PLEASE SEE IMPORTANT INFORMATION AT THE END OF THIS WHITEPAPER

The Blockchain Terminal

Real-time Validation, Security and Compliance for Hedge Funds, Wealth Management and Cryptocurrency Trading

WHITEPAPER

Last Updated: April 27, 2018

The Blockchain Terminal ("Blockchain Terminal") offers proprietary access to a robust, customized ecosystem of institutional grade tools and services that leverage blockchain technology for the wealth management industry. The Blockchain Terminal is designed for use by hedge fund traders, analysts, portfolio managers and operations staff. The Blockchain Terminal is a creation of CG Blockchain, Inc. ("CG Blockchain"), a New York company that has been developing the Blockchain Terminal since 2016. With dedicated Blockchain Terminals users benefit from a robust layer of security and functionality for familiar tools, as well as new capabilities to advance investment management objectives.

The Blockchain Terminal technology solution includes ComplianceGuard—Blockchain Terminal's foundational application—and is powered by the proprietary Blockchain Terminal Ledger. A hybrid system that combines a private blockchain and a public, permissioned blockchain, the Blockchain Terminal Ledger retains the integrity of critical data and maintains essential confidentiality. Both the Blockchain Terminal and the token to be issued by BCT Inc (the "BCT Token") are anchored to the broader Ethereum blockchain, with its production-tested infrastructure that supports developer engagement with the Blockchain Terminal.

The BCT Token will provide access to all the features and tools of the Blockchain Terminal, and enhance the convenience of Blockchain Terminal devices. With the BCT Token, users can access applications and tools offered on the Blockchain Terminal Fundstore. The innovative use of blockchain technology gives Blockchain Terminal users the support of a compliance framework with an immutable ledger for all transactions, real-time compliance enforcement, and ad hoc audits. The Blockchain Terminal system delivers a new generation of best-of-breed applications and critical data for traditional transactions and for the rapidly emerging, complex, and often-chaotic cryptocurrency asset class.

Table of Contents

Disclaimer

This whitepaper does not constitute an offer to sell or a solicitation of an offer to purchase any securities of any nature whatsoever, nor do the contents of the document constitute legal, tax, or business advice.

Certain statements in this whitepaper constitute forward-looking statements, and are subject to change. When used in this whitepaper, the words “may,” “will,” “should,” “project,” “anticipate,” “believe,” “intend,” “expect,” “continue,” and similar expressions or the negatives thereof are generally intended to identify forward-looking statements. Such forward-looking statements, including the intended actions and performance objectives, involve known and unknown risks, uncertainties, and other important factors that could cause the actual results, performance, or achievements of the Blockchain Terminal to differ materially from any future results, performance, or achievements ex- pressed or implied by such forward-looking statements. No representation or warranty is made as to the Blockchain Terminal future performance by such forward-looking statements, and all such statements speak as of the date hereof, and are subject to change.

At times, the Blockchain Terminal Fundstore may offer certain materials (“Third Party Materials”) or provide links to certain third party websites (“Third Party Websites”). By using the Blockchain Terminal, users acknowledge and agree that BCT Inc and its affiliates are not responsible for examining or evaluating the content, accuracy, completeness, timeliness, validity, copyright compliance, legality, decency, quality, or any other aspect of such Third Party Materials or Third Party Websites. BCT Inc and its affiliates, their officers, affiliates, and subsidiaries do not warrant or endorse and do not assume and will not have any liability or responsibility to you or any other person for the provision of any Blockchain Terminal services, Third Party Materials, Third Party Websites, or for any other materials, products, or services of third parties. Third Party Materials and links to Third Party Websites are provided solely as a convenience to the end user.

Glossary of Terms and Names

- **Application Programming Interface (API) –** A set of clearly defined methods of communication between various software components.
- **BCT Inc** – A Cayman Islands exempted company that will hold intellectual property associated with the Blockchain Terminal and issue the BCT Tokens.
- **Blockchain Terminal Fundstore** – An application store built for distributing best-of-class software, it is a source for subscriptions, tools, and services to customize the work environment on the Blockchain Terminal.
- **Blockchain Terminal Ledger** – A proprietary system that utilizes both a private ledger and a public, permission ledger to provide a hybrid, decentralized, immutable ledger that enables the Blockchain Terminal.
- **BCT Token** – An ERC20-compliant subscription token issued by BCT Inc and used to access Blockchain Terminal services. Access to the ERC20 compliant BCT Token is bound by the Terms and Conditions Relating to BCT Token Distribution, a copy of which will be available during the BCT Token sale.
- **Blockchain Terminal** – A device with proprietary access to a robust ecosystem of customized tools and services, the Blockchain Terminal enhances capabilities for wealth management professionals with respect to traditional and cryptocurrency assets, and integrates with existing software and data sources. Access to the Blockchain Terminal is governed by its End User License Agreement, a copy of which will be distributed with the Blockchain Terminal.
- **Blockchain Terminal Framework and API –** Public documented libraries and an application/programming interface that provide core tools for developers working and interacting with the Blockchain Terminal.
- **CG Blockchain** – A New York-based technology development company. Creator of ComplianceGuard, a central application on the Blockchain Terminal.
- **Chief Compliance Officer (CCO) –** The individual responsible for overseeing and managing regulatory compliance issues for an organization.

- **ComplianceGuard** – A cornerstone application of the Blockchain Terminal, designed to allow CCOs to record logbooks onto a private, time-stamped blockchain, creating an immutable record of all events and data.

- **Cryptocurrency** – Digital asset and medium of exchange that uses both distributed consensus and cryptography to secure transactions and control the creation of additional units.

- **Domain Name System (DNS)** – A hierarchical, decentralized naming system for computers, services, or resources connected to the Internet or to a private network. It translates common, easily remembered domain names to their numerical IP addresses, which are needed for locating and identifying computer services and devices with the underlying network protocols.

- **Hash** – A one-way cryptographic function that encodes data into a small packet that cannot be inverted or recreated.

- **Merkle tree, Merkle root, etc** – A hash tree in which every "leaf" node is labeled with a hash of a data block, and every non-leaf node is labeled with the hash of the labels of its child nodes. Named for the inventor, Ralph Merkle (Merkle [1980]).

- **NSlookup** – A program that lets an Internet server administrator or user enter a host name (e.g., "whatis.com") and find a numeric IP address.

- **Order Management System/Execution Management System (OMS/EMS) -** Systems focused on facilitating and managing the order execution of securities, as well as managing internal order flow and/or routing orders.

- **Practical Byzantine Fault Tolerance** – The term is derived from the Byzantine Generals' Problem where actors must agree on a concerted strategy to avoid catastrophic system failure, but some of the actors are unreliable.

- **Proof of Authority (PoA)** – The right to validate based on reputation so that, once earned, there is high incentive to retain a reliable reputation in the system.

- **Proof of Existence (PoE)** – This protocol inserts a cryptographic signature of data, typically a one-way-function using a standard algorithm like SHA256, into the blockchain as evidence of the data being stored.

- **Proof of Stake (PoS)** – A consensus mechanism alternative to PoW, which trusts input based on the stake the creator owns in the system. While it would save energy used for processing, the balance of incentives can become unstable.

- **Proof of Work (PoW)** – A proof that is difficult (costly and time-consuming) to produce but easy for others to verify. PoW uses a great deal of computing capacity, which increases the cost and the environmental footprint.

- **Redundant Array of Independent Disks (RAID)** – A data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.

- **Reference Implementation** – The standard from which all other implementations and corresponding customizations are derived.

- **SNMPv3** – Simple network management protocol for collecting and organizing information about managed devices on networks and for modifying that information to change device behavior; now at version 3.

- **Sandbox** – A testing environment that isolates untested code changes and outright experimentation from the production environment or repository. Only after the developer has fully tested the code changes in a sandbox should the changes be merged with the repository and thereby made available to other developers or end users of the software.

- **Service Level Agreement (SLA)** – a contract between a service provider and end user that defines the level of service expected from the service provider and specifically defines what the customer will receive.

- **Smart contract** – A computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of an agreement. Smart contracts assure the performance of credible transactions without third parties. These transactions are both trackable and irreversible.

- **Token** – A cryptographically verifiable entitlement to digital resources that can be exchanged for products or services.

- **Turing Completeness** – A system is Turing complete if a program can be written within it that will find an answer to a given problem, irrespective of runtime or memory use. Traditionally a system is called Turing complete, or computationally universal, if it can be used to simulate any single-taped Turing machine andif, given enough tape, a Turing machine could compute any program.

1. Introduction: The Motivation

The financial crash of 2008 and frequent cases of fraud within investment management industries have made high finance and alternative asset classes top headlines. After constant news describing massive frauds from Madoff to the recent USD 1 billion breach of the Punjab National Bank in Mumbai, investors are demanding that their assets be managed with a much greater level of security and that all transactions be attestable. Regulators are also demanding greater levels of compliance and consumer protection that adds complexity to routine transactions and requires stepping beyond the status quo to raise capital.

Blockchain appeared in the wake of the financial crisis as the underlying technology to enable "a peer-to-peer electronic cash system" (Nakamoto [2008]) in the form of cryptocurrencies, like Bitcoin and Ether. While cryptocurrencies dominated the news, the breakthrough distributed ledger technology of blockchain has emerged as the innovation that could upend business models and open a new era of transparency and decentralization for a wide range of industries including investment management. With an ingenious combination of cryptography and mathematics, transactions can be verified, cleared, and stored in a blockchain that provides an immutable audit trail.

