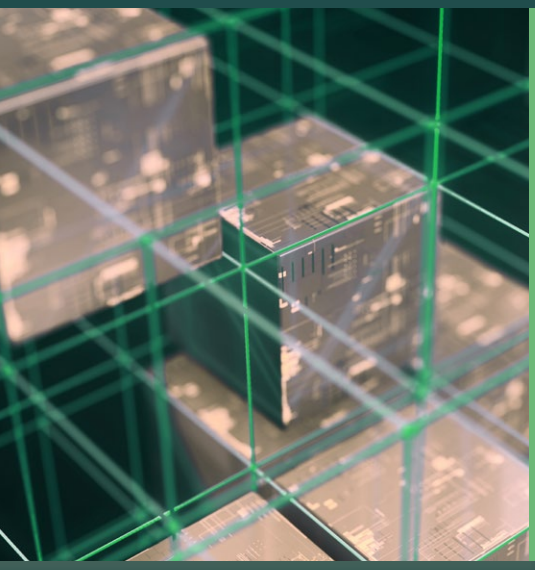
SEBA



November 2020

Blockchain Interoperability

Towards a connected future

The Digital Investor

Redefining Finance for the New Economy

Table of Contents

Authors

Yves Longchamp
Head of Research
SEBA Bank AG

Saurabh Deshpande
Research Analyst
B&B Analytics Private Limited

Contact

research@seba.swiss

Abstract

Interoperability is the ability of software to exchange information between different ecosystems. In the case of blockchains, it has the potential to break the silos and to create a network of blockchains. It is a catalyst for broader adoption of blockchains and crypto-currencies.

In this article, we provide a broad overview of blockchain interoperability, looking at the opportunities it creates, the challenges it faces, and its value accrual mechanism before describing the different solutions. Finally, we briefly present the Polkadot project, an ambitious and promising interoperability solution.

In this article, we provide a broad overview of blockchain interoperability, looking at the opportunities it creates, the challenges it faces before describing the different solutions. Finally, we briefly present the Polkadot project, an ambitious and promising interoperability solution.

1. Introduction

More and more people are considering blockchains as safe and promising. Thousands of projects relying on different blockchains have emerged in the last few years. They have specialised in payments, smart contracts platforms, data storage solutions, supply chain management, to name a few. These blockchains are either public or private and have made different choices in terms of security, scalability, and decentralisation, each with unique governance and a specific consensus algorithm.

As a result of all these choices and goals, there are no universal standards for blockchain developments. The blockchain ecosystem is heterogeneous, and the potential of this technology remains untapped if they operate in silos. For instance, we cannot trigger a payment (supported by blockchain A) after delivery occurred (according to supply management blockchain B). The reason this cannot happen is that blockchains are not interoperable.

Interoperability is "the ability of computer systems or programs to exchange information" according to the Oxford Dictionary. In the current setting, blockchains work mostly in a silo, limiting the possibilities offered, their use, and finally their adoption. Imagine how "successful" would the internet be if WhatsApp were not interoperable with your smartphone camera, Facebook with YouTube, and Amazon with a credit card payment system?

Soon, we can extend interoperability to a broader set of assets and activities. These activities can be - a blockchain land register enabling you to pledge your ownership rights on a borrowing/lending platform to get a mortgage; or your digital identity secured on a chain allowing you to unlock your bank account and get access to the social security system.

The current blockchain ecosystem looks like a thousand island archipelago with each island as a separate blockchain project. It is a complex landscape tough to navigate. Interoperability allows blockchains to communicate, to exchange data, and value. Interoperability could break silos and act as a catalyst for mass adoption of cryptocurrencies.

In this article, we provide a broad overview of blockchain interoperability, looking at the opportunities it creates, the challenges it faces before describing the different solutions. Finally, we briefly present the Polkadot project, an ambitious and promising interoperability solution.

In the next Digital Investor, we will dive deeper into different interoperability solutions and explore their value accrual mechanisms.

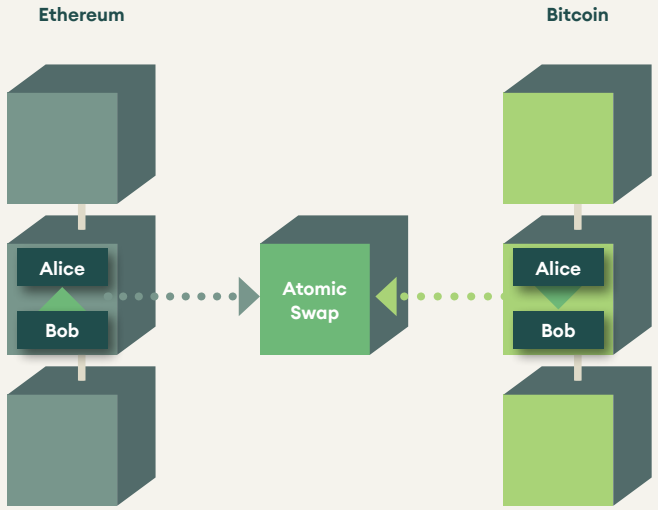
2.
Opportunities

Interoperability would facilitate the communication and exchange of value between blockchains. In this section, we present different functionalities that emerge with interoperability.

