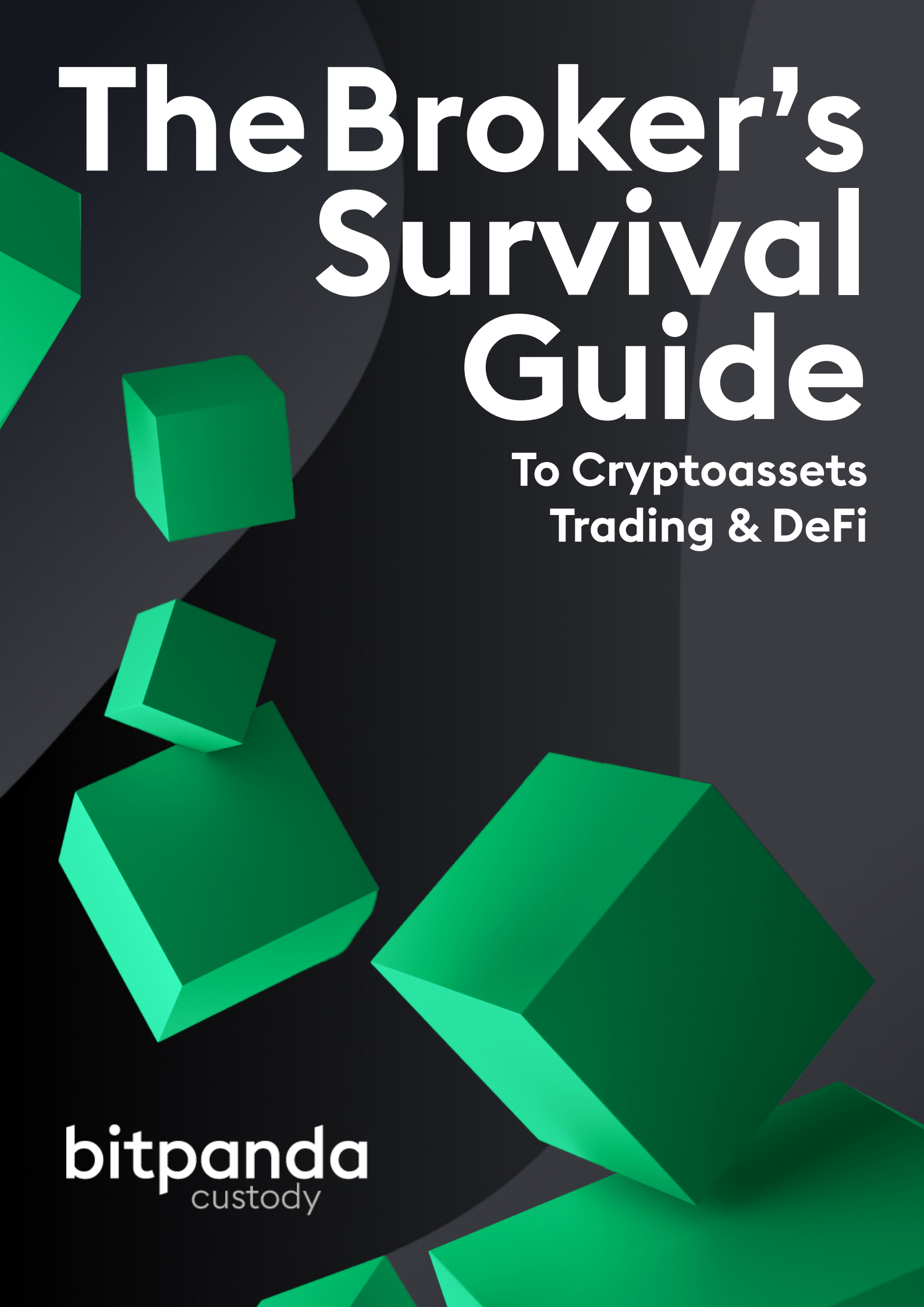
The Broker's Survival Guide

To Cryptoassets Trading & DeFi



bitpanda custody

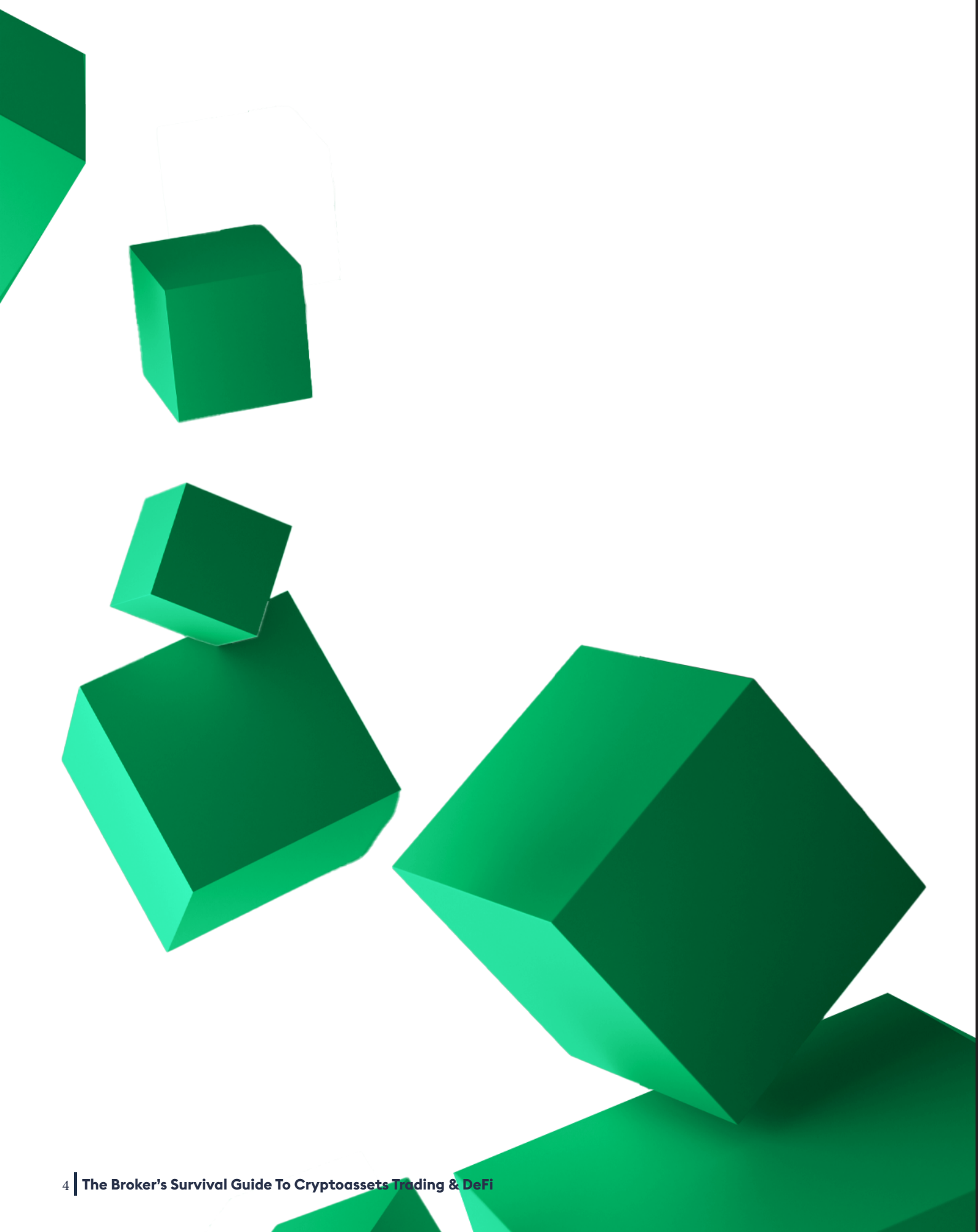
bitpandacustody

Registered cryptoassets firm with the UK Financial Conduct Authority (FRN No.928556)

custody.bitpanda.com

“Nothing changes: everything is different! The principles of brokerage largely remain the same, but brokers have to relearn operations when working with crypto.”

Alex Batlin | Founder and MD, Bitpanda Custody



Contents

Introduction

A huge amount of excitement was generated over 2021 for the crypto markets. Bitcoin made new all time highs and many new retail traders entered the market for their first time.

With all of that many brokers have been identifying the business case and exploring if they should offer crypto.

Are you an FX broker looking to expand a product offering? Or are you contemplating starting a crypto brokerage? Better still, are you a newly formed brokerage trying to navigate the waters? How many of you are already trading crypto? What are your liquidity sources? How do you handle crypto custody? How do you face your counterparties and settle trades without risk? Whatever the case may be this series is intended for you.

Once the initial business case is made, where and how to buy cryptoassets is the first stumbling block. As regulated entities, brokerages need to be able to deliver their crypto offering 24/7 to both retail and institutional clients in a proven and compliant manner, without the huge upfront investment in legal, regulatory or technology.

For all parties, liquidity is critical, and then to manage the delivery if required. Institutional liquidity requires committed market makers and stable infrastructures to ensure best and transparent execution. When volatility increases, slippage can become a real problem, and for larger volumes even more so as market makers withdraw. Current crypto exchange infrastructures seem to also to have problems during high demand.

Execution against a regulated liquidity provider as a riskless principal does not allow for certain conflicts of interest, such as front running, aggressive margining on perpetuals (CFDs) or leverage and internalising trades that could occur with an exchange. Popular venues also trade with a perpetual swap, in which the intraday margin is mostly tailored to the books of the exchanges.

The current liquidity and infrastructure for crypto are highly fragmented compared to FX, some in the space are charging 1-3% to transact in this market, much similar to FX in the 1980s- 2000s, as it grew up, fees and commissions decreased to a few basis points. There is a perceived opportunity from FX buccaneers and innovators to bring this asset class to port with them and seems to be the type of broker most likely to offer this as an add-on in the traditional space, first via CFD in 2017 onwards.

Crypto exchanges have suffered from growing outside traditional finance, and although this has produced innovation, it has left traditional counterparties to either build bespoke solutions or hire additional compliance and consultants to get it right. If integration is perceived as too cumbersome, branching out to this new asset class seems impossible, especially in a large institution where there are many stakeholders to convince. A set-up that is “out-of-the-box” via traditional connectivity or a plug-and-play solution allows the business case to be made, both for cost-effectiveness and risk management.