Investment managers, especially those focussed on hedge funds and alternative investments, are constrained by investor mandates. The execution of their fiduciary responsibilities in compliance with these mandates is opaque and difficult to track. This makes adherence to constraints and proper handling of exceptions difficult to demonstrate. Moreover, even when compliance is demonstrated, the attestation requirements of accountants, auditors, counterparties, partners and investors are burdensome and inconsistent. A solution is the Blockchain Terminal with embedded compliance solutions. The Blockchain Terminal leverages the power of blockchain technology in order to bring the security, assurance, transparency, and immutable trust demanded by wealth managers and the operators of hedge funds.

2. The Blockchain Terminal Solution

The Blockchain Terminal leverages blockchain technology to bring the security, assurance and immutable trust demanded by the hedge fund and wealth management industry to cryptocurrency investing. The central distinguishing feature of the Blockchain Terminal is a hybrid ledger that integrates both private and public permissioned blockchains. This ledger is anchored to the broader Ethereum blockchain through the use of Blockchain Terminal applications, modular productivity tools and services supported by the Blockchain Terminal. Application developers using the Blockchain Terminal have easy access to production tested infrastructure with embedded compliance functionality.

BCT Incintends to issue the ERC20 compliant BCT Token to be utilized on the Blockchain Terminal. The BCT Token will be used on the Blockchain Terminal to subscribe to services, or to otherwise license or purchase applications, on the Blockchain Terminal.

It is intended that CG Blockchain will transfer to BCT Inc all of the intellectual property associated with the Blockchain Terminal, other than the intellectual property associated with the ComplianceGuard application discussed below. It is also intended that BCT Inc will use proceeds from its sale of the BCT Tokens to fund the further development of the Blockchain Terminal and applications to be available on the Blockchain Terminal, through development agreements with affiliates of BCT Inc, including CG Blockchain, HF Blockchain Inc. ("HF Blockchain") and Optimumm Inc ("Optimumm"). HF Blockchain is a New York based company that is also an affiliate of CG Blockchain and Optimumm. Optimumm is an affiliate of CG Blockchain and HF Blockchain based in Saint Vincent and the Grenadines. It is further intended that BCT Inc will enter into a service agreement with an affiliate to operate and service the Blockchain Terminal.

2.1 BCT Components

The ComplianceGuard software application being developed by CG Blockchain and intended to be included on the Blockchain Terminal will be designed to securely journal compliance entries for hedge fund and asset manager CCOs. Once integrated into a firm's network, the Blockchain Terminal connects the firm to a private ledger that improves the overall integrity of critical data through consensus. Data that supports compliance is immutably stored on the private ledger during the normal course of business and can be retrieved and audited as needed. This journaled data interacts with the global Blockchain Terminalpermissioned ledger to provide an external anchor for internal activity that can be observed and verified by external constituents. This provides near real-time verification of adherence to compliance mandates. Auditors and regulators can verify the data without compromising confidentiality.

CG Blockchain believes that the ComplianceGuard application will reduce compliance burdens. It is built to serve different users including CCOs, investment analysts, operations personnel, portfolio managers, traders and external auditors. ComplianceGuard is the cornerstone application and reference architecture for development on the Blockchain Terminal. ComplianceGuard is being designed to provide an immutable ledger that supports compliance related services on the Blockchain Terminal and to provide an improved level of attestation for transactional activities performed by an asset management firm using the Blockchain Terminal. For more information about ComplianceGuard see Section 5 below.

The core features and benefits of the Blockchain Terminal and applications intended to be a part of the Blockchain Terminal include:

- **Immutable data for universal standardized audits** – When accessed through the Blockchain Terminal, all transactions will be timestamped onto the immutable distributed ledger. Notes and documentation are recorded in a secure and tamperproof environment. Review can be real-time and potentially problematic activities may be highlighted.

- **Robust tooling** – A simple interface allows for identifying and selecting from a catalog of carefully curated applications that support a broad range of front, middle and back office investment lifecycle activities. Applications are built in conjunction with the

ComplianceGuard framework and should be designed to meet standards for completeness, ease-of-use, secure operation and user support.

- **Native support for cryptocurrency as an asset class** – Professional tools and information sources help to connect the traditional hedge fund industry with the rapidly expanding investment opportunities in the cryptocurrency space.

- **Support for third party application development** – Blockchain Terminal developers and established software vendors benefit from a productive, advanced and effective environment. The open distribution channel provided by the Blockchain Terminal can reach existing and new users with tools to address both traditional and cryptocurrency assets while operating in the ComplianceGuard environment.

2.2. Design Principles

The Blockchain Terminal is being developed to conform to the following guiding principles and requirements:

- **Security** – Confidentiality, integrity and availability of constituent data will guide the development. Information storage will be designed to ensure confidentiality and consistency and provide for ease of access and audit. Data should be validated and verified according to established standards and within the context of a legitimate purpose of use. Applications and data stored by the platform should accommodate business continuity and disaster recovery planning.

- **Identity** – Strong authentication and authorization for provisioned resources will guide the development. Flexible credential management will allow roles and permissions for asset managers to have natural extension and mapping to supported roles of Blockchain Terminal applications. Credentials, authentication and authorization decisions are not intended to be available on an open basis. They will only be recognized and enforced at the individual firm level where credentials are established.

- **Integration** – Blockchain Terminal applications are not expected to run in isolation. Using the Blockchain Terminal, it will be possible for firms to integrate enterprise data, including reports and feeds from third party systems. Such integration is expected to be supported through a set of interfaces ("API") made available from time to time through the Blockchain Terminal that will provide near real-time data access and subsequent analysis. Blockchain Terminal applications should be adaptable to enterprise infrastructure and a central administrator should be able to identify and assign enterprise user directories, storage and data stores, allowing firms, through the Blockchain Terminal, to leverage Blockchain Terminal applications on existing infrastructure and platform investments that support robust service level agreements.

Open Community and Open Source – CG Blockchain and its affiliates are committed to the development of best-of-breed applications and promotion of the technologies and techniques that make the Blockchain Terminal possible. CG Blockchain and its affiliates expect to actively work with and promote open source blockchain architectures as legitimate, decentralized alternatives for users of the Blockchain Terminal. The BCT Token will be used to access the Blockchain Terminal as well as various applications made available to Blockchain Terminal subscribers. The Blockchain Terminal intends to also provide an open channel for the use of other blockchain cryptographic tokens on the third party applications hosted on the Blockchain Terminal where and whenever possible.

Blockchain Terminal development is intended to be community driven and the ComplianceGuard application's core elements are intended to be open source. Whenever possible, subsequent core developments will also be open source. CG Blockchain and the other BCT Inc affiliates involved in the development of the Blockchain Terminal intend to use and promote open source software and open communication channels for input. Whenever possible, CG Blockchain (and the other entities involved in development) will encourage Blockchain Terminal vendors and developers to do the same.

The Blockchain Terminal provides a mechanism for implementing cryptocurrency strategies and legitimizing hedge fund and other asset manager operations. For asset managers pursuing cryptocurrency as an asset class, it is critically important to employ an advanced class of tools for legitimizing and providing transparency to operations. Firms that seek to maximize returns from participation in this new investment opportunity presently receive little institutional support for struggling with a patchwork of vendors, technology solutions and manual processes. For example, calculating unrealized gains is a challenge because exchange liquidity is not uniform across all assets, thus creating large price discrepencies. Similarly, data taken across exchanges may not represent all required information. In this challenging environment enhancing existing systems with powerful new tools becomes even more important for an asset manager and its investors.

3. The Blockchain Terminal Ledger

a. Problems with the *Status Quo*

The introduction of Bitcoin (Nakamoto [2008]) and the subsequent rise of blockchain distributed ledger architecture created a revolution of digital asset ownership and multiparty trust. Cryptocurrency users and exchanges secure transactions using distributed ledgers, effectively replacing the model of trusted central authorities with decentralized networks of unknown actors who can nevertheless be trusted to validate transactions using consensus algorithms-based on cryptographic proofs.

In spite of the increasing viability of distributed ledger approaches, global capital markets, hedge funds, traders and asset managers typically continue to rely on traditional audit procedures to provide confidence among stakeholders and regulators. The Blockchain Terminal ledger approach provides a mechanism for any permissioned party with access to private fund or investment transaction data to attest to the legitimacy of the data with certainty and reasoned authority.

The immutable records created in blockchain-based systems streamline data verification and transactions and can be assured by comparing derived hashes within the blockchain ledger. The blockchains can be implemented in a number of ways, requiring either public or private consensus. Private, permissioned blockchains are commonly used to establish trust in business-to-business relationships. R3 Corda[1] and the Hyperledger Project[2] are recent examples of enterprise blockchain implementations that employ private, permissioned chains. Global accounting firms, including Deloitte[3], PwC[4], KPMG[5] and EY[6], have identified the utility of using blockchain-based notary services that have the potential to enable timely and fully automated financial audits that are seamless, error-free and tamper-proof.

In the hedge fund and asset management environment, managers require security for the most sensitive data (such as accounts, balances and positions). However, many permissioned ledger implementations do not use consensus mechanisms. They are unable to resolve the fundamental issue of trust without assistance from a third party.[7]

Because they require secure identity services, existing systems are only as secure and valuable as their participants. Controlling access, especially for a global ledger, can require extensive identity management and overhead cost in order to credential parties both within and outside a firm. Roles and permissions are difficult to add after a smart contract has been created to govern blockchain activity, and private keys are bound to a user wallet. The addition of new users raises concerns about appropriate access to legacy data, while removing users must assure that access to blockchain data has been restricted. Given the circulation of employees among financial enterprises, a past employee with credentials to a global permissioned ledger might see an opportunity to use those credentials in a different venue.

b. Elements

The Blockchain Terminal Ledger is comprised of two separate but related blockchain ledgers:

1. A private local ledger supporting the storage of sensitive data hosted within a firm; and

2. A private global ledger where the aggregated hashes of each constituent firm's private ledger data are posted at fixed intervals.[8]

[1] Hearn, 2016.
[2] Cachin, 2016.
[3] Andersen, 2016.
[4] Diemers and Koster, 2016.
[5] Brown, 2017.
[6] Crawford and Meadows, 2017.
[7] In the most robust implementations, permissioned ledgers achieve consensus using the Practical Byzantine Fault Tolerance algorithm (Castro et al, 1999) or a Proof of Authority consensus, where principal actors vote on data validity.
[8] Note that the private global ledger is not the public Ethereum network, but an additional component.