Atomic Swap

An atomic swap is an exchange of token ownership on two blockchains. Imagine that Alice and Bob both have bitcoin (BTC) and Ethereum (ETH) wallets and Alice wants to exchange BTC for ETH and Bob wants to exchange ETH for BTC. Interoperability would allow for a peer-to-peer and secure transfer of ownership, as illustrated in figure 1.

Figure 1: Atomic swap



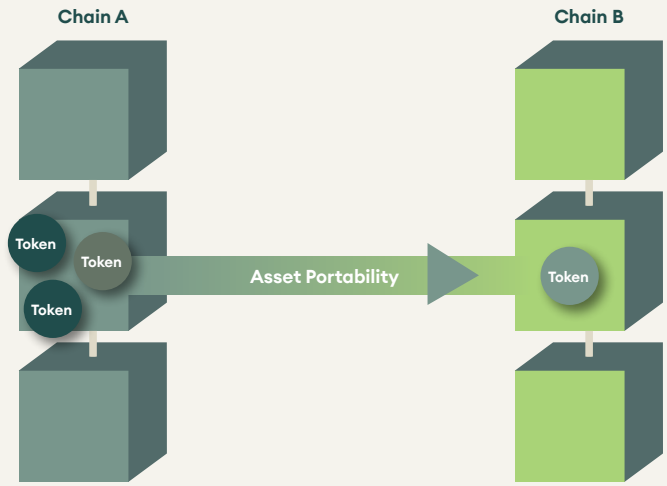
Source: SEBA Bank AG

As the name indicates, it is a swap of assets, and it is atomic. Atomic means that it is either executed fully or not executed at all. It does not allow partial execution, meaning that it is not possible only for Bob to receive the asset from Alice but not the other way round. Atomic swap eliminates the counterparty risk.

Asset portability

Asset portability is the ability to move a token (or a fraction of it) from one blockchain to another whilst maintaining its history in the first blockchain, as illustrated in figure 2.

Figure 2: Asset Portability



Source: SEBA Bank AG

An example of its application would be a healthcare ledger that securely stores our whole health data of patients. A patient may then, fully or partially, send the data to another ledger (health insurance, hospital or the attending physician). It improves the quality of the data as it would be recorded and aggregated on one chain and let the patient retain the ownership of their data.

Cross-chain oracles

Cross-chain oracles allow one blockchain to decide on an event it observes on another blockchain.

1. Say a financial platform A built on Polkadot allows liquidity providers to stake collateral on Ethereum and employs a Chainlink solution to monitor its value. If the value of collateral on Ethereum falls below a threshold, a liquidation will get triggered on platform A.
2. Using a supply management example, one can imagine firm A using its blockchain supply management solution to wait for its supplier to deliver a product. By being continuously informed about its order tracked on the supplier blockchain, firm A can optimally plan its production. The other way round, when the firm A stock of intermediate product provided by the supplier is running low, the system can automatically generate the order. This system can be generalised to several blockchains and firms. Interoperability would then creates one place to interact instead of multiplying bilateral solutions.

Asset encumbrances

Asset encumbrance is the ability to lock up an asset on one blockchain and unlock it if a specific condition on another chain is met. In the earlier example with liquidity providers, interoperability brings atomic transactions which eliminate the counterparty risk.

Collateralised loans are the perfect use case. Imagine you lock assets on a blockchain and get a loan issued on another blockchain; interoperability would eliminate the counterparty risk as both actions will take place atomically.

3.
Challenges

To create communication bridges between blockchains is different from standard Application Programmes Interfaces (API) in vogue nowadays. APIs allow one application to Create, Read, Update, and Delete (CRUD) data in another application. Updating or deleting data on a blockchain is non-trivial as the majority of the network participants must agree with the change. Blockchain design discourages updating history. As it is cumbersome to alter (update) or delete data, blockchains' APIs differ from standard ones as they allow only the CR out of CRUD functions. It implies that when a transaction takes place, it cannot be changed afterwards in case of a mistake. It has two implications. First, there needs to be a guarantee that both legs of a transaction take place simultaneously, or transactions need to be atomic. Second, the transaction inputs must be final.