Venues that are tailored to institutional flow from traditional markets provide a conduit to “old world” players to access liquidity via standard trading protocols such as FIX or are already compliant in a number of areas and are insured, which provides some protection against regulatory changes in the future.

Trading Bitcoin or Ethereum and a number of other top tokens need not be cumbersome and simple solutions inline with industry standards in traditional financial markets are emerging. A solution initially may involve a brokerage also supplying custody, but to avoid counterparty risk, it is worth considering exchange custody and client-side custody, moving the asset to and from the trading party as part of a standard EoD process.

“Large numbers of clients wish to engage counterparties that have a lot of similarity to traditional financial institutions. Being insured or regulated and having a previous track record, are a must for those from the “old” world to start engaging in Crypto and Digital Assets. There is a lot to explain, and it starts easiest with familiarity”

Lars Holst | GCEX

Counterparty credit and settlement risk, one of the biggest impediments for institutions entering the crypto market at scale, is rooted in the lack of credit intermediation services guaranteed by big bank balance sheets - the core function of traditional Prime Brokerage.

This is being overcome with the emergence of technology that delivers real-time atomic exchange of assets, trade and payments netting and clearing and settlement automation. With atomic exchange the trade is also the settlement and ownership changes in real-time on custodial blockchain ledgers eliminating trading counterparty credit and settlement risk.

The same technology can support a lending marketplace that facilitates frictionless crowdsourcing of virtually unlimited balance sheet for intra-day financing of trades.

By employing collateral resting in custodial accounts without having to move it and implementing borrows as real-time repo transactions on custodial blockchain ledgers, the entire spectrum of trading from fully funded, to margin, to fully on credit can be supported with no trading counterparty credit or settlement risk by shifting risks to a diverse range of lenders.

The idea of the "new normal", under the pandemic, has propelled digital transformation to the front of all CEOs minds. If disruptive and innovative technology has taught us anything, it's to always 'think ahead' as the future is unpredictable but full of promise if you know where to look.

In crypto markets, decentralised finance or DeFi and its applications look to be defining the future of finance. It is an ecosystem built around democratising finance and reducing the dependence on middlemen and third parties that plagues current centralised infrastructures causing unnecessary and nontransparent market friction.

For brokerages and funds, it represents an opportunity to tap innovation for yield opportunities and decrease settlement costs. For the more adventurous searching for "Alpha", DeFi could add revenue from flash loans, flash swaps, automated market making, decentralised exchanges, decentralised governance, and initial DeFi offerings.

"Excellence in overcoming inherent risks and complexities of cryptoasset safeguarding and administration, is becoming a key selection criteria for clients choosing institutional investors and service providers."

Alex Batlin | Founder and MD, Bitpanda Custody

“Pure technology can provide an alternative to credit intermediation without having custody or control over client assets, without becoming a counterparty to the transactions and without using or being limited by balance sheet. Through the digitization of assets held in a member’s own custodial account, real-time atomic exchange of assets, trade and payments netting, clearing and settlement automation, the right technology infrastructure can eliminate counterparty credit and settlement risk.””

Rosario Ingargiola, Founder & Chief Executive, Bosonic

Gateway To Crypto

Over the last few years we have seen a maturation in the crypto space in terms of companies building real products, protocols and solutions.

Blockchain technology is no longer a solution in search of a problem. We have seen many companies in the industry now building core infrastructure to manage the almost inevitable institutionalisation of the space.

Companies from multiple sizes and backgrounds choose to trade or take positions in crypto and now are actively selecting to add bitcoin to their balance sheet as a treasury exercise.

Interest in the space comes historically from technologists and innovators; later, those interested in alpha generation and emerging markets took part in the asset class. Institutional involvement perhaps started with the CME futures in December 2018, at the same time combined with a market collapse from a high of USD$20,000 which was not exceeded until 2021 and now.

Since then, trading systems, storage and regulations have developed substantially, and together more institutions are involving themselves in the space.

With significant risk comes great opportunity; however, engaging at an institutional level requires specific core infrastructure and "rules of engagement" to be in place to do so. When engaging with a crypto provider for trading, it is necessary to know how crypto trades are executed, along with slippage or measures of best execution.

Firms that can provide the same level of responses as to how they operate under other regulatory frameworks and procedures are at an advantage in engaging with institutions and professionals to automate their crypto trading needs.

Financial institutions are looking to engage at a similar level and terms to the other assets they trade in most cases, from compliance to connectivity.

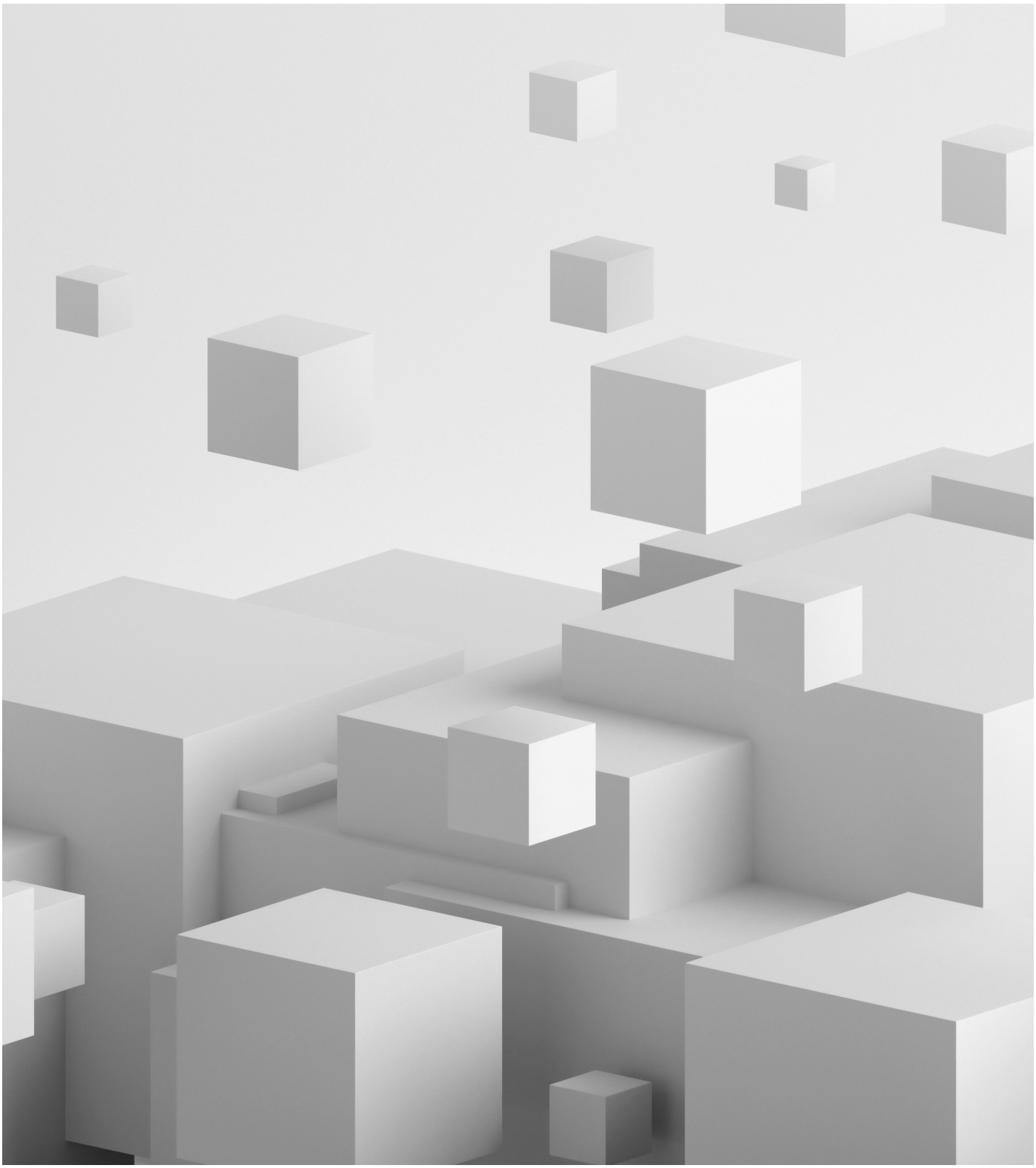
The Crypto Gateway perhaps started with CFDs (Contract for Difference) products in the case of some brokers (2017 onwards). Meaning wallets and technical aspects of cryptocurrency do not have to be managed. It also allows leverage to be afforded, more so if trades can be internalised. The same types of products, called 'Perpetuals' or 'perpetual swaps', are similar but "home-grown" from the crypto industry themselves. These are cash-settled instruments that track the underlying asset, and margin payments or interest payments are required to hold a position at a regular interval.

Traditionally, settlement payments were overnight, but in the case of perpetuals, it could be every 6 hours. Interestingly, this product has fallen out of favour with many regulators. For retail clients, in the context of losses associated with leverage products in general, CFDs are not permitted in some jurisdictions, including the United Kingdom. There is also client demand to have a wallet themselves, but at the same time, clients may not be happy using crypto exchanges as opposed to their trusted broker.

Crypto brokers starting now, who cannot offer CFDs, will be required to engage with crypto "physically" versus synthetics or other replicating instruments. Brokers and others now need to deal with wallets and trading venues not adhering to known standards, mainly because crypto brokers have set up outside the current financial system and have also been pushed away from it.

The crypto brokers have had two main obstacles in recent months, one adhering to trading standards, either in terms of having a FIX API or something more institutional, and infrastructure to cope at high frequency and high volume. Secondly, anti-money laundering has been seen as a risk, as by design, these are currencies based on cryptographic systems. As a result, they can anonymously engage in criminal activities or activities online compared to utilising a credit card or other payment providers.

When selecting an institutional venue, it is essential to consider the basic spreads and consider the entity you wish to engage with holistically. Gateway blockers include regulation, trading infrastructure, payments method and credibility.