This model of interaction follows a common practice for anchoring the mechanism of two chains using the mechanism called 'Proof of Existence."[9] This approach allows information stored to the Blockchain Terminal Ledger to be private but also externally auditable. The Blockchain Terminal Ledger will be designed to capture activities that support the alert and audit functions that hedge funds and other asset managers require for conformance to the mandates of regulatory and internal authorities.

The Blockchain Terminal will be designed to assure near total privacy using the global ledger in conjunction with a hedge fund's own private ledger. Because the privacy of the global ledger is never fully assumed, mechanisms used for storing data on the global ledger make extensive use of zero knowledge proofs in cases where journaled entries could be readily identifiable.[10] A blockchain notary service secured by the Ethereum network provides auditability support. In this way, the proprietary Blockchain Terminal dual ledger approach is tethered to a public source of distributed trust that both maintains confidentiality and security and provides transparency.

As a third layer of attestation, the Blockchain Terminal Ledger's global blockchain will be anchored to the public Ethereum blockchain to provide for added security, consistency and integrity. This process is explained with detail in "Attestation to the Ethereum Blockchain" section below.

c. Blockchain Terminal Ledger

Both the private ledger hosted by a firm and the permissioned global ledger will be implemented using Ethereum compatible technology which supports over US$98 billion[11] in value. This will provide native support for smart contracts and tokens that meet the ERC 20 token standard that is commonly used across a multitude of Ethereum public blockchain projects.. This established blockchain technology opens access to a robust community of supporters and developers who readily understand the transformative nature of the technology and the opportunity to migrate to a proprietary blockchain enabled by the BCT Token. In the meantime, bringing an open Ethereum-anchored blockchain to the hedge fund and asset management industry will provide both Blockchain Terminal users and the broader cryptocurrency community a decentralized ledger technology with a vibrant platform for the development of powerful and innovative applications.

i. Transaction Capture and Synchronization

The Blockchain Terminal private ledger will be hosted on-site as an isolated node or closed network of Blockchain Terminals operating on a firm's own network. It will be integrated into the existing OMS/EMS of the firm for the purpose of performing transaction and event capture.

[9] Araoz, 2013.
[10] Green, 2014 and Green, 2017.
[11] Cryptocurrency Market Capitalizations, see (https://www.coindesk.com/ethereum-price/), (https://coinmarketcap.com/) and (https://coinmarketcap.com), accessed Jan. 19, 2018.

The open specifications of the Blockchain Terminal Ledger allows integrators and developers to customize solutions for a firm's specific requirements. As transactions and events, including compliance alerts, are generated, representations of these structures are sent as messages to a subscribing queue. A listener to that queue is tasked with hashing all transactions and events within a fixed time interval and forwarding the data to the global Blockchain Terminal private ledger together with associated hashes. These hashes are in effect branches of a Merkle tree, whose Merkle root can sufficiently represent all data received over that scheduled interval to the Blockchain Terminal private ledger for processing.

The approach appends Merkle roots of associated transactions to the private ledger component, providing for flexibility in dealing with common variances in transaction and event volumes. In this way, the Blockchain Terminal private ledger will avoid issues of block formation and consensus overhead when dealing with high frequency transactions, acting on as many transactions within a minute as some other strategies may generate over the course of a day or longer.

Through the Blockchain Terminal a queue in a firm's internal network that processes transactions and generates events, will continuously attempt to publish journaled hashes to the Blockchain Terminal private ledger. Regular timing intervals will be established using negative acknowledgement ("NAK") messages to both the private and global ledgers should no transaction data appear within a scheduled journal window. Journaling a hash of an NAK message to the private or global ledger is an implicit mechanism for demonstrating that the publication mechanism is running consistently, even if transactions and events are not being generated by a firm's investment or operations activities. This regular timing interval commits a hash to the Blockchain Terminal private ledger and, subsequently, to the global ledger. The queue is critical to reconciling transactional integrity for a given period and eliminates the need for pulling transactions and events from outside the immediate window of interest to perform a reconstruction of hashes being used for validation.

The Blockchain Terminal global ledger uses a closed process of collecting transaction and event hashes from each Blockchain Terminal private ledger. This critical component does not require active inbound queuing, as throttling to the block creation and consensus latency are already accommodated by integration within each firm's own transaction environment. Scheduling and NAK messages are still used heavily in the journaling of private blockchain activity to the global ledger to allow for ease of correlation between observed blockchain hash entries and the private blockchain hashes from which they are derived.

ii. <u>Conceptual Network Architecture</u>

Figure 1 below provides a conceptual view of the current construct of the Blockchain Terminal network architecture. Each participating firm will establish a virtual private network ("VPN") connection to the Blockchain Terminal operating network. The connection to Blockchain Terminal global ledger nodes restricts network visibility allowing a firm's internal network to see only the global ledger node instance responsible for its journal activity.

Blockchain Terminal users will initially be provided a core suite of global ledger services; however, as the pool of interest increases with the expansion of the Blockchain Terminal architecture and network, other authorities, including regulators, auditors and prime brokers may all be potential candidates to serve as global ledger nodes.

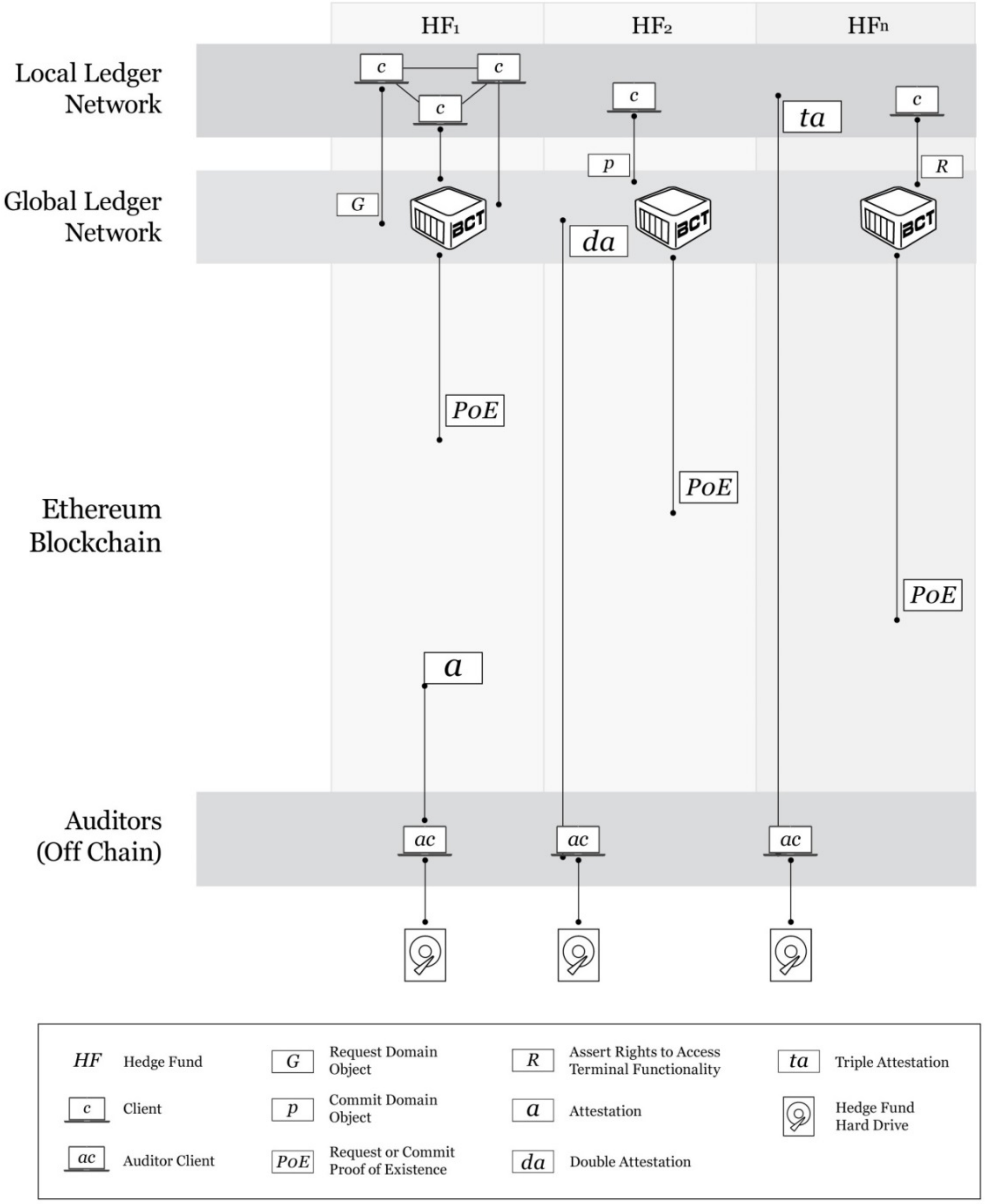


Figure 1: Conceptual Blockchain Terminal Ledger Network Architecture. Source, CG Blockchain, 2018.

d. Features

The Blockchain Terminal ledger architecture will be intended to have three component features leveraged across both private and global execution contexts:

1. **An identity-based authentication and authorization framework** – this will bind enterprise-validated identities from a directory service to roles and permissions saved on the blockchain.