For instance, if Alice transfers an asset from chain A to Bob on chain B, either Alice's is debited, and Bob credited, or neither action occurs.

Also, a blockchain API requires a waiting period before one can confidently view the response as valid. For instance, bitcoin works on probabilistic finality, not deterministic finality. It means that only after a certain number of blocks (usually 6 for bitcoin), can one say with sufficient certainty that contents of the blockchain are unlikely to be altered, in other words, the information in the blockchain is final. Once a block is final, the data can be bridged to another blockchain in all safety, eliminating the risk of a fork[1].

Besides atomicity and finality, interoperability faces the diversity of blockchains, as we mentioned earlier. As there is no standard, identity and events are recorded differently on each blockchain. An interoperability solution must propose a universal method to read data and to get a sense of it for all types of blockchains.

If an investor thinks that we will live in a world where multiple blockchains co-exist to perform different functions, then there needs something to allow those blockchains to work together. Interoperability solutions fill this gap.

4.
Why should investors care about interoperability?

Blockchains are difficult to design as a well-functioning blockchain requires alignment of incentives of different stakeholders. The complexity of a blockchain's design increases with every added functionality because incentive alignment needs to scale for incremental functionality. And with increased complexity, the attack surface grows as well. Therefore, blockchains are generally good at achieving only specific and limited goals.

If an investor thinks that we will live in a world where multiple blockchains co-exist to perform different functions, then there needs something to allow those blockchains to work together. Interoperability solutions fill this gap.

As of now, money is undoubtedly a use case that public blockchain solves. During this summer, Ethereum showed that blockchains could be good at other aspects such as lending/borrowing, yield automation, and so on. Over 150,000 BTC (worth more than USDbn 2) is on Ethereum blockchain, proving that there is a demand for cross-blockchain asset transfers. Existing solutions allow minting BTC (called as wrapped BTC) on Ethereum with some intermediaries. Interoperability would make these operations easier to perform.

Developers are building interoperability solutions that allow asset transfer between two different blockchains without the need for intermediaries. Seamless portability of assets among blockchains will allow easy access to liquidity and thereby enable liquidity providers to earn yield with less hassle. Thus, interoperability solutions will be able to accrue some value for facilitating the trustless and secure transfer of assets by charging some fee. As the cross-chain transfer volumes increase, interoperability solutions will accrue more value. Therefore, we think that there is merit in evaluating investment opportunities within different interoperability solutions.

[1] This section was largely inspired by the 2019 University of Arkansas Blockchain Center of Excellence White Paper Series "Towards Blockchain 3.0 Interoperability: business and technical considerations" by Mary Lacity, Tach Steelman and Paul Cronan.