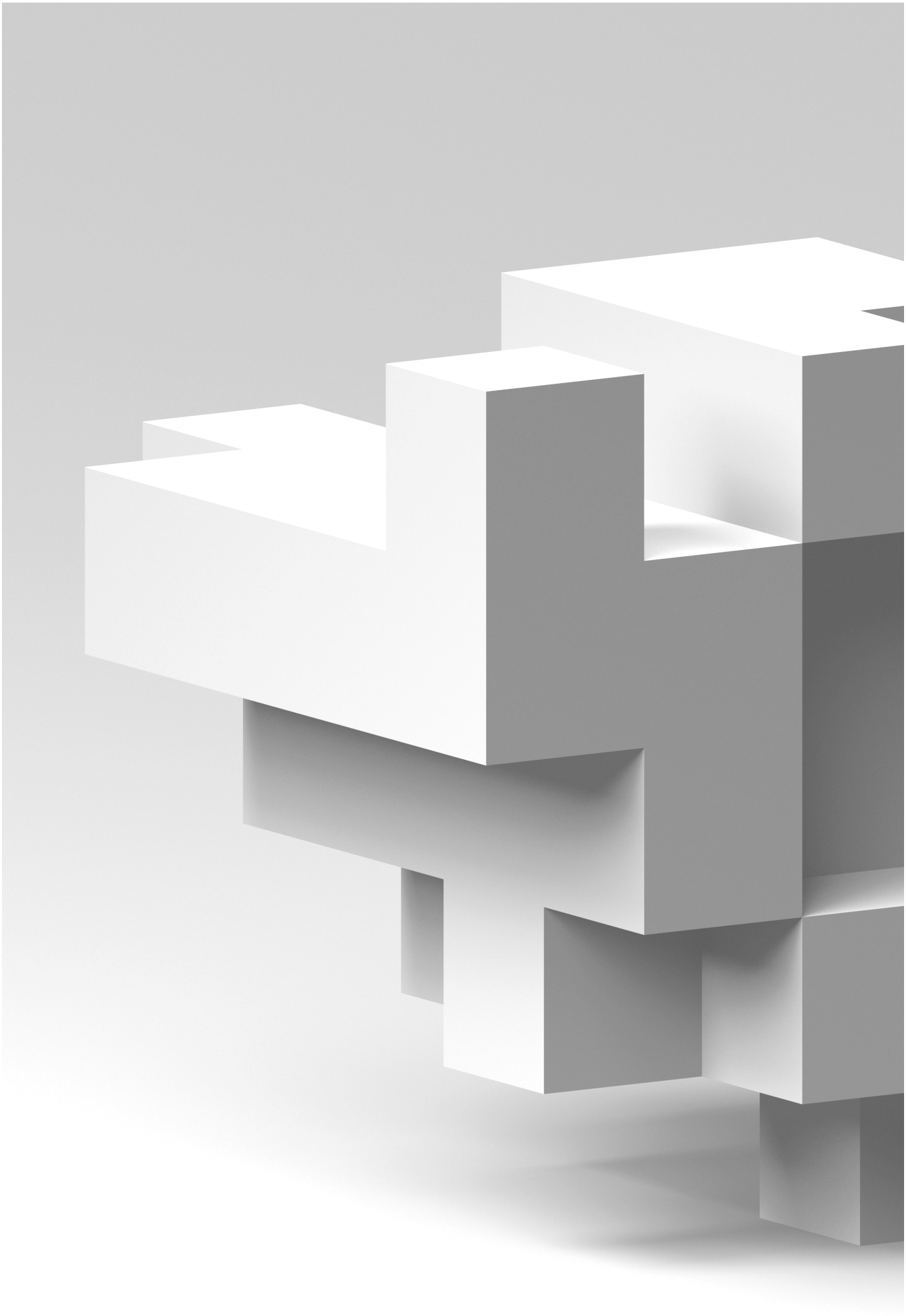


Trading Infrastructure

Many crypto exchange trading systems weren't originally designed to handle substantial volume and built by individuals outside the traditional financial industry. One may find the trade button may simply "not work" during times of volatility, or worse, prices and trading may fail entirely.

Check the type of institutional-grade technology employed, i.e., the matching engine and other associated connectivity is financial industry standard. Connectivity could take the form of WebSocket or FIX API or via different industry standards in FX, for example; that way, you can be more assured trade execution will be reliable.

It is also important to note the structure of the venue you are trading against. Are there any conflicts of interest that could arise in how trades are processed or with market makers and liquidity provision? How do these fare under more extreme trading conditions and volatility?



Regulations

Many jurisdictions have implemented specific registration procedures for crypto firms in addition to or related to the currently regulated trading statuses.

In the Financial Conduct Authority's (FCA) case, it was decided to move towards FCA registration, but the asset class mainly remains outside the regulated perimeter as a whole.

Compliance should consider the jurisdiction where the clients are registered or operating and check accordingly. It may be prudent to deal with counterparties in jurisdictions with robust legal frameworks and regulators who recognise crypto assets– providing some protection.

Unfortunately, regulators have not always been particularly detailed, meaning sticking to the top few traded assets by volume and leaving privacy coins out of scope should be considered. Along with this, assets and token structures that have been dealt with in law and by regulators may make the best choices to avoid additional regulatory risk and business problems.

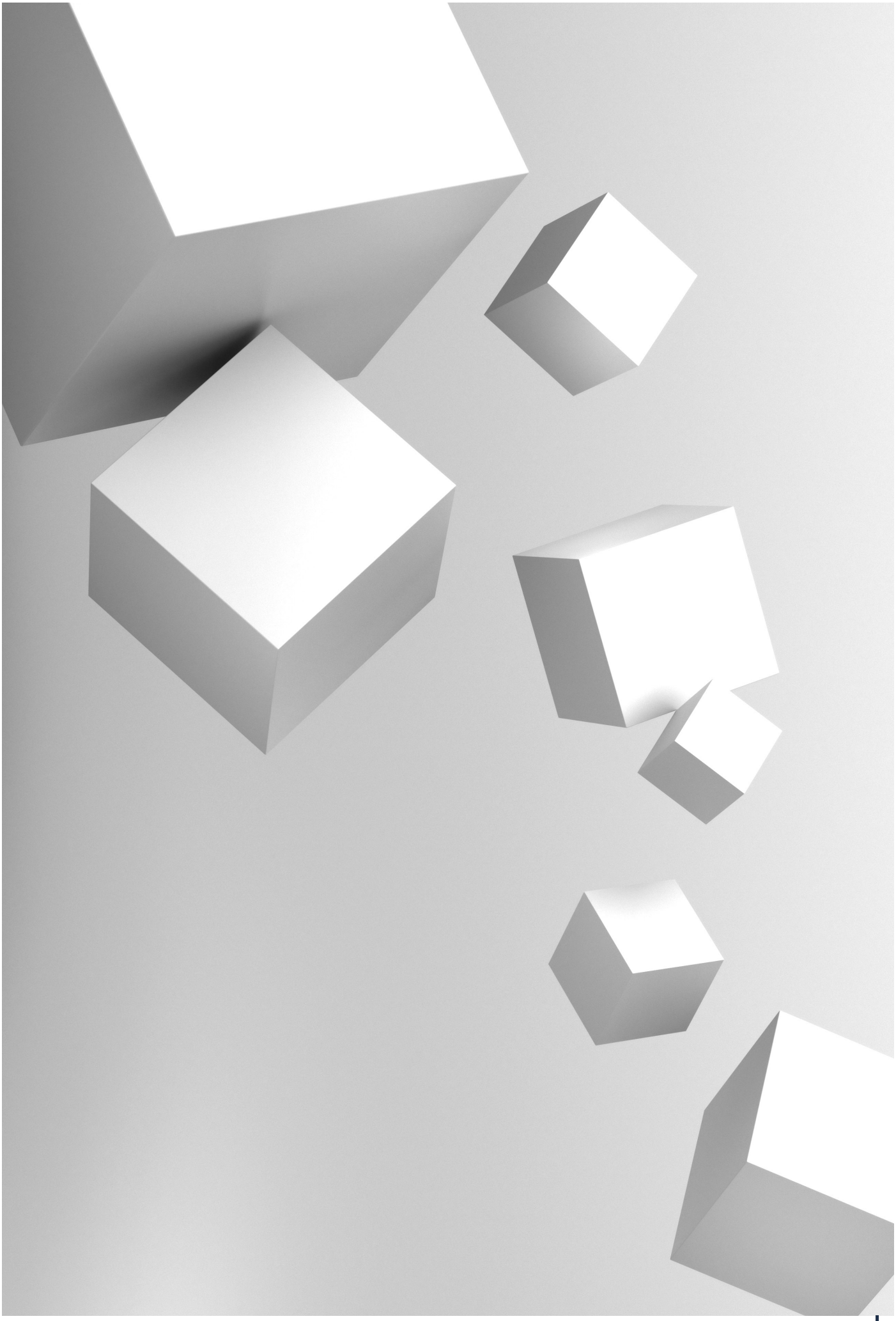
Small-cap coins can be manipulated; Initial Coin Offerings (ICO) are not usually present on the largest institutional venues and can be considered illegal financing and securities. Not only can trading such coins be problematic, but their custody and storage, along with additional functionality in their operation, cannot be assured.

The main regulatory aspects to consider are Know your Customer (KYC) and Know your Transaction (KYT), and companies strong in both can be regarded as institutional.

KYC procedures should be similar to other regulated brokers dealing with traditional financial products. Incoming bitcoin and crypto asset transactions should be screened for their association with the dark web or other activity associated with crime or terrorist financing. Uniquely most blockchain-based tokens and currencies provide a super audit trail compared to fiat.
The "Travel Rule" for cryptocurrencies hasn't precisely taken form yet, mainly pertaining to how information about fund provenance is passed between financial institutions. However, it is essential to consider how the exchange sees itself as compliant, considering this in the VASP framework from FATF. Exchanges should be prepared to implement more robust AML and KYC to be fully compliant or look to independent, insured crypto custodians to support this effort.

If these checks are not undertaken, there is a chance crypto assets obtained may be tainted, and clients may have issues trading them in the future.