2. **A registration service** – this will represent canonical data models and ontological structures against those models, which are used to support both application integration through a standard message bus and the application of deterministic or non-deterministic logic.

3. **A native programming model** – for the constraining behaviors associated with relationships established on the blockchain, which, in the case of Blockchain Terminal implementation (using an Ethereum blockchain), is provided by the popular Solidity smart contract programming language.

i. Identity-Based Authentication and Authorization

While public, permission-less blockchains work without need for user identity, the Blockchain Terminal will operate using a role-based identity service that is assured by an established web-root of trust in order to create a layer of transaction accountability. Within the Blockchain Terminal private and global chain architectures there will only be two types of identity that require management: BCT Inc (or an affiliate), as the identity providing governance over the global ledger and each individual firm using the Blockchain Terminal, in providing authority over the governance of its own private blockchain.

Each Blockchain Terminal that is connected within a firm’s internal network will generate a local key pair. If only a single Blockchain Terminal is running locally, transactions will be journaled between the private and public key of the same key-pair. All Blockchain Terminal related transactions on a local network will be trusted using the same web-root of authority for that firm’s implementation and the local peer-to-peer ledger network will be secured using standard public key encrypted protocols that permit for peer-to-peer connections.

All user identity functions will be relegated to Blockchain Terminal applications, which through use of the Blockchain Terminal Framework and APIs, will be federated back to a firm’s own identity management infrastructure (e.g., Active Directory, OpenLDAP, etc.) or a locally provided implementation of a lightweight directory access protocol (LDAP) server implemented on the Blockchain Terminal local server installed at the firm. Blockchain Terminal users will not have broader blockchain identities that exist outside the scope of the firm itself. It is expected that a local system administrator or the CCO within a firm will manage registrations.[12] All transaction activities performed in the scope of a Blockchain Terminal subscriber account will be journaled through the interface of the supported Blockchain Terminal application. This

[12] If users anticipate engagement with environments where OFAC/AML considerations weigh heavily, the diligence for registration protocols will fall to the individual application providers in conjunction with those parties seeking subscription. The Blockchain Terminal is not envisioned as a counter-party, custodian, facilitator or beneficiary of any transaction on its system.

allows reasonable separation of the Blockchain Terminal (in its role as a journaling node on the firm's local network) and the identity of a user who may be logging into a specific service provided by the Blockchain Terminal.

A firm's local web-root of trust certificate will be propagated to the Blockchain Terminal global ledger environment to authenticate a firm-based network node attempting to journal an interaction with the global Blockchain Terminal Ledger.

Applications will be encouraged to use the Blockchain Terminal Framework provisioning policies to ensure that enterprise roles and permissions can continue to be audited centrally by a firm's systems administrator. The provisioning policies are anticipated to be developed in the future. To the extent that an application allows for a global identity enrollment using a third-party verification service, the Blockchain Terminal Framework will have the ability to disable these mechanisms to ensure strict compliance with electronic device usage policies that a firm may have in place.

ii. Registration of Canonical Structures and Ontologies

A Blockchain Terminal user or vendor may register canonical structures and ontologies against the Blockchain Terminal private ledger. Vendors may also register to the global ledger to support integration and interactions with applications. This will occur in the context of a notary service in which BCT Tokens can be used to submit data as a permanent anchor to the target ledger.

Traditional transaction activity is built upon regulatory standards. In the same way, the Blockchain Terminal encourages the introduction and reuse of various common domain objects and behaviors that can be stored, serialized and parsed. These objects include standard categories: accounts, securities, strategies, locations (custodians), positions, orders, transactions, balances and prices. Concepts from FIXML[13] and FpML[14] can be similarly adapted to registration on the Blockchain Terminal.

The Blockchain Terminal Framework and API will provide a simple standard for applications designed to address and store domain objects. Each object will form a collection that persists to the Blockchain Terminal private ledger so that it may be referenced by applications that utilize the data. An administrator can easily audit data and quickly set references to individual collection entries as being invalid if necessary. Integrated processes may add to collections, but cannot modify existing data; and the collections are immutable. The Blockchain Terminal Ledger will offer Turing Completeness by executing smart contracts and embedding the
m in transactions (i.e., interactions) that occur within a firm (in the case of a private ledger), or between the firm and the Blockchain Terminal. The Blockchain Terminal private ledger will also guarantee that only objects that are built to an accepted standard, as referenced in

[13] CME-Group, 2017.
[14] FpML, 2015.

registered domain models and supporting ontologies, can be used in applications and shared in application-supported integration.

The collections may potentially in the future be used in many ways.

Security master validation:

- A collection of firm-traded securities built from a user’s source system of record as a trading security master includes:

- An application that performs trade capture audits.

- Automatic validation of trades processed through applications on the Blockchain Terminal and API, for ensuring integrity against user’s known security master.

- CCO notifications will be triggered should a trade address a security that was not previously traded. This will validate its specific trading guidance for industry, geographic, custody and specific concentration.

- Option for CCOs to auto-add new securities to transaction logs or suspend integrated feed, pending review.

Price validation:

- A collection of prices is kept for each firm security in the security master collection.

- A Blockchain Terminal application can perform retrospective profit-and-loss over a given strategy, by retrieving price as of a given date.

- CCOs can receive an alert when a price for a specific date does not exist.

- CCOs can receives alerts when a price exists and the price has not changed for a specified interval of consecutive days.

- CCOs can ask an operations analyst to provide a reason for the price discrepancy. A new as-of price can be added to the security’s price collection. All applications using the price collection would be automatically updated.

Balance reconciliation:

- A collection of balances of securities for each user strategy will be available through the Blockchain Terminal.

- Reconciliation on a morning-by-morning basis will be available to ensure positions in custody match stated positions/balances for an account.

- Trade breaks can be recorded prior to reconciliation.

- Reconciliation resolutions can be journaled and maintained adjacent to repaired position data.

- Applications using the data API can be updated.

iii. Native Programming Model

A native programming model runs a collection of smart contracts on the underlying network of the Blockchain Terminal private and global blockchains. The smart contracts operate through the use of BCT Tokens. The Blockchain Terminal reference system will have two contract operations available that write a hash to the public Ethereum blockchain via the Blockchain Terminal private ledger:

- **Object enrollment** – A one-time process that proves the structure of a domain object or ontology on a network. This includes real-world validation of domain objects and ontologies and saving associated component references to the Ethereum blockchain operating as a global ledger through BCT Tokens.

- **Request for notary record** – A catch-all operation used to create a verifiable timestamp of data entry. This is executed by submitting a hash of the data and a timeout for other parties to sign it.The Blockchain Terminal will then notify the appropriate parties.

Similarly, the Blockchain Terminal Reference Implementation (the standard from which all other implementations and corresponding customizations are derived) only offers two operations to read data from the Blockchain Terminal ledger:

- **Verify object** – A verification algorithm that checks the validity of the domain object and ontology registration records on the Ethereum blockchain. The Blockchain Terminal will address queries on both the private or global ledgers as the verification request searches for and returns matching object enrollment records.

- **Search notary data** – The Blockchain Terminal will search for the hash of notarized data from a valid role. Users can ensure information has not been altered as of the moment it was notarized.

These operations are foundational and can be called for by executing transactions with BCT Tokens sent to either components of the Blockchain Terminal. They are the basic building blocks. The complete Blockchain Terminal is expected to permit the message-based integration and validation of transactional data that is fundamental to the architecture of the Blockchain Terminal.

Incentives to write applications that use the Blockchain Terminal will include integrated subscriptions accessible through Blockchain Terminal to products and services provided by CG

Blockchain and other third parties. It is anticipated that the Blockchain Terminal private and global ledgers will be open and accessible to developers for the performance of direct interactions using BCT Tokens to support smart contracts.

e. Consensus

The Blockchain Terminal will be operated through two mechanisms of consensus: Proof of Authority[15] and Proof of Work.

1. Proof of Authority ("PoA")

A mechanism common in enterprise blockchain implementations, PoA does not require nodes to solve arbitrarily difficult problems or to prove veracity in appending transactions. Instead, it is given permission ("authority") to make these additions. The private chains implemented by the Blockchain Terminal and created by nodes installed through a Blockchain Terminal at the location of each firm, will, employ PoA. At present, the Blockchain Terminal's global ledger will also use a PoA approach.[16]

2. Proof of Work ("PoW")

The PoW mechanism by which the public Ethereum blockchain achieves consensus is work intensive by design. The transition to a Proof of Stake ("PoS") authority-based on tokens held will reduce intense power requirements of PoW-based networks. The Ethereum network nodes are responsible for competing to generate the solutions to cryptographic based challenges that earn tokens for appending data onto blocks and onto the Ethereum distributed-ledger.

Differentiation between PoA, PoW, and Proof of Stake (PoS) on the Blockchain Terminal Ledger PoA is a consensus mechanism based on identity as a stake. Unlike PoW and PoS, in which stake is based on monetary value, PoA uses the participant's identity to validate transactions using official documentation. This will be the only true identity per participant.

Consensus in PoA is reached by referring to a list of independent validators, which are nodes in the global ledger network. For a new node to be added it must be signed off by a pre-approved and pre-existing group of authority nodes. This group is formed by independent validators who are selected after they obtain an active notary public license within the United States, prove zero criminal record, display strong moral standing and comply with additional requirements. PoA limits the amount of damage a malicious actor may cause, minimizes opportunity for collusion, and allows control over which of the authority nodes can mint blocks on a private network.

Control and security of the network are improved using PoA rather than PoW and PoS. PoA is also resistant to so-called "51% Attacks" (in which a group of miners acquires "51% of a

[15] Czaban, 2017.