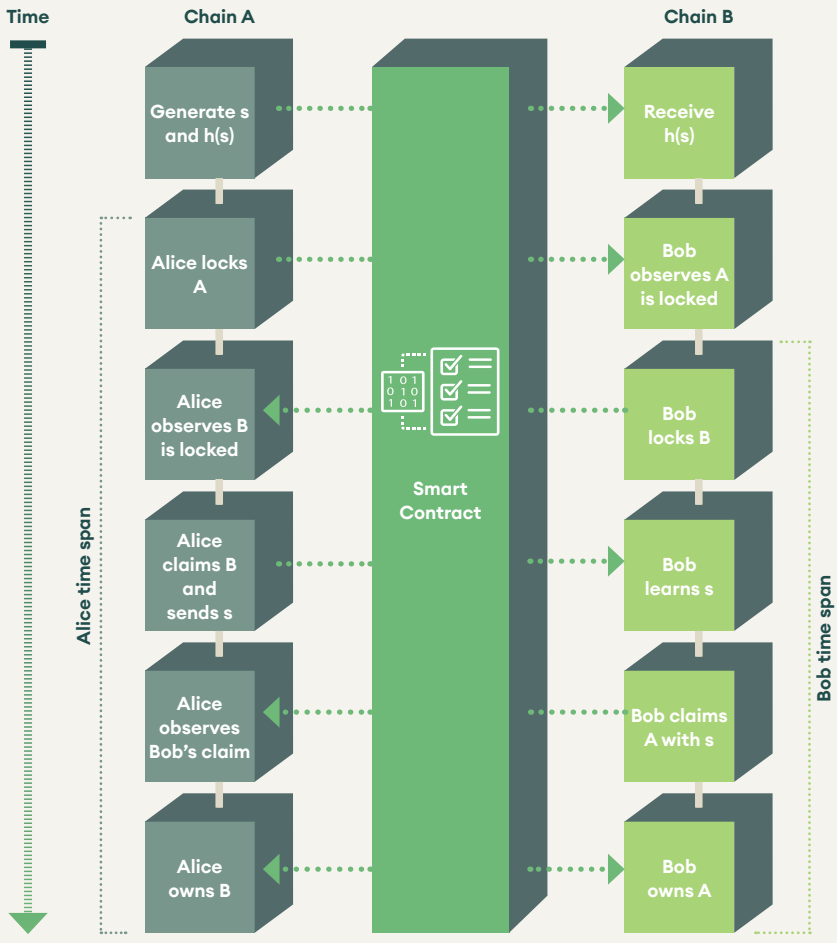
5.
Solutions

From a high-level perspective, there are three ways to design interoperability solutions. The one that interests us the most is the general sidechain/relay solution as it offers the maximum flexibility. We also describe two other solutions, Hash-time locked contracts (HTLC), and notaries.

Hash-time locked contracts

Hash-time locked contracts (HTLC) are smart contracts that link two chains bilaterally, creating only cross-dependency between the two. As the name of this solution suggests, HTLC uses hash and time locks to secure a transaction between two blockchains. Imagine Alice wants to exchange and an asset A on chain A with Bob whose asset B is on chain B. To start the process, Alice generates a secret s and sends the secret's hash h(s) to Bob. In a second step, Alice locks her asset in a smart contract. Bob then observes that asset A is now locked in the smart contract and locks his asset B in the same contract. Alice sends a transaction to claim asset B and the secret s. As Bob knows the secret as well, he is now in a position to unlock asset A and takes possession of it. If the secret is not transmitted correctly (or not received) and no one can claim any asset, after a predefined period, the assets are unlocked and given back to their original owner.

Figure 3: Hash-time locked contracts (HTLC)



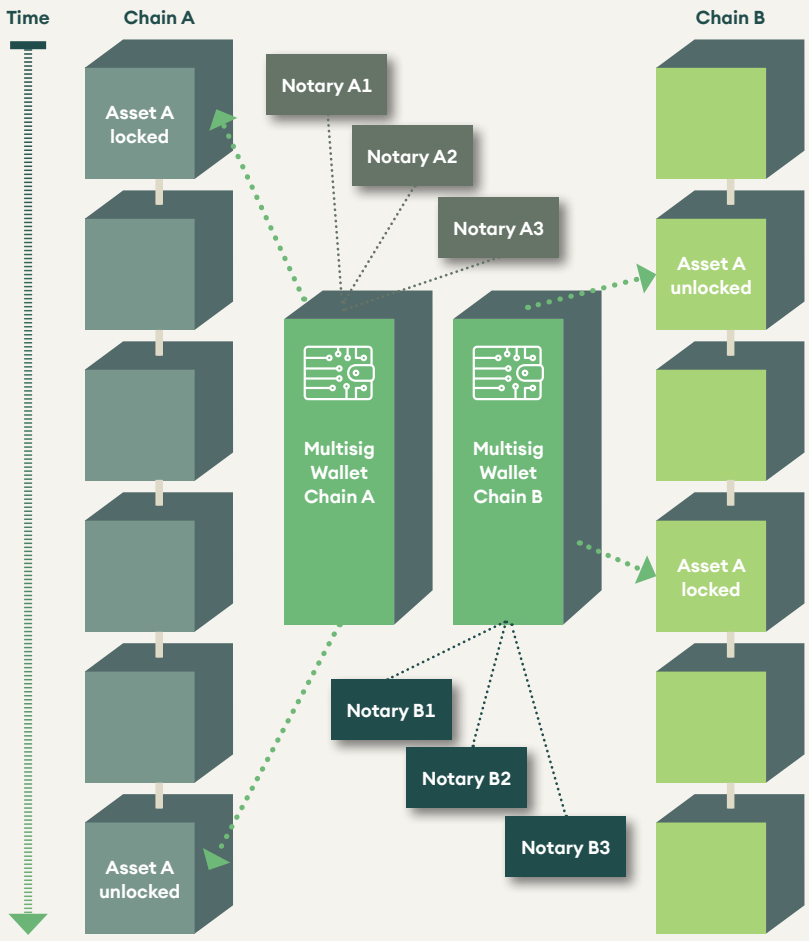
Source: SEBA Bank AG

HTLC is an elegant solution that uses decentralised smart contracts to create a trustless platform for interoperability. One of the significant limitations of the HTLC is that it does not allow for assets to move from one chain to another; it only permits for a change of ownership in different chains, like an atomic swap. Besides, it is a bilateral solution working for Chain A and B in our example. Therefore, it would require n(n+1)/2 smart contracts to connect n blockchains.