Across the globe regulators are moving to bring crypto under their control and it is important to keep up to date with the latest changes as they occur.



Regulatory Frameworks

On the 6th of January 2022 the USA's House Financial Services Committee held a hearing on the future of cryptocurrency regulation. As part of that hearing they called on CEO's from several crypto companies to testify.

Whilst each jurisdiction and regulatory body in the world can take their own approach to the setting of rules, often there will be one that leads the way and informs the decisions made by the rest of the western world. Regulators now feel some pressure to rush through regulation of the crypto and DeFi space as it continues to gain traction with institutional investors and retail traders. What happens in America could very easily happen here in the UK next.

Knowing that the hearing could impact future regulations a number of companies involved released their own suggestions for Regulatory Requirements in the industry. Coinbase, Ripple, Binance & FTX have all created guidelines for digital asset regulation designed to help the committee develop cryptocurrency regulations.

Key Principles for Market Regulation

In FTX's proposal they identify 10 key principles that should be followed when considering the rules and regulations over the industry:

1. Proposing One Primary Market Regulator with One Rule Book for Spot and Derivatives Listings.
2. Full-Stack Infrastructure Providers and Maintaining Market-Structure Neutrality.
3. Custody of Crypto Assets – Key Functional and Disclosure Requirements.
4. Full-Stack Market Infrastructure Providers and the Lifecycle of a Trade – Addressing Risk Related to Token Issuance and Asset Servicing, Orderly Markets and Settlement of Trades, Cross Margining and Risk Management of Positions.
5. Trading Platform Providers – Ensuring Regulatory and Market Reporting.
6. Ensuring Customer Protections.
7. Ensuring Financial Responsibilities are Met.
8. Ensuring Stable Coins Used on Platform Meet Appropriate Standards.
9. Full-Stack Infrastructure Providers – Ensuring Appropriate Cybersecurity Safeguards are Kept.
10. Full-Stack Infrastructure Providers – Ensuring Anti-Money Laundering and Know Your Customer Compliance.

They open initially by discussing the jurisdictions of different bodies and how there should be one primary regulator for the crypto industry. This of course makes sense, there can be so many different asset classes represented on a blockchain that regulating the space would require the SEC for anything considered a security, but on the same blockchain you could facilitate derivative trading which would fall under the purview of the CFTC.

The details of the proposal are well worth a read but for Crypto Brokers in the UK the suggestions made for **Custody of Crypto Assets, Cybersecurity Safeguards, AML, KYC and Ensuring Regulatory and Market Reporting** are the ones to pay attention to as they are rules that often transcend nations.

Custody of Crypto Assets: Key Functional and Disclosure Requirements.

FTX suggests that a number of important questions should be answered by regulators on the issue of custody. While individuals and funds should be given the freedom to self-custody the importance of correctly storing your cryptocurrencies shouldn't be overlooked and as FTX points out "Where custody is performed on a customer's behalf by a platform operator or intermediary, appropriate safeguards should be disclosed in policies and procedures of the custodian."

To meet the requirements Crypto Brokers in the UK should consider if their custodian has Insurance, what wallet architecture they use, how private key security, management and transfers are managed, managing risks related to insider collusion or fraud; and physical security of data centres.

"Market supervisors should require regulated platform operators to perform regular diligence on their vendors and to have sufficient business continuity and disaster-and-recovery programs in place in connection with their vendor suite."

At Bitpanda Custody we always anticipated that regulations would take this direction which is why it was a priority to become registered with the UK's Financial Conduct Authority. Our FCA registration is another example of our commitment to providing regulatory compliant custody for brokers and exchanges in the United Kingdom.

Full-Stack Infrastructure Providers: Ensuring Appropriate Cybersecurity Safeguards are Kept

For brokers and exchanges cybersecurity is not a secondary thought. The importance of securing assets and data is vital, yet we hear of regular hacks against exchanges and brokers with devastating consequences. Additionally, with many brokers and exchanges, client funds are commingled or swept into a few addresses at times throughout the day.

This is usually because the infrastructure they are built on makes this cheaper and faster to do as well as allows for faster trades. The problems arise from hacks where funds aren't segregated, as large amounts can be stolen in one swoop.

FTX is proposing that regulators adopt policies that help facilitate the standardisation of cybersecurity safeguards domestically as well as globally. Bitpanda Custody understood the need for segregated accounts from inception.

With our Trustvault platform a broker/exchange can open as many subwallets as they want, meaning that clients can have their own cryptocurrencies in segregated wallet addresses but still access capital for trades and liquidity with sub-second latency. This is just one feature that we believe can satisfy potential future rules on cybersecurity.

Our upcoming rollout of an Ethereum DeFi simulator and decoder should further help with providing additional security measures. In simple terms, institutions will be able to simulate a transaction to see where the funds will actually end up before signing a transaction. But the key here will be the ability to see in plain English what they are signing (Decoder) and where their funds will likely end up (Simulator) vs. spending time and effort figuring out what the underlying binary or transaction hash data says. In this way, Bitpanda Custody is enabling early detection of fraud or illegal activity and minimising the potential for financial losses.

Full-Stack Infrastructure Providers: Ensuring Anti-Money Laundering and Know Your Customer Compliance

Appropriate use of KYC as part of user onboarding and conducting regular anti-money laundering surveillance of user activity (both on the trading venue and via the scrutiny of related on-chain transfers in and withdrawals out) is the key takeaway from the recommendations. FTX suggests that all marketplace

operators should regularly perform self-audits.

AML compliance is going to be a requirement globally from both a KYC and KYT stance. At Bitpanda Custody, we already have compliance baked into our platform with tools in place to meet these recommendations beyond even the standards set recently by the SBAI (Standards Board for Alternative Investment).

When transactions are received by one of our clients they are all automatically run through Chainalysis and any suspicious transactions are flagged and investigated by our compliance team. Equally, outbound transactions are also monitored and investigated. Additionally, for all inbound and outbound Ethereum transactions, we provide our clients with transaction risk rating and counterparty cluster information e.g. gambling, mixers, terrorist financing etc. through our webhook payloads.

This ensures an easier way of monitoring for direct transactional exposure risk, eliminating the need for institutions to manually perform pre-flight checks themselves, which saves on time, cost and effort.

Trading Platform Providers: Ensuring Regulatory and Market Reporting

Crypto Brokers in the UK need to be able to report transactional activity if and when required. This can become a time-consuming task if the underlying wallet infrastructure isn't built with reporting in mind. The recommendations being put forward to the House Financial Services Committee are more focused on the risks of market manipulation.

"Regulatory reporting of transactional activity should be required in order to provide market supervisors appropriate visibility into the trading platform, and to better allow supervisors to police for market manipulation and other unfair trade practices." We looked at how Bitpanda Custody can help with compliance and operational due diligence requirements when we recently reviewed the SBAI Operational Due Diligence on Crypto Assets guidance.

With our TrustVault custodial wallet platform, institutions can view transactions enriched with AML & DeFi data on web or mobile apps, export to CSV, or query via APIs, all in the currency of their choice.

For institutional investors, we've included better NAV reporting by allowing them to see the value of all their portfolio assets deposited on protocols by a point-in-time, frequency or number of valuations view.

Building On The Right Solution Matters

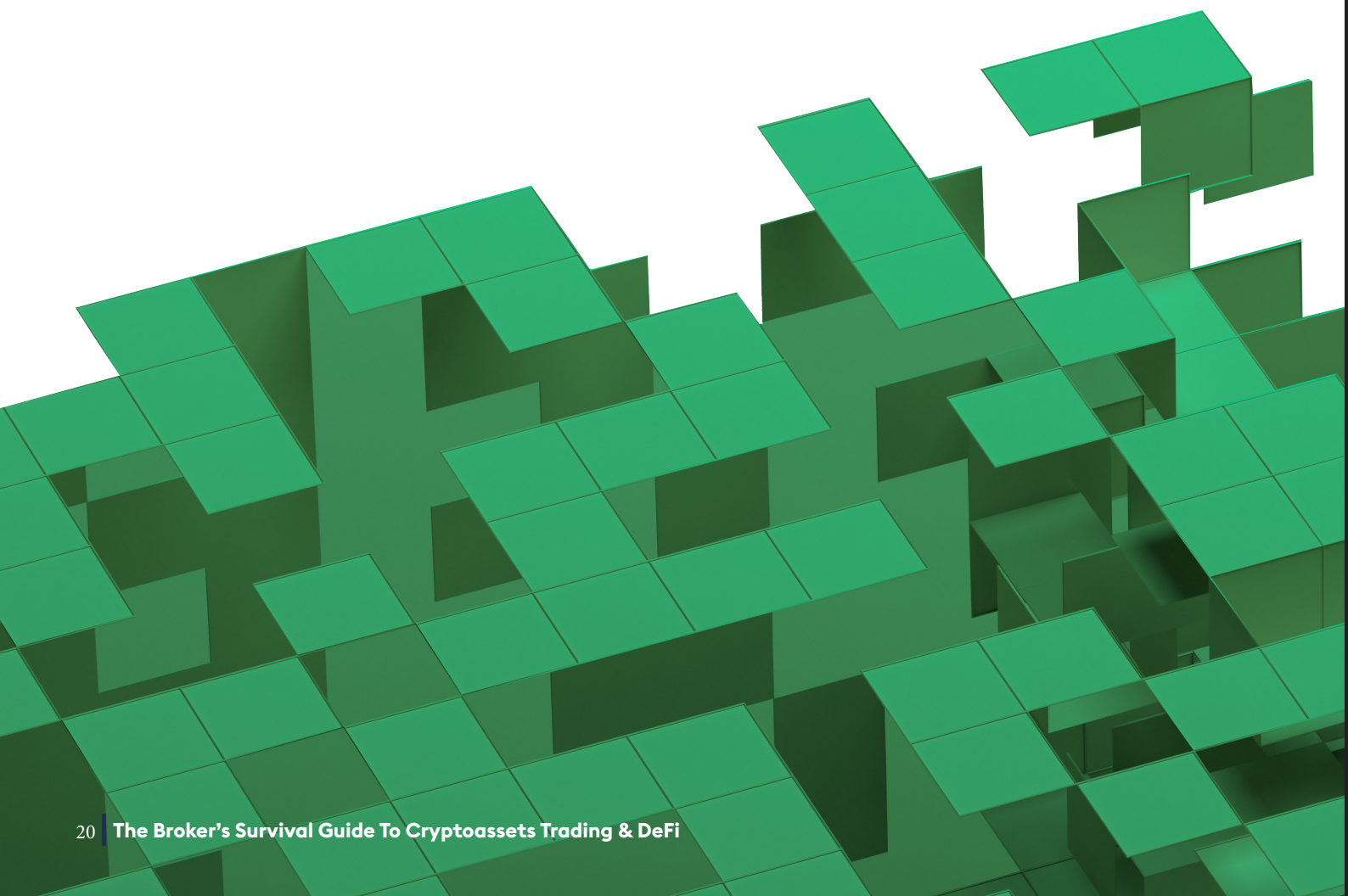
With more and more governments looking at formal regulations for the crypto and decentralised finance exchanges and brokers are considering their position and making changes to pre-empt new laws. Waiting until regulations come through could lead to serious disruption to operations and potential losses in revenue.