[16] As the number of participants in the Blockchain Terminal ecosystem increase to include other stakeholders with interest in the data of the public ledger, the distribution of this ledger may transition to another consensus mechanism, such as Proof of Work or Proof of Stake.

network's computing power). In PoS, an algorithm grants participants with the highest monetary stake authority to validate the blocks, whereas PoA validators are incentivized to act in the best interest of the network because their identity is public. PoA is therefore more reliable for maintaining a private network and ensuring that the block issuers remain accountable.

f. Attestation to the Ethereum Blockchain

The Blockchain Terminal will bridge the multiple layers of blockchain self-attestation to the broader immutability of the public Ethereum network. At scheduled intervals, a PoE client process from the operating nodes that supervise the construction of the Blockchain Terminal private ledger (and do not append transactions) will submit a Merkle root to the Ethereum network for all transactions against the Blockchain Terminal global ledger occurring within the timeframe.

The PoE hash can be identified and used for verification of the internal consistency of the Blockchain Terminal global ledger for the period. An outside observer could identify the transaction written to the Ethereum ledger and use that Merkle root for verification of the internal consistency of the Blockchain Terminal global ledger for the corresponding period.

g. Development

The Blockchain Terminal application development environment will be available for permissioned user access and will provide users access to a sandbox environment in which to upload code, manage supporting components and configuration, package applications for consideration and provide supporting information for marketing and price. Developers who are satisfied with the execution of their code in their local development environment may package and share applications with Blockchain Terminal systems on their local network.

The Blockchain Terminal staff will identify preferred integration and development partners that can assist, augment, or develop on behalf of interested parties. The Blockchain Terminal team intends to actively support the Blockchain Terminal development community.

It is anticipated that the Blockchain Terminal staff will support the open Blockchain Terminal community process for capturing, sharing, vetting, prioritizing and performing platform improvements that will contribute to the ongoing evolution of Blockchain Terminal as a platform. Every new application deployed provides an opportunity to engage and understand the value of shared features that will support the users, extend to new applications and markets and be helpful for the developer community as a whole.

4. Blockchain Terminal Fundstore

The Blockchain Terminal will offer a standardized storefront for application developers and third party vendors on which to publish and distribute user applications. Hedge fund users will have access to third party institutional-grade data and execution for cryptocurrency trading. The curated collection of applications can be acquired using BCT Tokens.

In addition to compliance functions, the features and functionality of the Blockchain Terminal is intended to be designed to enable broad interaction with a number of standard hedge fund information flows and decision-making processes, as shown in Figure 2 below.

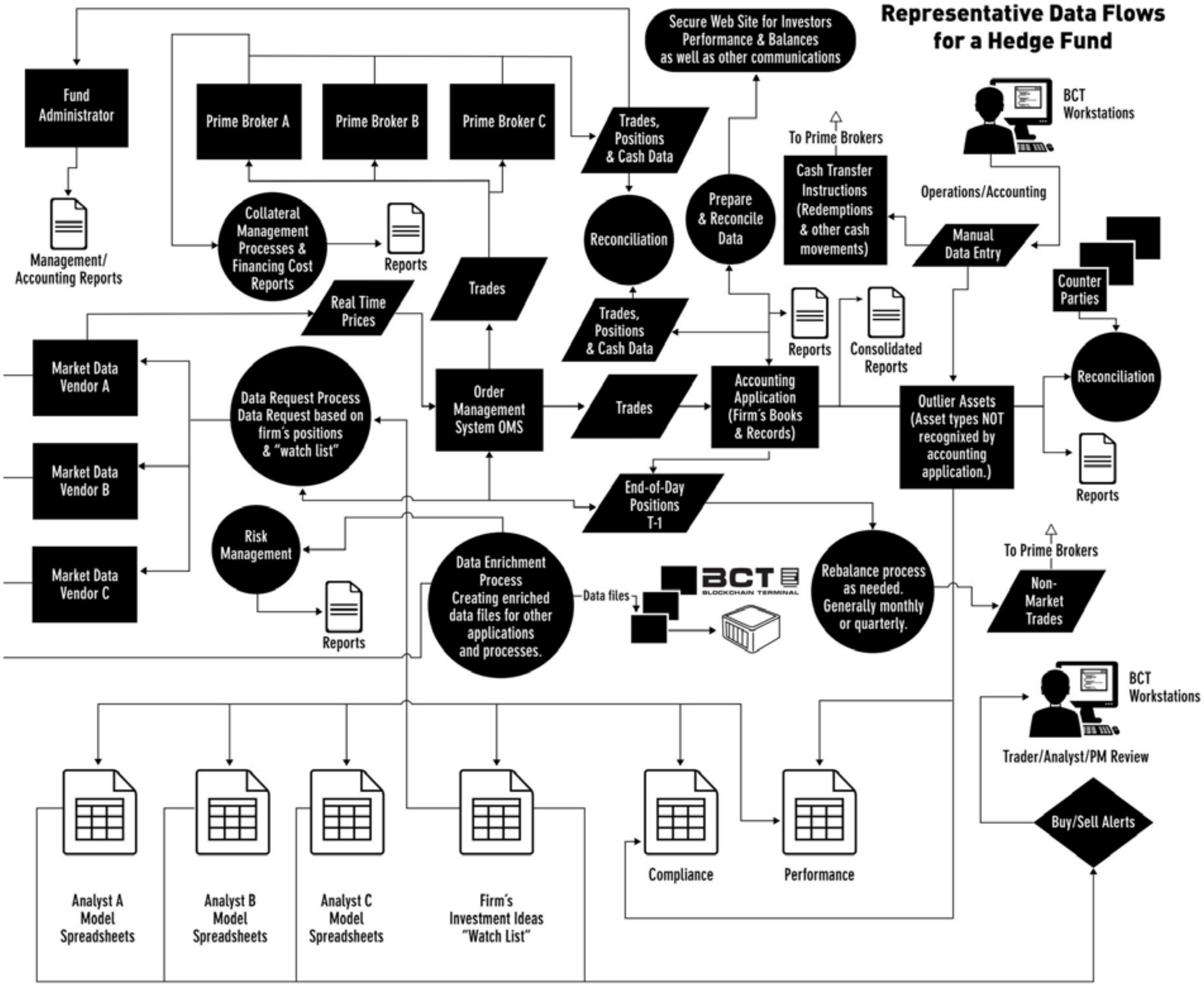

Representative Data Flows for a Hedge Fund
Fund Administrator
Management/ Accounting Reports
Prime Broker A
Prime Broker B
Prime Broker C
Trades, Positions & Cash Data
Secure Web Site for Investors Performance & Balances as well as other communications
BCT Workstations
To Prime Brokers
Cash Transfer Instructions (Redemptions & other cash movements)
Operations/Accounting
Prepare & Reconcile Data
Reconciliation
Manual Data Entry
Collateral Management Processes & Financing Cost Reports
Reports
Trades
Real Time Prices
Trades, Positions & Cash Data
Reports
Consolidated Reports
Counter Parties
Market Data Vendor A
Market Data Vendor B
Market Data Vendor C
Data Request Process Data Request based on firm's positions & "watch list"
Order Management System OMS
Trades
Accounting Application (Firm's Books & Records)
Outlier Assets (Asset types NOT recognized by accounting application.)
Reconciliation
Reports
End-of-Day Positions T-1
Risk Management
Reports
Data Enrichment Process Creating enriched data files for other applications and processes.
Data files
BCT BLOCKCHAIN TERMINAL
Rebalance process as needed. Generally monthly or quarterly.
To Prime Brokers
Non-Market Trades
BCT Workstations
Trader/Analyst/PM Review
Buy/Sell Alerts
Analyst A Model Spreadsheets
Analyst B Model Spreadsheets
Analyst C Model Spreadsheets
Firm's Investment Ideas "Watch List"
Compliance
Performance

Figure 2: Flow diagram of processes in a hedge fund with Blockchain Terminal's position outlined. It is intended that all regulated activities will be conducted through third party applications. Built with data sourced from: Thompson and Associates, 2010.

a. System Innovation

The Blockchain Terminal has been designed to bridge interactions between cryptographic assets, their blockchains and a hedge fund and asset management industry operating within a complex global regulatory environment. Interactions with these core data flows and constituents will position Blockchain Terminal applications to create innovation in a number of systems within traditional hedge fund infrastructure, including:

- **Order management and execution management systems** – EMS is layered above the OMS and application algorithms will generate multiple orders across venues and over a period of time. Applications are designed to display market data and provide users with robust algorithms for addressing a variety of market environments or enacting specific strategies in order to provide complete and efficient access to traditional and cryptocurrency trading destinations with the purpose of transacting orders.

- **The Blockchain Terminal will serve as an overlay to existing or arranged connectivity for users.** The Blockchain Terminal may enlist applications that bring other platform connectivity to the Blockchain Terminal so as to provide differentiated trading and execution services. In these instances, the Blockchain Terminal Fundstore will serve as a distribution platform and the relationship between application provider and user is apart from the Blockchain Terminal itself.

- **Portfolio management systems** – Through applications provide asset managers and buy-side teams with tools to manage their funds including portfolio analyses, order management, compliance functions, risk management functions, reporting and middle office solutions.

- **Safety and compliance solutions** – For convenience, compliance with cybersecurity best practices and ease of use, the Blockchain Terminal will support wallets (hardware and software-based) native to the Ethereum ecosystem that can be linked to electronic identities and can be used to generate an assured audit trail and track and trace the chain of events, authorizations and modifications.

- **The BCT Token will permit the development of entries that create a PoE entry**, allowing individuals and companies to prove the existence of a certain document, transaction, audit, or right at any given point in time.

