

Cryptoasset Risk Mitigation Services

Specialized for infrastructure providers, institutions, family offices, and investors



Capabilities

Cryptocurrency Trading

introduces new, unique operational risk

	Traditional Trading Risk	Cryptocurrency Trading		New Risk
Customer Identity	Customer knowledge essential to meet service, suitability, and compliance needs	Parties can anonymously transfer value through the blockchain	➤	Violation of BSA/AML and regulatory compliance
Security	Online access limited to firm's own system	Access to the record requires public and private keys	➤	Vaults and wallets create crime, cyber and potential data theft risk
Network	Trading information contained within highly regulated systems (e.g., exchanges, DTCC & Bloomberg, etc.)	Trade details are broadcast to a distributed network*	➤	Trading information could be discernable even if data is secure (e.g., company positions)
Data	Trading mistakes can be removed from the books and replaced with corrected trade	The block is added to the chain creating an immutable** record	➤	A permanent record offers benefits and risks
Third Parties	Most trading is confirmed with a phone call from the back office	Unknown miners validate new blocks when created	➤	Business interruption by attack or sovereign intervention

* Distributed network could be public or private, permissioned or unpermissioned depending the specific blockchain implementation

** An immutable blockchain record can not be changed

Insurance “Links”

between cryptocurrency and traditional insurance markets

	Operational Risk Overview	Specific Cryptocurrency Operational Risk	“Links” to Traditional Insurance Markets
Custody	<ul style="list-style-type: none"> • Cryptocurrencies need to be custodied like traditional assets • However, they have unique technical qualities that require specific risk mitigations 	<p>Cold Storage Access keys can be stored on air-gapped devices, creating extremely high-value targets for theft</p> <p>Hot Storage Access keys stored online are easier to access and potentially easier to hack</p>	<ul style="list-style-type: none"> • Network security (i.e., cybersecurity) policies written with digital wallets in mind • Crime policies • Physical vaulting • Counterparty risk if cold storage is with a third party
Distributed Data	Blockchain-based assets are stored on broadly distributed ledgers	<ul style="list-style-type: none"> • Trading is reliant on nodes of distributed data that will likely be overseas and held by unknown parties • While making it difficult to corrupt data, it also makes an institution reliant on access to outside systems to operate 	Business interruption policies with an understanding of the blockchain
Mining (May be out of scope for this discussion)	Miners are individuals or companies that set up computers to calculate the cryptographic hashes and validate the ‘blocks’ of data	A proof-of-work (PoW) or proof-of-stake (PoS) system is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work or stake from the service requester, usually meaning processing time by a computer, or underlying value	<ul style="list-style-type: none"> • E&O and D&O • Reputational risk for involvement with cryptocurrencies viewed as supporting illicit activities

BlockRe Can Assist

with trading platform risk mitigation, compliance, and audit

BlockRe assists in providing full audit of crypto-related trading operations, risks, processes, procedures, reporting, and KYC/AML

Risk Mitigation	Compliance and Audit	Technology Support Platforms
<ul style="list-style-type: none">• Security Assessment• Insurance• Loss prevention• Threat Intelligence and Analysis• Asset tracking• Incident tracking	<ul style="list-style-type: none">• Regulatory Compliance, KYC/AML, and Legal Support• Ensuring clients have appropriate KYC/AML controls in place.• Reporting and Controls• Audits	<ul style="list-style-type: none">• Selection• Integration• Configuration• On boarding• Training• Support

Examples

BlockRe can provide an objective assessment of the potential risks and losses surrounding aspects of crypto trading – **providing level of protection against potential E&O lawsuits**

BlockRe can help develop a suitable AML program built for crypto compliance that could **prevent regulatory fines**

BlockRe can assist in selecting the best technology vendors and **securing suitable vendor insurance policies**



- Identify and mitigate any significant risks
- Provide security and assurance regarding risks or liabilities
- Enable rapid design of a cryptoasset insurance policy

Specific Ways to Engage BlockRe



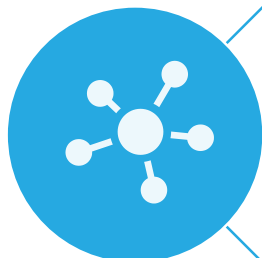
Risk Mitigation Professional Services

BlockRe can prepare a **thorough review of your current or proposed cryptocurrency custody processes** and a threat assessment of security weaknesses that can be addressed through risk mitigation



Insurance Coverage

BlockRe can **broker bespoke coverages** that address crime, cyber, E&O and D&O issues specific to cryptocurrency better than brokers unfamiliar with the new technologies



Technology Platforms

BlockRe can report and make specific **recommendations to your technology team** to reduce risks associated with the marketing and trading of cryptocurrencies

Contact Information

info@blockre.io

www.blockre.io