For existing crypto brokers making those changes to the backend of their platforms can take some time so many are beginning the process now. For brokers and exchanges moving into crypto from traditional markets, this can be avoided by building on the right infrastructure solution. In either case, using Bitpanda Custody's Trustvault platform for custody can reduce the friction and cost of meeting many of the possible regulatory requirements that may develop from this week's hearing.

FTX RECOMMENDATIONS ON:	WHAT BITPANDA CUSTODY OFFERS:
Custody & Crypto Assets	TrustVault uses Scalable HSM technology that protects your private key whilst allowing for recovery & account management. We are an insured custodian registered with the UK's Finance Conduct Authority.
Cybersecurity Safeguards	With Bitpanda Custody's TrustVault, all of our clients' addresses & accounts are segregated & never commingled. Our solution has multi-party authorisation & the ability to set admin rules on who can access funds & how.
AML & KYC Compliance	Transaction monitoring is available as standard, giving you inbound & outbound transaction notifications enriched with AML risk data. Transactions are run through Chainalysis & suspicious activity is investigated by our compliance team.
Ensuring Regulatory & Market Reporting	View transactions enriched with AML & DeFi data on web or mobile apps, export to CSV, or query via APIs. For institutional investors, we've included portfolio reporting enabling institutions to more accurately report on NAV by allowing them to see the value of all assets deposited on protocols by a point-in-time, frequency or number of valuations view.

Payments

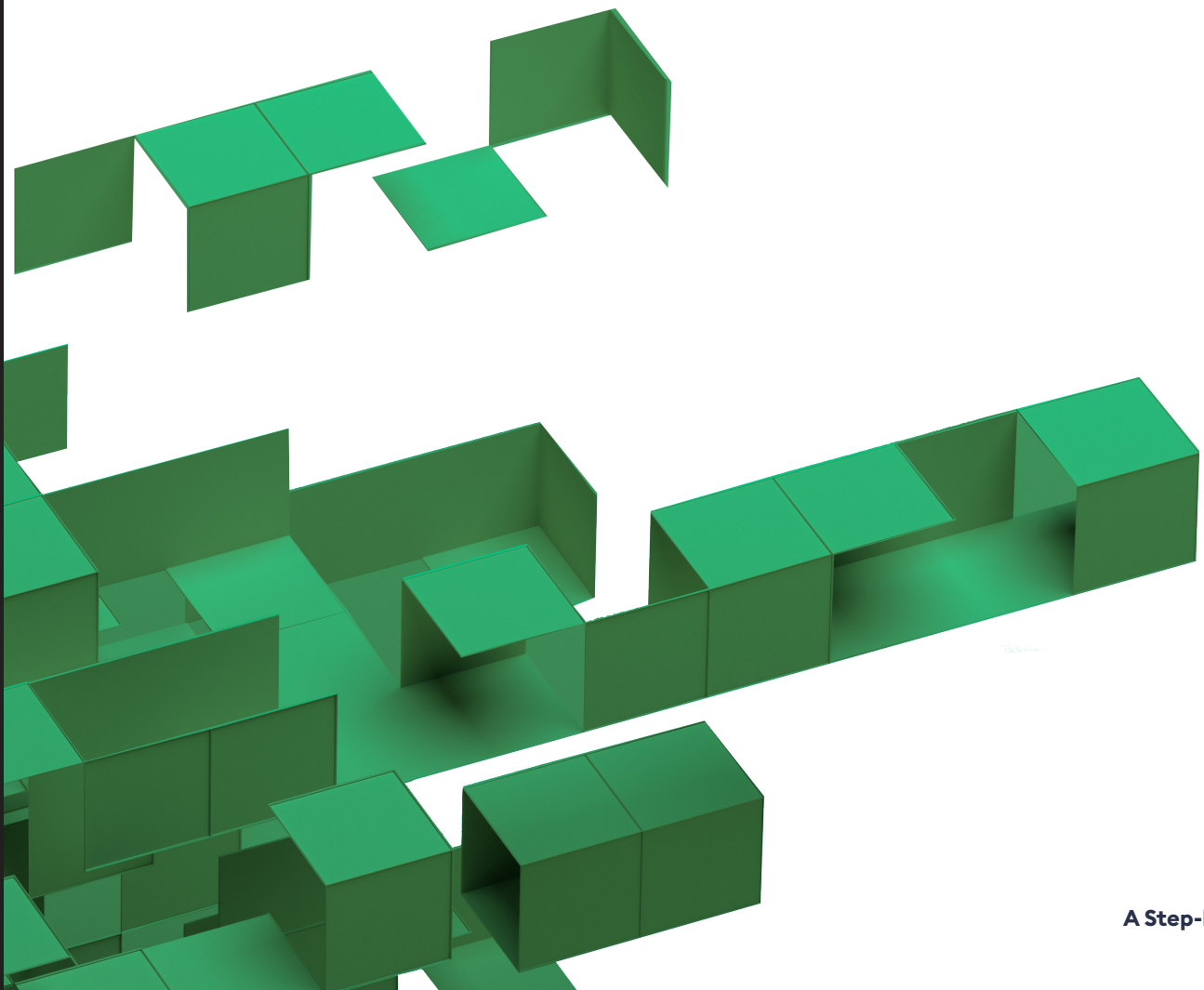
Some digital asset exchanges take solely or primarily payments in stablecoins such as USDT (Tether). However, theoretically, it is the goal of crypto to remove market friction, and stable coins are part of this. Clients should be wary of companies engaging solely on that basis and may wish to consider these companies' reputability. Banking relationships and other credible payment rails may go some way to reassure clients that on/off ramping crypto assets and fiat is not an issue, especially if withdrawals need to be requested from the exchange more frequently or for large amounts.



Credibility

People and previously regulated individuals are a good starting point, meaning they know institutional workflows and existing regulatory frameworks. However, these may not be directly applicable to crypto assets. A review of the jurisdictions of incorporation and regulatory permissions held is vital to verify a trading venue will work as an institutional counterparty.

All in all, the next generation of crypto trading platform providers will have to further integrate with the global financial system and regulators as a whole. This means that compliant turnkey solutions will most likely reign supreme over the crypto-based industry venues of the past. One side of it means existing crypto Exchanges will gain better technology, banking relationships and compliance. Still, on the other side, traditional players will build their stack from the other direction, incorporating new technology. It then depends on who can attract more clients and which side has credibility over the other?



Crypto Asset Custody

Decentralised Finance & Digital Asset Trading For Brokers

The market cap of cryptoassets markets is growing fast. Institutional interest is rising, and players view the industry as an opportunity for growth compared to traditional financial markets.

Cryptoassets, a subset of digital assets, are based on a fundamentally different technology, known as blockchain, as compared to traditional financial rails. As such, brand new infrastructure is required to safeguard and administer traded cryptoassets. In addition, new decentralised financial services, known as DeFi, are on the rise, offering new trading, lending and hedging venues as well as passive yield opportunities.

The technology landscape is complex, yet getting it wrong risks losing your assets. Aside from technology, custody of assets is becoming a regulated activity. Building your own infrastructure and getting regulatory approval is becoming prohibitively expensive and time consuming.

In response to this emerging movement, crypto custody solutions like Bitpanda Custody's TrustVault platform, are one of the latest innovations to appear in the digital asset ecosystem, signalling the dawn of institutional capital entering into the cryptoasset industry. Brokers are increasingly using such independent custodians to accelerate their go to market timelines whilst reducing costs and risks.

Read on to discover the fundamentals of cryptoasset custody, its challenges and solutions. Learn what you can do to harness the opportunities while avoiding the pitfalls.

How is Crypto Asset Custody Different From Traditional Financial Custody?

Custody is an umbrella term used in financial services that refers to the ability to safeguard and administer assets. Crypto custody shares the same goals as traditional custody, but focuses on safeguarding private keys and using them to only sign authorised transactions, versus holding and servicing assets.

That's because cryptoassets are stored on decentralised ledgers, and have embedded transactional logic. So the custodian is no longer concerned with record keeping and servicing. Yet every transaction must be signed with the correct private key, and submitted to the network. Which means that loss or theft of private keys along with signing of fraudulent transactions are the new key risks to be managed by custodians.

For brokers, having control of private keys on behalf of clients is the equivalent to offering custody services. The fundamental problem in digital assets lies in how easily assets can be lost without the proper foundational layer that secures the storage and use of private keys. Yet for customers and brokers alike, many of the solutions available today are either too slow, expensive, difficult to manage, complex, not scalable or simply not secure enough to handle potential threats.

Security Problems & Loss of Private Keys

As already mentioned, the loss or theft of private keys is detrimental. If a hacker gets hold of the private keys, they can transfer funds to an address only they

control. If the keys are lost, assets can never be spent, rendering them useless. Therefore, lost or stolen keys equates to lost or stolen assets.