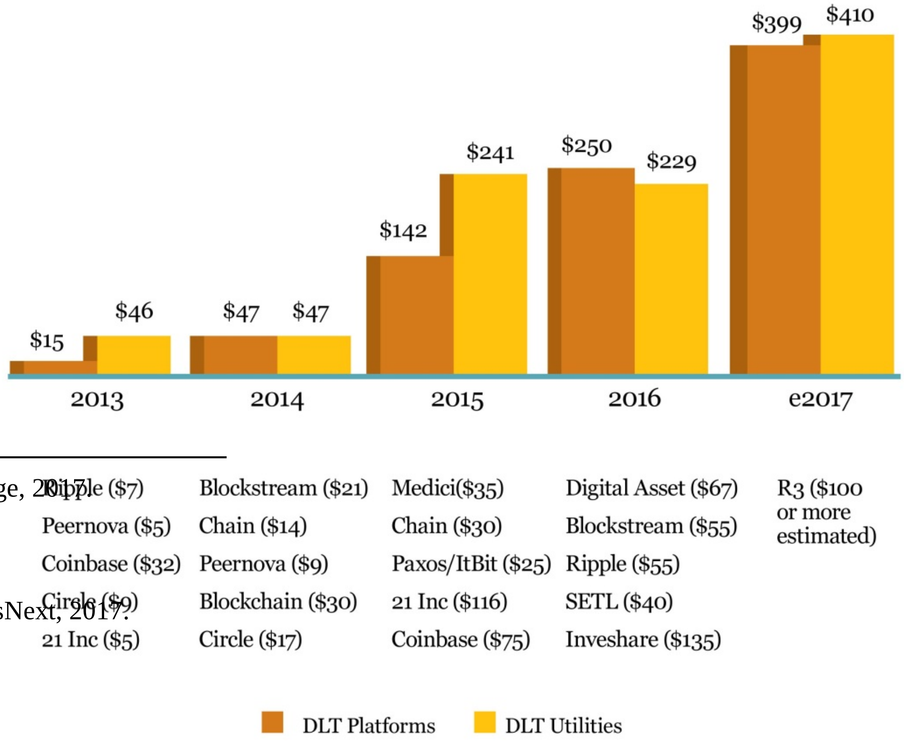
b. Blockchain and Cryptocurrency Applications

The Blockchain Terminal is positioned at the crossroads of two burgeoning areas in the hedge fund and asset management industry: increased demand for technology and increased interest in both cryptocurrencies and blockchain technology. Pressed by competitive pressures, the industry is turning to technology and increasingly cryptocurrency and blockchain solutions as a means to regain its previous standing.

A September 2017 survey of hedge fund managers by BarclayHedge revealed that 24% of the hedge funds surveyed either had invested in cryptocurrency or planned to invest within the next six months.[17] One study of 120 private fund advisors reported that "The findings are consistent with anecdotal evidence suggesting that the returns attainable through crypto investments have no short-term match in legacy systems."[18]

The related blockchain technology industry has seen a dramatic increase in investments in recent years. A report from the AITE Group explains that blockchain technology "is poised to give businesses a lower operational base, greater automation and faster delivery times."[19] Other research has reported that "blockchain technology plays a primary role in front office and investment functions, in the securing of crypto assets, but also in private investment fund managers' attempts to satisfy the growth expectations of clients."[20]

The staggering price fluctuations of cryptocurrencies are one indicator of the surge of interest in this market. Also striking is a sudden increase in the number of hedge funds devoted to cryptocurrencies and blockchain technology over the past year (see figure 3 below). A total of 17 crypto hedge funds were reported in existence between the years 2011 and 2016. As of November 2017, that number had multiplied to a total of 99 funds.[21]



[17] BarclayHedge, 2017.
[18] Kaal, 2017.
[19] Aite, 2017.
[20] Kaal, 2017.
[21] AutonomousNext, 2017.

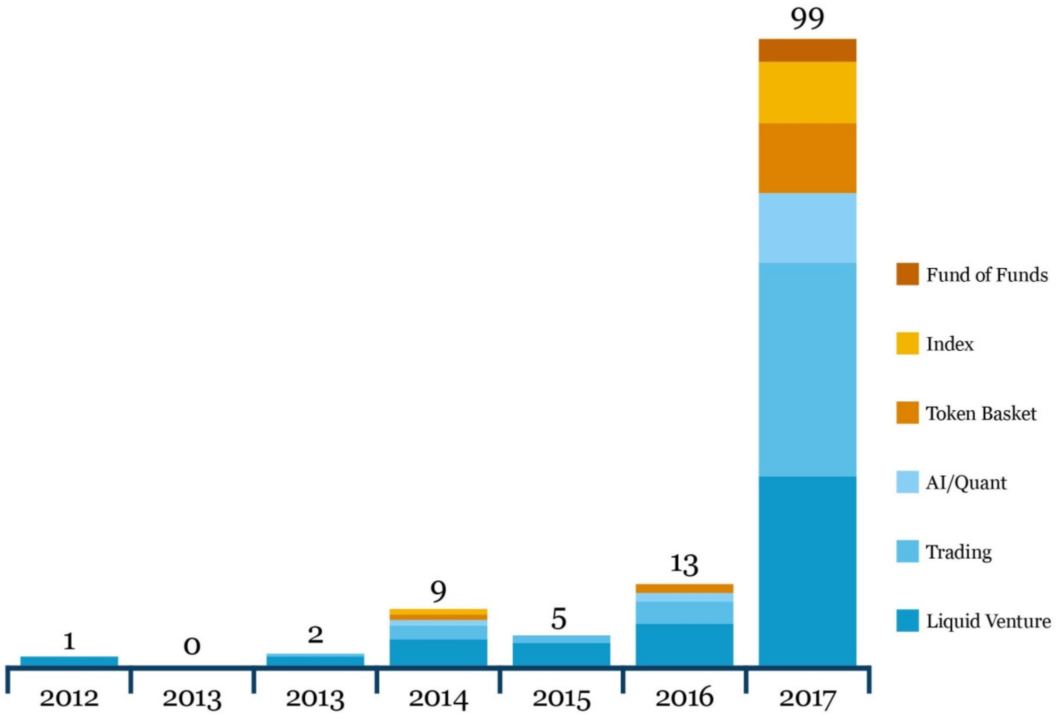


Figure 3: External investment going into select distributed ledger technology initiatives and derivatives, 2013-2017 (in USD millions). Source: Aite, 2017.

Figure 4: Crypto Funds by inception year and strategy: To truly understand the market fit of the Blockchain Terminal solution, it is important to first recognize the growing importance of technology within the hedge fund industry in general — along with recognizing the particular gap in tools to analyze this new asset class. Source (AutonomousNext, 2017).

c. Blockchain Terminal Application Categories

The Blockchain Terminal is intended to provide support for three different types of application architecture:

1. **Contained applications** – executed in the runtime scope of Blockchain Terminal hardware and its local resources.

2. **Metered applications** – listed for subscription and use within the Blockchain Terminal, but not executed in the runtime scope of the Blockchain Terminal and its local resource. They are hosted independent of Blockchain Terminal hardware, while still registered for use with local APIs. These applications will rely on Blockchain Terminal infrastructure for integration and for leveraged Blockchain Terminal components such as logging, persistence

and identity management. Metered application registration, billing and support will be managed from the Blockchain Terminal after installation.

3. **Linked applications** – while displayed on the Blockchain Terminal, they will not be integrated. These applications may be registered with the Blockchain Terminal for product placement. When users select a linked application, they will be brought to a different online location. These curated applications will be promoted to Blockchain Terminal users.

5.ComplianceGuard

ComplianceGuard demonstrates a productive use of the Blockchain Terminal ledger. It is a secure tool for recording a CCO's logbooks and is already deployed with a number of hedge funds.

ComplianceGuard is being devloped to integrate with a firm's OMS/EMS to record all transactions on the Blockchain Terminal ledger. It provides real-time transaction monitoring and visibility into instances of concern for both regulatory and mandate specific compliance. It also is intended to enable immediate remote *ad hoc* audits of transactional data, should compliance issues arise.

a. Features

ComplianceGuard is being developed to journal investment and fund activities, propagates alerts, stores compliance alert resolutions and facilitate the audit of alert resolutions. The alerts are generated through the pre-trade and post-trade compliance parameters specified at the OMS/EMS application.

A firm's activities are collected via mechanisms established during the installation and integration process. As transactions are processed, transaction data is committed to the Blockchain Terminal and hashes are placed on the Blockchain Terminal private ledger. Transaction data also includes alerts that are configured at the side of the OMS/EMS. These alerts are distributed to parties determined by the firm and may include internal staff and external constituents, including limited partners (such as investors, fund of fund managers and regulators).

For the purpose of journaling against the Blockchain Terminal global ledger and to eliminate the need for a Blockchain Terminal global administrator to observe the employment actions of constituent firms, BCT Tokens do not use pseudonymous public keys. In this credentialed connection, the Blockchain Terminal reads transaction blocks from a firm's private ledger and writes the hash root of those blocks to the Blockchain Terminal global ledger. Confidentiality is secured as no Merkle roots associated with hedge fund private ledgers are individually identifiable nor do they reveal any proprietary information.

Journal entries are available for review by CCOs or personnel designated by a firm in order to address alerts regarding irregularities or issues detected as the result of the compliance parameters configured in a hedge fund's OMS/EMS system. Responses include the comments and other supporting documentation that help establish accountability for the activity that occurred and are subsequently journaled to the Blockchain Terminal private ledger using ComplianceGuard.

ComplianceGuard will be designed to allow Blockchain Terminal users to access the private and global components of the Blockchain Terminal ledger. With access to transactions from a firm's private ledger, it is possible to identify applicable hashes. An auditor is able to combine these identified hashes and scan the Blockchain Terminal global ledger for the root hash. By necessity, the hash on the global ledger will occur with a slight delay in relation to the last private transaction hash being observed. The auditor of the global ledger simply looks for related hashes on the global ledger on the approximate end-date of a specific transaction chain to receive verification that all transactions have been hashed to the Blockchain Terminal global ledger and that the Blockchain Terminal private ledger has not been altered.

