Bakkt® Warehouse: Security First

Protecting our customers' assets securely is a foundational component of everything we do at Bakkt. Bakkt's digital asset infrastructure leverages enterprise security capabilities, including those that protect Intercontinental Exchange's dozen exchanges around the world, including the New York Stock Exchange. This is complemented by defenses that are needed for the unique requirements of digital asset safekeeping.

Foundational

The operational demands of the emerging digital asset industry, coupled with the unique risks and threats facing digitalasset holders, create a complex threat landscape that cannot be sufficiently addressed with legacy systems and defenses. Small mistakes, inconsistencies in processes, or organizational gaps can provide attackers the foothold they need to make headlines. The cornerstone of the Bakkt Warehouse is a zero-trust methodology that underpins the secure storage of digital assets.

Bakkt Warehouse

The Bakkt Warehouse is comprised of both online ("warm") and offline, air-gapped ("cold") digital asset storage. Bakkt systems algorithmically balance between both warm and cold storage tiers to minimize risks associated with warm storage. To further protect our customers, Bakkt's warm and cold wallets are covered by a $125,000,000 insurance policy from a leading global syndicate. This coverage will be reevaluated from time to time based on changing market conditions and updates to operational best practices. In addition, Bakkt is working with one of the largest custody banks in the world, BNY Mellon, as part of its safekeeping process.

WARM WALLETS

- Stores a small balance of bitcoin held in the Bakkt Warehouse
- Private keys are created and stored on FIPS 140–2 level 3 hardware security modules (HSMs) and no individual has access to private key material
- Network connected, but all withdrawal requests are received, verified, and processed by dedicated staff located in multiple geographies; requests are validated, both manually and systematically, against a policy ruleset that controls for parameters such as amount, destination, and velocity of transactions
- Additional anti-collusion and insider threat controls require multiple individuals from multiple teams in multiple locations be involved to process a transaction
- 24x7 on-site, armed security
- Advanced insider threat capabilities

COLD WALLETS

- The majority of bitcoin stored in the Bakkt Warehouse is offline
- Air-gapped systems stored in bank-grade vaults with sophisticated physical security controls
- Wallet keys are sharded and encrypted at creation, with multiple key shards needed to sign a single transaction
- Geographically distributed multi-signature transaction signing
- Segregation of duties between internal teams
- 24x7 on-site, armed security

bakkt™

Operational Security

All Bakkt operations start with a zero-trust, need-to-know approach, adding additional layers of security to minimize the impact potential of any risk. To preserve the security of key operations and personal security of staff members, Bakkt has implemented strict operational controls designed to prevent insider threat and staff collusion, erroneous destination wallet addresses, customer account spoofing, and numerous other scenarios. These controls include separation of duties with teams having different reporting lines, obfuscated key holder identities, strict social media guidelines, and geographically separated multi-signature operations.

Systems Security

Bakkt stores client private keys on hardened systems in cold storage and on FIPS 140-2 level 3 HSMs. Systems are sourced using approved procurement processes that address supply chain risk. Bakkt-developed applications and those procured from external vendors are required to support multifactor authentication and are centrally controlled by a global security team. All Bakkt managed devices (i.e. servers, laptops, network devices, mobile devices, etc.) have extensive security controls to prevent unauthorized access, limit authorized access, and safeguard against local and remote attacks. Regular penetration tests are conducted including external, internal, and physical evaluations of all operations facilities. For the continuous improvement of our security and operational processes, Bakkt proactively seeks input from vendors and law enforcement agencies.

Facility Security

All operations requiring access to encrypted cryptographic material or to similarly sensitive systems or processes are done within secure facilities that require staff members to authenticate using a combination of biometric, PIN, and proximity card. These facilities operate closed circuit 24x7 video monitoring, have 24x7 armed security, and intrusion detection, fire suppression and environmental control systems. Access to encrypted cryptographic material can only be accomplished in restricted areas by authorized staff members that require additional authentication protocols.

Disaster Recovery

At Bakkt, the protection and secure recoverability of private cryptographic keys, used to store digital assets, is a core competency. Bakkt has robust controls for Disaster Recovery (DR) and Business Continuity Planning (BCP) which help prepare for the restoration of normal services as quickly as possible in the event of a service outage due to unforeseen circumstances or a physical disaster. The Bakkt Warehouse operating system is fully supported in both the primary and backup datacenters and can operate independently from the location of ICE trading and clearing systems.