Security risks only increase when assets are managed by organisations rather than individuals, as private keys need to be shared. It's easy to share keys – just hand over a copy, but impossible to unshare! If someone with the knowledge of the private key leaves the firm on bad terms or has hidden intentions, the organisation is left exposed to potential theft and loss of their digital assets from the individual if they're unable to move the assets off the addresses quickly.

But even if the keys are not lost or stolen, assets can be still stolen as a result of fraudulent transactions. Ideally the keys are never exposed to users. Instead transactions should be proxied through a custodian, who can apply controls to ensure that all approvals are gathered and all policies are satisfied, before the transaction is submitted to the blockchain.

For example, multisig controls allow both sharing of wallets in an organisation, and approval workflows, e.g. 2 out of 3 employees must approve a transaction. Approval lists can control where the funds can be sent. However, given the almost infinite variety of required controls, it is important to work with a custodian who can support custom automated rules to ensure that any scenario can be accommodated for.

Latency & Friction

To avoid loss or theft of private keys, it is a good idea to store and back them up in a secure place. One option is to store them off-line i.e. create the key inside a secure electronic device, known as a hardware wallet, and keep the device in a physical bank vault.

This is known as cold-storage, which sacrifices convenience for security, as every transaction requires a physical trip to the bank. The introduced latency may not be an issue for long term investors, but is a show-stopper for traders.

Cold storage solutions are therefore often impractical when handling thousands of transactions and countless keys. With latency of up to two hours or more, today's brokers require sub-second transaction submissions which independent custodians can provide.

The alternative is to keep the keys on your laptop or

mobile phone harddisk. This is very convenient as keys can be quickly used when signing transactions in a web browser or mobile app, but easily hackable.

Security can be enhanced by storing the keys in a hardware wallet, as the key cannot be extracted by hackers. All the user has to do is attach the wallet device to their laptop when a signature is required.

However, sharing physical devices is a challenge for traders dispersed across different geographies. This causes significant friction, makes the process expensive, and means frequent trading is more difficult as it is tied up with manual processes to sign transactions.

Transparency & Segregation

Historically, lack of transparency is considered one of the main contributing factors towards reputational disrepair or prolonged crises for financial institutions. Like in traditional finance, the larger the total transaction sums become, the more of an issue poor visibility and transparency turn out to be.

Many crypto custodians rely on omnibus accounts, where customer assets are commingled on a single address. It simplifies key management, and allows cheap and fast off-chain transfers. Yet, it sacrifices transparency, as the customer no longer has an independent mechanism to monitor transactions, and fully relies on the custodian to act in an agreed manner e.g. no re-hypothecation. Omnibus accounts also introduce legal uncertainty under liquidation, i.e. are assets on or off the balance sheet.

Lack of transparency introduces additional and often unnecessary custodial counterparty risk, which may be unacceptable to traders. Solutions that support segregated accounts i.e. one or more dedicated addresses per customer, offer the means to independently monitor transactions, reducing the level of trust required in a custodian.

In the worst case scenario, keys for segregated accounts can be simply handed over to customers, unlike omnibus accounts where handing over keys to one customer will mean losses for all others.

Reconciliation Difficulties

There is an additional problem with using omnibus accounts. Cryptoassets like BTC and ETH do not allow inclusion of reference numbers in transfer transactions. And since all accounts are pseudonymous i.e. you don't know their owners identity, it is hard to reconcile transfers to specific customer deposits or payments.

The solution is to create a new address for each customer, or payment. This way any received assets can be reconciled against a customer or a payment.

However blockchains do not have an alerting system for incoming transactions, so to reconcile transactions, you need to not only create a new address, but monitor all blockchain transactions that send funds to that address. Once a transaction is detected, the received balance can then be added for example to customer trading credit.

Following on with our trading credit example, if brokers need to process withdrawals, then the customer's balance needs to be first reduced by withdrawn amount, and only if there is sufficient cleared balance, should the transaction be placed on chain.

Whilst it is possible to perform all of the above operations manually, such an undertaking becomes overly expensive in a 24x7 operating environment. This means non-programmable end-user solutions like hardware wallets are simply not practical. You need solutions with APIs to allow automated straight-through-processing.

Compliance Risks

Monitoring inbound and outbound transactions is also important from a compliance point of view. You need to be able to quarantine received funds, and block sending of them, if they have direct exposure to high-risk counterparties.

A custodian should be able to perform such activities; however, a broker may wish to have additional policies e.g. block any transfers to a gambling address. In this case a custodian could augment the transaction alert data sent to the customer with transaction risk data, to reduce the burden of compliance.

Asset Variety & DeFi Support

The programmable nature of blockchain has precipitated an explosion of new asset classes. Anything and everything can be now quickly and cheaply issued

and managed as a token on blockchain. But this variety comes at a complexity cost - a custodian needs to be able to support a huge variety of assets and transactions types.

Complexity only increases when such assets are used with DeFi services. A custodian needs to support an ever growing variety of transaction types that such services offer, coupled with the transactions permitted on the asset itself.

Traditional custody, where assets are sent to the custodian and they perform all the necessary actions, simply does not scale in this new model. The custodian will never be able to keep up with all of the innovation.

Instead, a custodian must be able to securely sign any DeFi and asset transaction. This can be achieved by using the new blockchain architecture that uncouples data and associated business logic, user interface and transaction signing.

The data and business logic that governs assets and financial services resides on the blockchain. The user interface resides on a website, and any number of website apps can use exactly the same blockchain smart contracts, allowing customisation of the user experience but shared data usage.

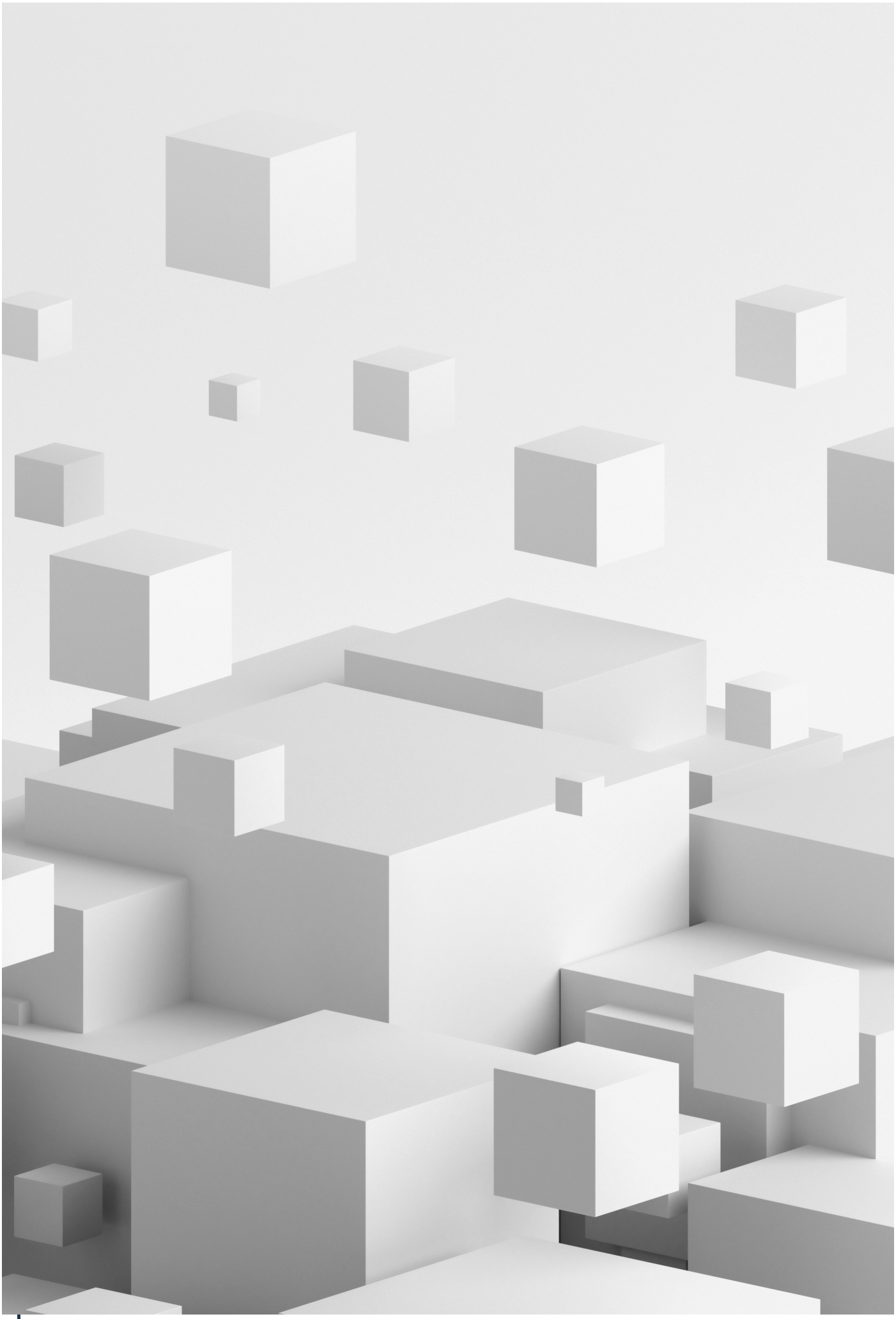
Finally, the signing of transactions is done by the custodian. This means that the custodian is only responsible for authenticating the transactions generated by the website, signing them, and submitting them to the blockchain. Such a scheme allows a custodian to offer universal support for assets and financial services. This vastly improves the utility of assets, as compared to asset-holding-only custodians.

However, the custodian must be able to interpret which transaction is being requested e.g. trade a specific asset, and have the ability apply controls such as multisig approve lists to ensure that transaction has been approved by all required parties and within policy.

Credit and Lending

A variation on the themes above are bilateral arrangements between custodian and crypto exchanges, whereby pledging funds in custody translates into trading credit on the exchange, without the need to transfer funds.

Beyond on-exchange trading credit, the custodian is in a unique position to support under-collateralised lending. Addresses on blockchain are pseudonymous i.e. you don't know who you are dealing with. But the custodian has the ability to dereference aggregated addresses to portfolio balances, both on-chain and on-exchange. The custodian can then perform risk analysis, especially if coupled with pledge enforcement, and secure best credit rates for the customer.