This audit approach preserves privacy and eliminates the need for permissions on the Blockchain Terminal global ledger. All parties can see public hash data for a given firm, fund or account, but only an authorized user for a specific firm, fund or account can verify the integrity of that data using the data of the Blockchain Terminal private ledger.

Similarly, alert resolutions are posted in the transaction window as they are made and their hashes are captured on the firm's private ledger and added in the calculated hash to the Blockchain Terminal global ledger. In this way, all CCO logbook actions can be verified as having been made in the period.

b. Integration

ComplianceGuard is intended to be pre-installed on each Blockchain Terminal and to work in a standalone or API integrated mode. In standalone mode, the firm is responsible for uploading transactions to the ComplianceGuard application. CG Blockchain expects that Blockchain Terminal vendors and integrators will be available in the future to facilitate direct integration with transaction processing and report generating systems of hedge fund users.

c. The ComplianceGuard Reference Implementation

The ComplianceGuard Reference Implementation is a self-contained platform delivering integrated platform software installed on a desktop terminal built into the Blockchain Terminal. When connected to a local area network, it serves as a node that creates the replication and consensus required for the Blockchain Terminal private distributed ledger.

Technical features of the ComplianceGuard Reference Implementation include:

- **A self-contained server** – Built into the Blockchain Terminal and, if desired, part of a CCOs office or data center. A RAID storage configuration maintains the core Blockchain Terminal private ledger and other key elements used locally by Blockchain Terminal applications running locally.

- **User desktop terminals** – The Blockchain Terminal is a security hardened compact desktop system installed at one or more workstations accessible to staff and traders. It presents a small footprint with large monitor real estate and keyboard, as well as USB ports to accommodate hardware wallets and peripherals. ComplianceGuard is embedded in this deployment.

- **Anticipated components** – In the future, mobile, tablet and other component choices are expected as part of the system to enable remote access to critical information.

6. The BCT Token

Two tokens co-exist in the Blockchain Terminal ecosystem: A native token that will power the Blockchain Terminal ledger (the "Native Token") and the BCT Token (which is an ERC 20 compliant token and created in the public Ethereum network) that is being sold by BCT Inc, an affiliate of CG Blockchain, in accordance with the Contribution Agreements and Distribution Terms and Conditions found on the BCT Inc, website. The BCT Token will be used to pay for subscription and entitlements to the services provided on the Blockchain Terminal. Each BCT Token held by a purchaser will be credited against a Native Token through a smart contract on a one-to-one basis. The Native Token will serve as the delivery mechanism for allowing BCT Token holders to access subscriptions and entitlements on the Blockchain Terminal. Together, the two tokens secure integrity and provide incentive for the correct functioning of the Blockchain Terminal. Participants in the Blockchain Terminal community will be able to use BCT Token to:

- Request or commit domain objects and ontologies to the Blockchain Terminal ledger.

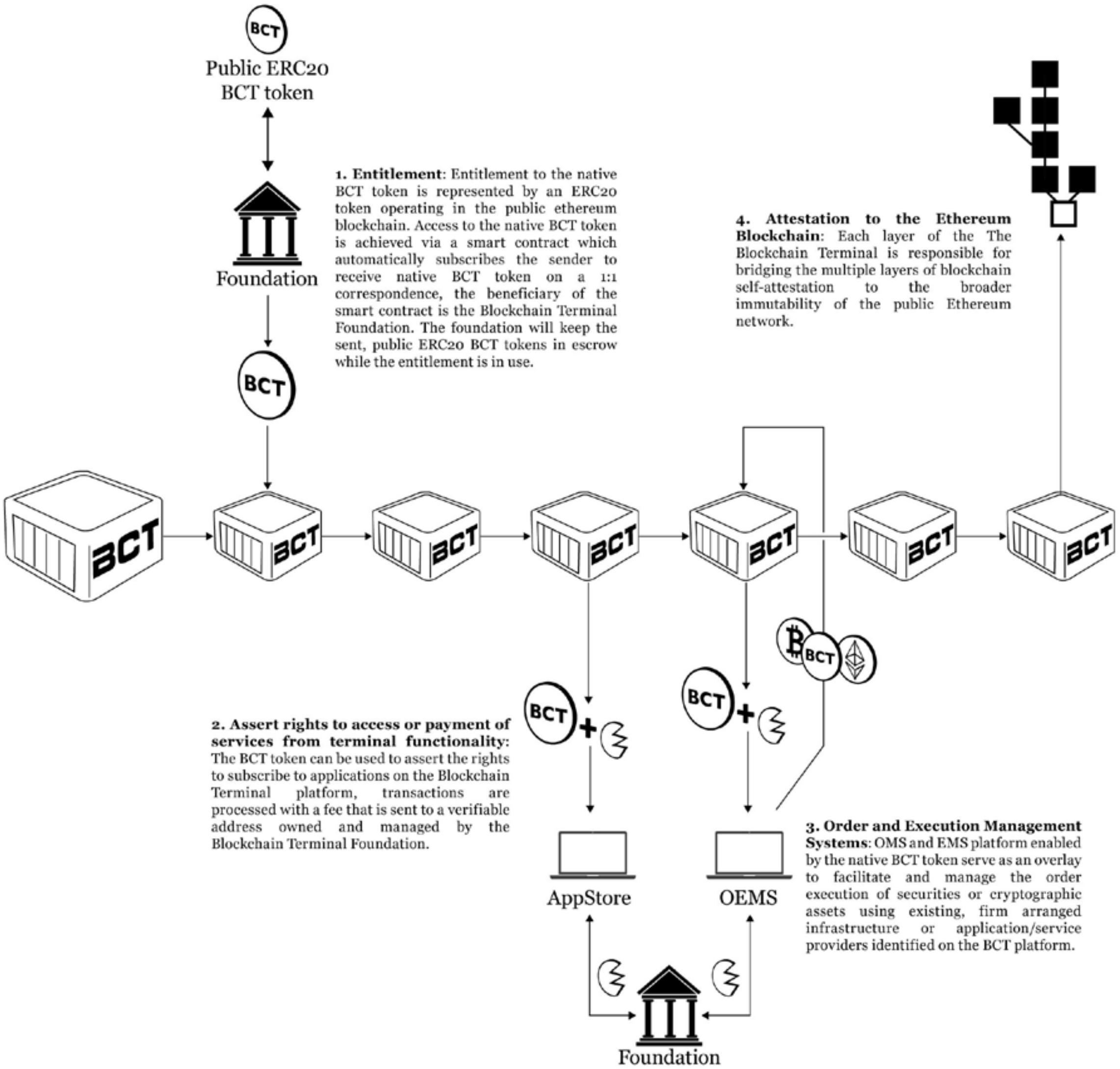
- Request or commit a PoE to the Blockchain Terminal Ledger.

- Access applications on the Blockchain Terminal (either on a one-time use or subscription basis).

- Enable core services of the Blockchain Terminal platform

The Blockchain Terminal permissioned ledger is strongly centralized, making entitlement to the robust public Ethereum network the most secure choice. Because holders of the BCT Token will use the Blockchain Terminal and its services, they will be pre-disposed to use established practices and processes both in software, and hardware. This practice provides personal and institutional cybersecurity and will ensure the control and preservation of their entitlement to Blockchain Terminal services using off-line cold storage methods, which the public ERC20 BCT Token will support.

Figure 5 below illustrates a hypothetical BCT Token lifecycle inside a Blockchain Terminal.



1. Entitlement: Entitlement to the native BCT token is represented by an ERC20 token operating in the public ethereum blockchain. Access to the native BCT token is achieved via a smart contract which automatically subscribes the sender to receive native BCT token on a 1:1 correspondence, the beneficiary of the smart contract is the Blockchain Terminal Foundation. The foundation will keep the sent, public ERC20 BCT tokens in escrow while the entitlement is in use.

4. Attestation to the Ethereum Blockchain: Each layer of the The Blockchain Terminal is responsible for bridging the multiple layers of blockchain self-attestation to the broader immutability of the public Ethereum network.

2. Assert rights to access or payment of services from terminal functionality: The BCT token can be used to assert the rights to subscribe to applications on the Blockchain Terminal platform, transactions are processed with a fee that is sent to a verifiable address owned and managed by the Blockchain Terminal Foundation.

3. Order and Execution Management Systems: OMS and EMS platform enabled by the native BCT token serve as an overlay to facilitate and manage the order execution of securities or cryptographic assets using existing, firm arranged infrastructure or application/service providers identified on the BCT platform.

Figure 5: Simplified token lifecycle showing its many different stages and relevant constituents. Note that the BCT Token is bound in its complete utility to the Blockchain Terminal through the Native Token and has the sole purpose of representing entitlement to services provided using the Native Token.

BCT Token balances will be accrued through the normal course of use of services and applications provided on the Blockchain Terminal in the form of fees.

It is intended that subscriptions to use third party applications on the Blockchain Terminal will be denominated in BCT Tokens. However, in some cases, applications made available on the Blockchain Terminal may have their own native token and may additionally require the use of such tokens for the provision of services. In such cases, users of Blockchain Terminals will be responsible for acquiring necessary application tokens. Subscription or service transactions in BCT Tokens may incur a fee, payable in BCT Token. BCT Tokens used can subsequently be returned to circulation as part of the scheduled Phased Implementation Plan. For more information about the Phased Implementation Plan see Section 8 below.