Notaries

Another way to design interoperability is to get inspiration from real life notary system. Notaries are trusted third parties that facilitate transactions by checking the validity of a transaction and the existence of assets. Transposed to the digital space, notaries consist of trusted signatories of a multi-signature wallet connecting two chains (notice that single notary solutions are also possible). Imagine Alice wanting to move the native crypto-asset of chain A on chain B. Alice would lock asset of chain A to a multi-sig wallet attached to chain A and owned by a set of reputable notaries running a full node. When done, another multi-sig wallet attached to chain B and owned by a group of reputable notaries would unlock asset A on chain B. If the asset can be repatriated from chain B to chain A as well the system is said to be two-way pegged.

Figure 4: Notaries



Source: SEBA Bank AG

6.
Polkadot

Conclusion

Interoperability is the ability of computer systems to exchange information and value. It is a catalyst for blockchain and cryptocurrency adoption as it has the potential to create a network of blockchains by building bridges between them. Relay/sidechains is a general and promising solution, offering more possibilities than Hash-time lock contracts or notaries. Among the possibilities, atomic swap, asset portability and asset encumbrance are set to be used extensively in our view, shaping the digital ecosystem of tomorrow.

While facilitating secure and trustless value exchange, we expect interoperability solutions to capture value in future. Therefore, we think that interoperability solutions demand investor attention.

Polkadot is a blockchain for blockchains; it connects all the blockchains of today and tomorrow. While Ethereum aims to be the platform to build decentralised applications, Polkadot itself is designed for no purpose other than to connect blockchains. It has no inherent application functionality: it is a scalable heterogeneous multi-chain.

Polkadot built its architecture around three elements: a relay chain, parachains (short for parallel chains) and bridges. The Polkadot blockchain is the relay chain; it is at the centre of the ecosystem and relays the information of the parachains. The parachains or sidechains are the existing blockchains attached to the relay chain. They can be the bitcoin blockchain, the Ethereum blockchain or the ones built on the top of Polkadot. Finally, bridges are the gateways that connect the parachains (not built on Polkadot) to the relay chain. Parachains built on the Polkadot do not need a bridge as they have this functionality embedded.

Polkadot introduced the following four participants to make the relay chain, the parachains, and the bridges work together in a trustless environment: Validators, Nominators, Collators and Fishermen.

- Validators are the participants that create and propose Polkadot blocks. They perform most of the security work. To accomplish this, they need to run a full relay chain node and stake a significant amount of DOT, the Polkadot native currency.
- Collators run full node parachains and submit parachains data to the validators. Collators gather information and propose a block to the validator. For instance, a parachain collator focusing on bitcoin will check bitcoin data and propose it to a validator.
- Nominators contribute to the security of the Polkadot network; they risk capital by investing DOT in validators, signalling their trust. In return, they receive a portion of the validator staking reward.
- Fishermen are “bounty hunters” looking for misbehaviour in the Polkadot network. In case they spot provable malicious behaviour, they receive a significant reward.

Polkadot enables blockchains to upgrade themselves without a fork. These forkless upgrades are enacted through Polkadot’s transparent on-chain governance system and create the possibility to upgrade and to avoid hard fork and a potential breaking of a community.

In the next Digital Investor, we will deep dive into Polkadot and other interoperability solutions and explore their value accrual mechanisms.

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.

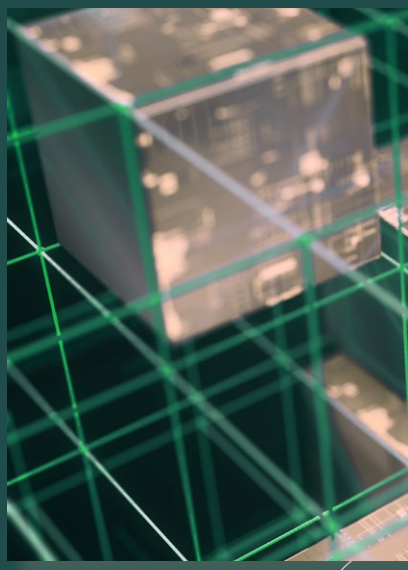
This document may not be reproduced or copies circulated without prior authority of SEBA. Unless otherwise agreed in writing SEBA expressly prohibits the distribution and transfer of this document to third parties for any reason. SEBA accepts no liability whatsoever for any claims or lawsuits from any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



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