Putting It All Together

The right custodian partner will assist the broker in building confidence in their operational capabilities, and as such more likely to attract more customer trading higher volumes. And do so faster and cheaper. If the custodian is able to support access to a whole range of venues and services, including DeFi, brokers will also be able to better source liquidity, and offer differentiating features like yield and margin.

So here are some key features to look out for and question:

1. High-performance security at scale. Can the custodian provably safe-keep private keys and manage transactions in near real-time, even under heavy load? Is the infrastructure resilient against failures?
2. Flexible controls. Can groups of people manage cryptoassets in a controlled manner e.g. multisig, allow-lists? Can you easily add custom controls e.g. to control DeFi transactions?
3. Segregated accounts. Can you create as many individual keys as you need and independently monitor transactions?
4. Compliance monitoring Can you get notified of the transaction risk and make a decision on how to proceed?
5. DeFi support. Can you manage a wide range of cryptoassets across a multitude of decentralized financial services?
6. Exchange accounts. Can you securely transfer funds between centralised exchanges?
7. Clearing and settlement. Can you use your cryptoassets in custody to clear and later settle OTC transactions?
8. Trade credit. Can you use your cryptoassets in custody as trading credit on exchanges?
9. Under-collateralised lending. Can you use your cryptoasset portfolio under custody to secure loans?

Emerging brokers face two choices. Either they build the infrastructure themselves and take all the burden of risk, manage complexity alone, and apply for their own custodial wallet license (which can take up to a year or more).

Alternatively, they can choose an independent crypto custody provider like Bitpanda Custody – backed by a wealth of trust and expertise, and a functional, integrated solution that grows as your business scales.

Clearing & Settlement

How to Eliminate Counter-party Credit and Settlement Risk as a Digital Asset Broker On Layer 2 Blockchain

Institutional demand for access to cryptocurrencies and other digital assets has undeniably arrived. This is evident from headlines about large outright purchases of Bitcoin, to the land grab for institutional infrastructure through acquisitions and investments by the leading traditional financial institutions and fintech players.

Many of these institutions will access the digital asset markets through regulated brokerages, and therefore, many traditional brokerages and new, specialized brokerages, are looking to offer digital asset trading and services to their clients. Once a brokerage firm is comfortable with their regulatory positioning, the next major tasks include:

1. determining how they will handle custody safely and in a compliant manner;

2. how to efficiently access highly fragmented liquidity; and

3. avoiding or eliminating counterparty credit and settlement risk. the focus of this blog in our series.

How do you bring together neutral, regulated, insured custody with aggregated global liquidity from all the top retail and institutional exchanges, market makers and OTC desks for best execution, as well lending and borrowing, plus the trading screens and APIs to deliver all of this to the end customer? Read on to learn how Bosonic brings together world-class, independent digital asset custody from Bitpanda Custody and deep liquidity from GCEX in an Infrastructure-as-a-Service offering that can power your digital asset brokerage with the lowest possible risk and cost.

How Does Clearing and Settlement Work in Traditional Markets vs. Digital Asset Markets?

The process involves trade netting to identify what is owed to whom between a number of different parties, while simultaneously enforcing how a payment will be settled. Clearing is arguably the most complex of the two functions, since it involves netting down trades from many different counterparties into a net settlement amount due between the parties. For maximum capital efficiency and lowest risk, this must be done multilaterally in real-time. Typically, settlement is the riskier process since it involves managing the actual transference of ownership of fiat and digital assets in order to achieve finality.

In traditional markets, clearing and settlement of trades can take up to three days, thus, there's typically a large financial institution who acts as the backstop for the money owed. These can be Tier-1 banks serving as the Prime Broker and/or Central Counterparty (CCP) or other clearinghouse organizations who are then responsible to make sure that there is no counterparty credit or settlement risk, even if the original counterparties to the trades don't settle.

Currently, the biggest barrier to adoption for institutional investors, and especially fiduciaries in crypto and digital assets, is that there is no Tier-1 bank prime broker, central clearinghouse or institutional consortium like DTCC or CLS Bank providing an equivalent solution to fully eliminate these major risks to trading counterparties.

What is Prime Brokerage Anyway?

There is confusion in the digital asset space about what a prime broker provides to its clients. Some associate lending or liquidity aggregation with prime brokerage, but the core function is actually credit intermediation. This means substituting the Prime Broker's credit for the client's credit so that the client trades legally and financially in the name of the Prime Broker, i.e., on the prime broker's own credit line with other counterparties and/or their counterparties' Prime Broker.

This is similar and functionally equivalent to a clearinghouse which novates trades by becoming the buyer-to-every-seller and the seller-to-every-buyer, and bearing all the counterparty risk for both sides of every trade. Huge amounts of balance sheet, loss-reserve funds, member capital, insurance programs and other sources of funding sit behind these services.

Today, no organization in the digital asset space has a big enough balance sheet to facilitate true credit intermediation at scale for the entire institutional market. Even if a major bank decided to take balance sheet risk as a Prime Broker, it likely would have limited utility, because very few market participants would qualify for this credit underwriting and the balance sheet requirements would be very high and thus, the leverage gained would be very low (e.g, CME Bitcoin futures leverage is approximately 2:1 maximum so the clearinghouse can manage the risk).

The way the existing digital asset marketplace is structured, there is no such guarantor for clearing and settlement, so if the net amounts due aren't settled, it can result in a total loss. A default can have a cascading effect as other counterparty settlements fail – known as Herstatt Risk – and can ultimately force even major market participants into default and bankruptcy. Leverage in the system can make this cascading effect even more extreme.

Fake Prime Brokerage

Some companies claiming to provide "prime brokerage" services in digital assets actually increase their clients' counterparty credit and settlement risk substantially. How so? These firms 1) hold their client assets directly and/ or, 2) extend unsecured credit (aka leverage) to their clients for trading, 3) place client assets at centralized exchanges or create credit relationships with the exchanges, and they 4) establish credit lines with market makers and OTC desks that are not secured by any collateral. This is necessary in order to access liquidity on the clients' behalf or for their own hedging (where they are acting as a principal or riskless principal on the trades).

When assets are deposited with a centralized crypto exchange, the traders are issued the equivalent of a promissory note for their deposit held in an omnibus structure. However, these promises to repay could be rendered worthless if the exchange suffers from a hack, fraud or flash crash that results in off-market trading and liquidation of levered positions that blow through client collateral, creating debit (negative) balances on client accounts. Such losses may be mutualized and borne by all the clients of the exchange. Additionally, accounting information for all trades cleared and settled internally is in a regular database and not blockchain-based with cryptographically provable transactions and ownership chains, making it easy to manipulate and adding another dimension of risk. Institutional clients and fiduciaries want to avoid even indirect exposure to retail exchanges as counterparties. Needless to say, they also want to avoid uncollateralized credit risk with market makers and OTC desks.

With such so-called "prime brokerage" firms, whether they are trading with the client as a principal or on an agency basis, the client is accepting substantially increased and non-transparent counterparty credit risk for the convenience of having a single account to access multiple sources of liquidity. Even where advanced execution technologies are provided, the gains do not justify the risks for institutions and fiduciaries.

Institutions entering the space could have a false sense of security based on their experience and reliance on traditional prime brokers – they need to remember to ask these digital asset "prime brokers" some critical questions, such as: 1) who is my counterparty to the trades?; 2) how big is the counterparty's balance sheet?; 3) will my assets be held at retail exchanges?; 4) will I have indirect exposure to credit based trading with exchanges or market makers or even other clients?; and 5) if yes, are these credit arrangements collateralized or unsecured?

Settlement Network Risks and Limitations

In the OTC crypto market where trades occur off-exchange between clients and market makers and OTC desks, trades are settled bilaterally between each pair of trading counterparties. While some wallet solutions are dressed up as a "settlement network," and may make it easier and faster to settle net amounts due bilaterally between the parties, material counterparty credit risk still exists.

In such self-custody solutions, the counterparties must, at the time that settlement is due:

1. have the assets to settle–which is dependent on trade netting and receipt of settlement payments from many other parties;

2. agree to settle; and

3. have someone agree to go first, i.e., you transfer USD and hope to receive BTC in return from your counterparty–rinse and repeat with every counterparty, every day.

For brokers and asset managers who are fiduciaries, these are unacceptable risks. Furthermore, regulated entities generally can't self-custody client assets, which can make certain solutions commonly used to facilitate bilateral settlement unsuitable and not regulatory compliant.

Other attempts at trying to create a settlement network have different tradeoffs such as forcing all counterparties to a single custodian "walled garden," and then forcing allocation of capital to specific individual exchanges on a pre-trade basis, or forcing use of custodian provided liquidity and trade execution.

Ultimately, it is critically important to be able to trade not just with any counterparty at a single custodian from a single pool of collateral in the client's own account, but with any counterparty at any custodian. This requires a cross-custodian trade execution and trade netting and settlement capability that uses a shared protocol, and avoids transferring risks to the participating custodians.

It seems obvious that to scale, this solution needs to leverage blockchain and smart contracts with atomic settlement movements that are payment-vs-payment (PVP: concurrent and atomic).

Mere promises to pay based on contractual obligations with settlement movements that are delivery-vs-payment (DVP: "who goes first" or Herstatt Risk issues) are not even used in traditional markets for net settlement between institutions.

Flavors of Liquidity Aggregation

Liquidity aggregation is critical for any institutional crypto offering, but not all "aggregations" are created equal. Some digital asset trading platforms do the technical work of integration to multiple liquidity sources and display consolidated liquidity in the aggregate with useful execution tools. However, to make the aggregation actionable, clients must:

1. have an account and assets at each underlying e change;

2. have a credit line with each underlying market maker in order to trade on the aggregation; and then

3. they must rebalance assets on the various exchanges and make bilateral settlement payments continuously.

These solutions are generally noncustodial with respect to the platform provider, which is important, but there are material flaws in this approach including:

1. not eliminating counterparty credit and settlement risk to the underlying exchanges and market makers;

2. extremely inefficient use of capital (collateral); and

3. substantial manual human reconciliation and rebalancing effort with increased operational risks and costs.

