding means splitting the main chain into multiple parallel chains to process transactions. This is similar to upgrading a single-lane road into a highway with many lanes, in the case of Ethereum, 64.

Through sharding, computing power and storage capacity can be distributed across multiple systems, lowering the requirement from node operators. Each shard will have its very own independent state and transactional history. So, there will be no need to run a full Ethereum node contrary to the current version.

Among all the chains running in parallel, the Beacon Chain will function as a coordination layer to coordinate all system activities, storing and managing validators registry, choosing block producers, and applying the rules of consensus.

Figure 4: ETH 2.0 Sharding Structure



Source: SEBA Bank AG, Vitalik Buterin's website

4.
Layer-2 solutions

There are five types of approaches through which layer-2 solutions are deployed (see figure 3). We present all of them in this section.

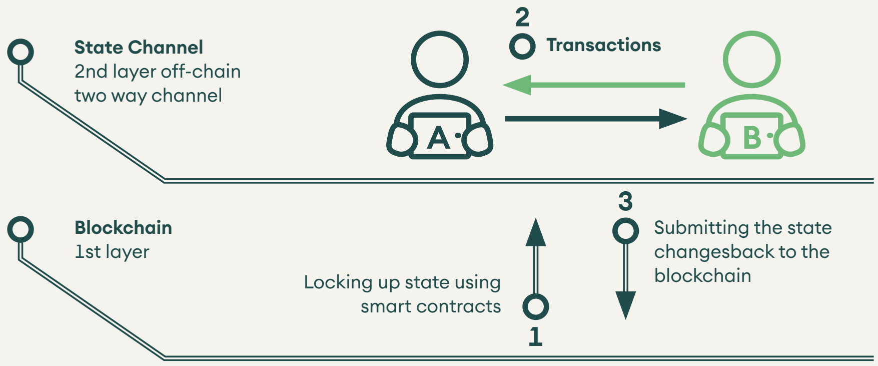
State channel

State channel solutions allow users to transact multiple times on a different chain (layer 2). In contrast, the main chain (layer 1) processes only two transactions, one when the channel is opened and one when the channel is closed. By doing this, the main chain does not process all the transactions but still provides the same level of security in transaction finality. Once the transactions are complete and the channel is no longer required, the participants submit their copies of transaction history to cross-verify their copies of data to ensure there are no discrepancies. Post this, the final net transaction is uploaded on-chain, and the channel is closed.

State channels are advantageous when there are multiple small transactions and the parties know each other. The limitations of State channels are that funds are blocked as long as the channels are active. It is also time-consuming to open and monitor different channels. Further, only limited smart contract functionality is available.

Projects working on State channel include Celer and Raiden Network. Figure 5 shows how a state channel works.

Figure 5: State channel and the steps involved in doing a transaction



Source: SEBA Bank AG, Vitalik Buterin's website

Plasma (Child chains)

Plasma consists of multiple copies of the main chain running alongside it. Thousands of transactions are processed in these child chains, bundled up and sent back to the main chain as a single transaction. By definition, a child chain is a trustless and non-custodial chain where users control their funds. Hence if there are any errors or exploits, they can refer to the latest correct snapshots of the plasma chain and restore their tokens.

The advantage of plasma layers is their high throughput to process over 1,000 transactions per second at a fraction of the cost. Here, one necessarily does not need to have a fixed number of known entities or individuals to transact with, and they can be flexible. Like state channels, plasma solutions do not fully support smart contracts and are suitable only for transactions and swaps.

Projects that use plasma layers include Polygon and OMG Network.

Sidechains

Sidechains and child chains (plasma) are similar except for one element: security. While plasma chains rely on the security of their main chain in a trustless environment and are optimised for high throughput performance and security, side chains are separate blockchains running in parallel with the main chain and have their own consensus mechanisms and security algorithms.