Other liquidity aggregators that often position themselves as "prime brokerage" are custodial given the clients open an account similar to that of a centralized exchange and transfers assets into their custody. These types of aggregators may send your assets to exchanges and/or open up uncollateralized credit lines with market makers to source liquidity for you or for their own hedging purposes.

They often become the counterparty to the trades as principal or riskless principle. The underlying liquidity sources may not be transparent to the client, nor is the markup on the underlying core liquidity, increasing the spread that clients may receive and therefore execution costs. While providing some convenience, these types of solutions increase risk substantially.

Truly tradable aggregation of liquidity with no counterparty credit or settlement risk is only possible with Tier-1 bank or clearinghouse credit intermediation. Today, this doesn't exist in digital asset markets. The only viable alternative is the approximation of credit intermediation based on technology which performs an atomic exchange of fiat and crypto assets that have been digitized onto Layer-2 custodial blockchain ledgers with realtime clearing and settlement.

This solution allows clients to face any liquidity source they choose, from exchanges to market makers, OTC desks and other market participants from the safety of their own custodial account. Brokerages can take advantage of existing pools of deep liquidity such as GCEX offers from their own account at their own custodian.

Lending and Borrowing

Institutional lending and borrowing are highly intermediated and inefficient in digital asset markets. Lenders generally entrust their assets to lending intermediaries and have to transfer their assets to this intermediary. The intermediary then seeks to find a borrower, AML/KYCs the borrower, and then enters into an agreement with the borrower. The borrower then sends collateral assets to the intermediary (e.g., USD) who then transfers the loan proceeds or assets (e.g., BTC) to the borrower. The intermediary then has to actively manage the default risk and eventually sends a portion of the interest rate paid by the borrower to the asset owner after first taking their cut. The current solutions have too much risk, not only to the intermediaries holding the assets, but with assets moving between various parties, and without a way to compel the return of coin when the crypto appreciates beyond the value of the collateral.

A model has emerged where lenders and borrowers hold fiat or digital assets at their own trusted custodian and avoid any asset movements. Lenders can

easily manage their interest rates and risk parameters such as initial, variation and liquidation margin levels (LTV levels), as well as credit preferences. The assets are digitized without moving them from the owners' accounts to facilitate programmatic lending and borrowing in a real-time lending marketplace. This approach makes it possible for anyone with collateral on the network to be able to borrow assets made available for lend programmatically, on-demand, elastically, intra-day and at high velocity with no commitments on duration. Lend/ borrow transactions can be executed as a repo transaction in real-time on custodial blockchain ledgers as an atomic exchange. This will make it possible to achieve unprecedented levels of capital velocity and trading activity.

This frictionless approach using digitized assets held by custodians can provide the institutional market with an aggregation of virtually unlimited third-party balance sheet for large-scale Prime Services like short lending, margin and leverage financing. This will support asymmetric trading relationships between various counterparty funding configurations, e.g., credit vs. fully funded, credit vs. margin, credit vs. credit, margin vs. margin, etc., while allowing the parties to be fully funded legally intra-day, and shifting credit risk to a wide range of willing lenders who know how to price these risks. It will also facilitate a competitive lending marketplace without intermediation, rehypothecation risks, or movement of collateral, as well as drastically reducing systemic risk by distributing risks away from any single balance sheet and guarantor structure.

Preparing For A DeFi Future

What Can Digital Asset Brokers Do to Plan Ahead For a DeFi Future?

Today's emerging digital asset brokers should note that decentralized finance (DeFi) is a broad and complex playing field. There is a big AML/KYC question to solve for institutional participation in DeFi. In the current DeFi landscape, interactions are anonymous, but brokers need transparency because institutional clients will require it.

Brokers can partner with a custodian like Bitpanda Custody who can facilitate staking and lending from a custodial account while maintaining policies and controls necessary for regulatory compliance.

Institutional DeFi-like services amongst parties that each AML/KYC through a regulated custodian, such as the above described lending marketplace, offer a nearterm solution for opportunities like margin and leverage financing for a yield.

Without a doubt, future solutions will bridge to the broader DeFi protocols and unlock tremendous potential gains in both access to liquidity and crowd-sourced balance sheet, as well as yield farming.

Institutional Technology Infrastructure that brings custody and liquidity together

It is important to clearly understand all of the risks and tradeoffs in order to scale an institutional digital assets brokerage. The key foundations and capabilities of a winning solution include:

1. Custodian Agnostic: hold your fiat and crypto assets in your own account at a neutral, compliant custodian that focuses on bullet-proof asset custody and security.

2. Real-time Clearing and Settlement with Atomic Exchange: tokenize your fiat and digital assets at your trusted custodian on a Layer-2 blockchain and experience trade execution as an atomic exchange on-chain in milliseconds, with zero counterparty credit or settlement risk -- Payment-vs.-Payment.

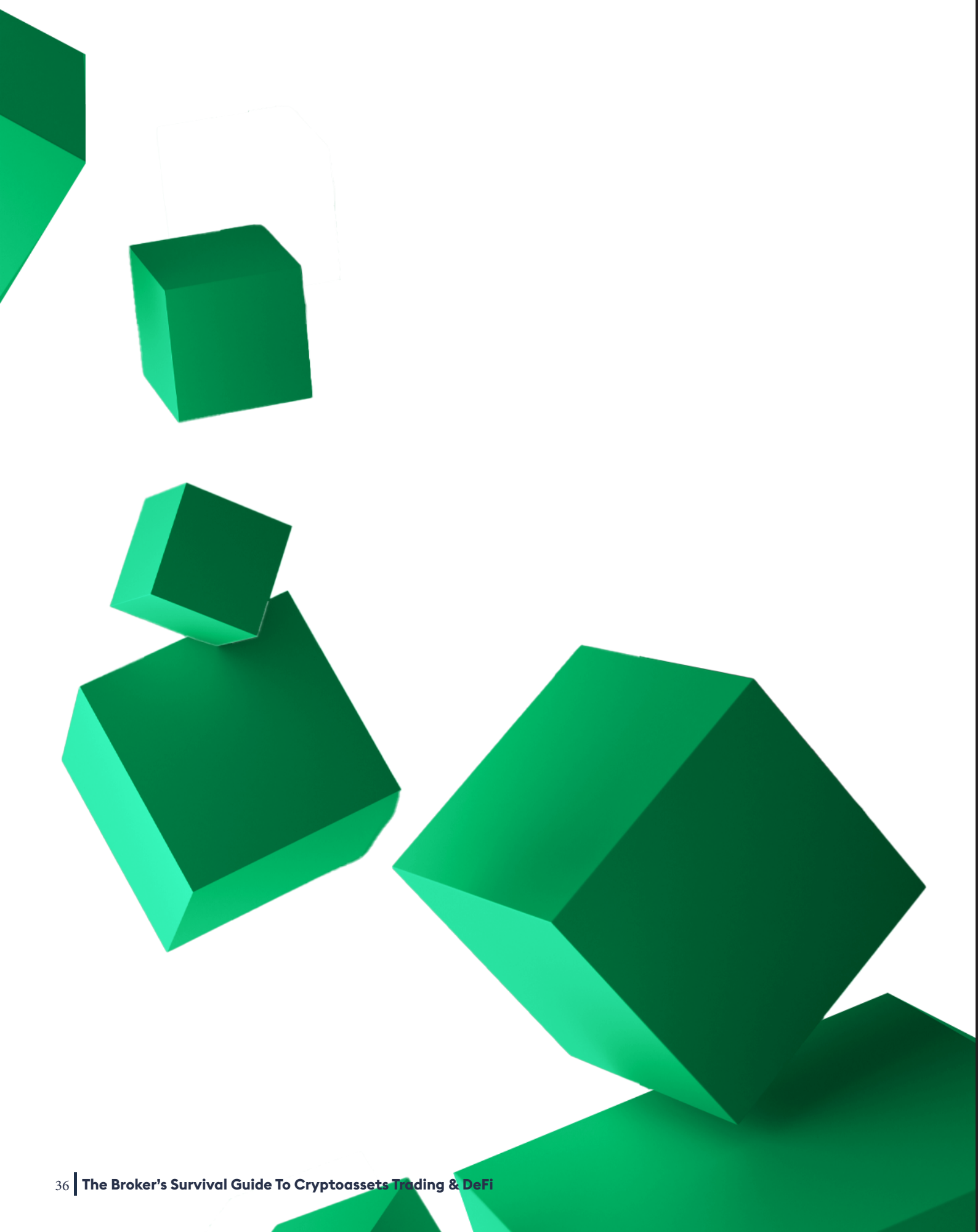
3. Automated Net Settlement Movements: continuous net settlement processed by custodians based on standing instructions from the clients and without any custodial balance sheet or credit risk, and without operating a clearinghouse.

4. Cross-Custodian Trading and Net Settlement: trade with counterparties at any other custodian with cross-margining, continuous netting, and custodian-to-custodian atomic net settlement on behalf of all trading counterparties.

5. Tradable Liquidity Aggregation: freedom to choose any counterparties for liquidity from retail and institutional exchanges, ECNs, market makers, OTC desks and brokerages, with a full range of trading platforms. White label capabilities for all trading needs including a lit CLOB exchange, dark pool, and liquidity aggregation with smart order routing, as well as an RFQ block trading solution.

6. Lending/Borrowing via Institutional DeFi: ability to aggregate unlimited third-party balance sheet through a lending marketplace where collateral stays in lender and borrower accounts at their own custodian(s). Margin and leverage financing are facilitated with repo transactions in real-time, executed as an atomic exchange on custodial Layer-2 blockchain ledgers.

7. Real-Time Payments: facilitates cash sweeps at the custodial blockchain level for multi-asset brokerage operations that need to support instant margin movements for clients 24x7.



Ready To Get Started

Interested in discussing how our high-performance wallet automation platform can help you optimise the speed, control and cost of your crypto asset operations?

Schedule a demo and intro call with us or choose how you'd like to talk to us.

bitpanda custody

Registered cryptoassets firm with the UK Financial Conduct Authority (FRN No.928556)

custody.bitpanda.com