The advantage of sidechains is that they are usually blockchain agnostic and can support multiple base layers by creating a peg with any blockchain they want to run along. These side chains may have their own tokens, can support smart contracts, and only communicate with the mainchain when they want to update the state of their ledger. These side chains can achieve up to 10,000 TPS depending upon their design. However, this also does not come without its disadvantages. Users have to transfer the custody of funds to the side chain, and the security mechanism of the sidechain may be weaker than the main chain.

xDai and Polygon are sidechains for Ethereum.

Rollups

Rollups bundle thousands of transactions into a single rollup block, publishing only summary data on the main chain. It can potentially provide a 100X increase in throughput as all the computation and storage happens outside the main chain.

By batching transactions and moving processing off-chain, rollups significantly reduce transaction fees and processing time. There are two types of rollups:

Optimistic Rollups

Optimistic rollups use a sidechain to process a batch of transactions parallel to the Ethereum mainchain, summarise it and notarise the transactions on top of the mainnet. They work with a basic assumption that all transactions submitted to the mainchain are valid. Only when a user challenges a summary, the entire block is computed on the base layer. As a result, to give sufficient time for a challenge, funds are locked for some time, typically one week, before releasing them on the base layer.

Optimistic rollups can process around 2,000 basic transfers per second or around 300 smart contract calls in their current implementation. These are also compatible with the Ethereum Virtual Machine (EVM). This means that optimism rollups can do everything that Ethereum does. However, there are two trade-offs. First, the funds are at risk if a malicious transaction is not challenged and second, withdrawing funds to the mainchain is also time-consuming.

Examples of rollups are Optimism and Arbitrum. These projects are already live, and popular projects like Uniswap, 1inch, and Chainlink, among others, are already using them to save transaction costs for users.

Zero-Knowledge (ZK) Rollups

ZK Rollups run all computations off-chain and submit a validity proof on Ethereum. They differ from optimistic rollups because there is no trust assumption as the validity proof is printed on-chain. While optimistic rollups require evidence of fraud during the challenge, zk rollups have validity proofs for every transaction.

They are reported to be able to process over 3,000 transactions per second on Ethereum 1. As there is no trust assumption, there is no delay in moving funds from Layer 1 to Layer 2 and vice versa. Currently, there is no generalised EVM-compatible zk rollup based solution, and only specific solutions for transfer or exchanges are available.

Loopring is a decentralised exchange working on zk rollups with transaction costs of less than a cent.

Validium

Validium uses validity proofs similar to zk rollups but keeps the data off-chain instead of sending it to the Ethereum main chain. Since all the data is kept off-chain, Validium can achieve an even higher TPS per validium chain of up to 20,000.

However, since the data is not on-chain, validium requires some trust assumptions, and a majority of validators can choose to freeze funds by not providing data.

StarkWare's StarkEx is a validium-based solution. StarkEx is integrated with the derivatives exchange, dYdX, and the NFT platform, ImmutableX.

Table 3: Comparison between different layer-2 solutions and the trade-offs they make

	State Channels	Plasma	Sidechains	Optimistic Rollups	ZK Rollups	Validium
Full smart contract support	✗	✗	✓	✓	✗	✓
Trustless	✓	✓	✗	✓	✓	✗
Instant withdrawal	✓	✗	✓	✗	✓	✓

Source: SEBA Bank, Matter Labs

5. Conclusion

For blockchains and crypto assets to achieve their lofty promises of world computers and money for the internet, they must be able to scale sustainably. For this, a combination of both layer-1 and layer-2 solutions will be required. Currently, chains are sacrificing decentralisation to achieve scalability, or a hotchpotch of solutions are being implemented with limited integrations between them, worsening the user experience and fragmenting the user base. Solving scalability will not be a winner-take-all scenario, and different use-cases will require different scaling and security needs. Improvements in scalability from layer-1 and layer-2 solutions will multiply in the future, leading to sustainable, scalable blockchains.

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 clarifications. 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 officers, 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 difficult 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 specific 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 office 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

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