7. Blockchain Terminal Management

The Blockchain Terminal is a creation of CG Blockchain. The intellectual property associated with the Blockchain Terminal, other than ComplianceGuard and other third party applications, is anticipated to be transferred to BCT Inc, the issuer of the BCT Tokens. It is also intended that BCT Inc will use proceeds from its sale of the BCT Tokens to fund the further development of the Blockchain Terminal and applications to be available on the Blockchain Terminal, through development agreements with affiliates of BCT Inc, including CG Blockchain, HF Blockchain, and Optimumm. It is further intended that BCT Inc will enter into a service agreement with an affiliate to operate and service the Blockchain Terminal.

An affiliate of BCT Inc is expected to be responsible for high-level governance and coordination functions for the Blockchain Terminal and its ledger network. Initially, the Blockchain Terminal global ledger network will be strongly centralized; however, its permissioned state provides opportunities to broaden and diversify the validators on the network. Qualified participants may include auditors, regulators and service providers who share an interest in maintaining the integrity of the Blockchain Terminal global ledger.

Responsibilities of BCT Inc affiliates will include:

- Govern and initiate the BCT Token generation event and distribution.

- Provide support for program development and oversight for the Blockchain Terminal application approval process. Manage the workflow associated with candidate approvals and listings in the Blockchain Terminal application catalog. Conduct conferences, presentations and meet-ups to provide vendor and developer support.

- Develop consensus and provide organization for the Blockchain Terminal community by encouraging and promoting innovation and effective distribution of applications and services to both traditional and emerging investment managers.

- Provide governance for domain models and ontologies made available to the Blockchain Terminal global ledger. Operate and maintain object enrollment and notary features of smart contracts on the global ledger.

- Maintain the hosting environment and configuration of permissioned network features including the web-root of trust for VPN connectivity with hedge funds and other asset managers and provide support for information security across Blockchain Terminal global ledger nodes.

8. Phased Implementation Plan

Phase I – Design and initial deployment

- Deployment of terminals loaded with a lightweight online version of applications for research and data analytics; will only be accessible using BCT Tokens.
- Development of basic integrations with ComplianceGuard and third party implementations.
- Candidate architecture and reference application released in the form of the ComplianceGuard application.
- Documentation and resources released for community review.

Phase II – Engagement (2018-2019)

- Full store integration of platform applications.
- Road show introducing Blockchain Terminal applications and services at developer events.
- Developer support site introduction: public repositories, API documentation, examples and public communication channels.
- FinTech incubation and promotion of application developers for the Blockchain Terminal.
- Community involvement and open review of platform considerations for the development of terminal-based solutions.

Phase III – Promotion (Ongoing)

- Expansion of subscription and accounting features.
- Continuous improvement of the Blockchain Terminal.
- Expansion of the Blockchain Terminal community.

Blockchain Terminal implementation scheduling is subject to change as emergent platform priorities, resources and broader community involvement are considered. There can be no guarantee and any or all of these steps will be successfully implemented.

Appendix A - Blockchain Terminal Architecture

The architecture of the application development platform provides a framework for standardized development and implementation that lends consistency of user experience to applications available for the Blockchain Terminal. It will also enforce and constrain the behavior of applications hosted by Blockchain Terminal devices that draw data from the private and global ledgers.

A. Language Support

Blockchain Terminal applications can be authored in a number of languages. Java, Scala, Python and JavaScript are intended to be the initially supported languages that will have API bindings.

B. Interface

Interface guidelines will be provided for user experience with the Blockchain Terminal. Application authors are free to use any UI framework of their choosing, although HTML5, CSS 3.0 and support for responsive device access are encouraged.

C. Service Tier

The Service Tier of the application environment is designed to provide stable, managed access to:

- Manage accounts, authenticate/authorize users, set permissions for application features and assign user roles that use these permissions.
- Read and store data to components of the Blockchain Terminal ledger or the public Ethereum network.
- Intercept integration feeds of the core Blockchain Terminal compliance application, thereby getting near real-time order, transaction, security, pricing and other data integrated with Blockchain Terminal hardware.
- Create permissioned synchronous and asynchronous integrations that leverage Blockchain Terminal’s private chain for creating immutable, private ledger entries.
- Access time and DNS functionality.
- Manage scheduled tasks.
- Observe and manage application statuses.

D. Integration

Integration with data from the Blockchain Terminal will be supported using three primary modes:

1. **REST/RESTful services** – provide ease of integration for the purpose of interacting with the application environment and integrated feeds using a synchronous mechanism.

2. **Publish and subscribe messaging** – based on the Advance Message Queuing Protocol (AMQP), this integration approach allows developers to define publish and subscription channels for integrating their application to receive events asynchronously or in near-real time. Publish and subscribe messaging channels can be used to create an event bus-based sharing between Blockchain Terminal metered and contained applications.

3. **WebSockets protocol** – allows for reactive event modeling from the Blockchain Terminal.

Each integration model will use native Blockchain Terminal authentication, authorization and logging. This provides a simple mechanism for developing robust applications and integrating them into a compliance-vetted environment.

E. Persistence

Blockchain Terminal applications may write to components of the Blockchain Terminal ledger, enterprise database facilities, or to their own storage. Applications may also read from the Blockchain Terminal ledger or access public blockchains, or call web services and oracles.

F. Security

Security on the Blockchain Terminal is intended to be defined in terms of identity management, authentication, authorization and resilience:

Identity – The firm's administrator will manage user identity. Blockchain Terminals can be integrated with one or more local identity providers on the hedge fund network, including Active Directory and LDAP. By specifying the correct search key or user credentials, the Blockchain Terminal API will provide authentication and authorization using enterprise credentials. Roles defined for users in the Blockchain Terminal Framework and API can be written back to primary enterprise identity management systems for the purpose of a federated and full audit.

In the absence of integration to an enterprise system, the Blockchain Terminal environment will maintain its own LDAP directory implementation, providing a lightweight mechanism for user, group, permission and role management across the Blockchain Terminal Framework and API-integrated applications. This environment will be similarly queried as an LDAP provider from the broader enterprise. User entries are supported as X500 named entities and certificates are specified as X509v3 compatible.

- **Authentication** – will be performed against the API using username/credential pairings. Credentials can include passwords, public key certificates and mobile tokens.

- **Authorization** – authenticated user authorization occurs against the full Blockchain Terminal role base.

- **Resilience** – the local LDAP provider can be backed up to a standby instance hosted on either another Blockchain Terminal device or separate LDAP server.

G. Logging and Audit

Application logging will follow standard, ISO-compliant formats with info, error, and other logging levels as part of the framework. It will include support for building internal logging chains, which can be used to reconstruct application behavior, for auditing purposes.

H. Monitoring and Process Management Interface

All applications running on the Blockchain Terminal will be monitored and restarted from a global administration console available through the Blockchain Terminal. Process monitoring will enable system administrators to easily identify applications in use, tokens spent by each application (to better manage budget) and extract basic logs associated with system-events associated with their running.

SNMP datagrams can be trapped and integrated through the monitoring interface into standard log capture tools and analyzed by network and infrastructure products.

I. Scheduling

The Blockchain Terminal development environment will have a scheduling interface that can be used by developers to schedule jobs, including reports, feeds and email associated with specific application tasks. Scheduled tasks can be exposed to the time and monitoring interfaces and can be journaled as a ComplianceGuard event to ensure tasks run when scheduled with sensitivity to other application dependencies.

J. Time

The Blockchain Terminal will use a timestamp authority ("TSA") server to offer a secure, reliable, time source. This feature will be available to all running applications, whether on or off Blockchain Terminal and enables true synchronization of internally generated block headers and other compliance events. Timestamp authority is preferable over native system time, which can fall out of sync.

K. Native DNS and NSLookup

The Blockchain Terminal development environment will provide native DNS and NSLookup to ensure that internal services do not hit external network servers, thereby preventing DNS-based attack vectors for hosted applications.

Appendix B – Hypothetical Blockchain Terminal User Story Examples

Hypothetical 1 – Core Blockchain Terminal Functionality

Blockchain Terminal vendor submits application for approval – A "vendor" is a developer or traditional application developer interested in the Blockchain Terminal as a distribution environment for an existing or newly developed tool.

Using the Blockchain Terminal Framework and APIs, the vendor completes testing of the application in the local development environment and prepares to upload the application to a Blockchain Terminal in the vendor's possession. The new application is not available outside of the immediate local network of the vendor's Blockchain Terminal.

The vendor enters the developer sandbox environment, uploads the new application and is provided an IP address for local shell access to the runtime environment for the application. A firm administrator can help with the installation of necessary tools to this sandbox environment.

Once fully configured, vendor visits the sandbox management console that allows submission of the configured application. Additional information regarding the application description, supporting links and documentation is included in the submission. Upon approval, vendors receive notice that the application has been posted to the Blockchain Terminal.

Hedge fund user browses and selects application – A hedge fund employee receives a Blockchain Terminal. As part of the setup process, the hedge fund's Blockchain Terminal administrator has configured the Blockchain Terminal settings to integrate with the hedge fund's enterprise active directory server, allowing use of the same credentials used for other systems accessed at the hedge fund. Hedge fund user roles allow browsing and subscription to applications on the Blockchain Terminal.

Hedge fund users can browse a curated application directory and make selections from a number of categories. A global application search allows for further exploration on the basis of basic and advanced filters that allow use of criteria such as category, description, author, price and last update.

If a search identifies an application of interest, the user can view details about the application, including its description and past comments and reviews offered by other Blockchain Terminal users. Prices are intended to be clearly listed for installation and monthly support, as applicable.

Because the terminal is configured as an enterprise terminal, should a hedge fund user subscribe to an application both the hedge fund Blockchain Terminal administrator and a designee of the CCO are notified. The user is informed that the request to add the application is in process and that a status notification will arrive by email.

The hedge fund Blockchain Terminal administrator receives CCO approval of the subscription. By logging into the local administrative environment it is possible to view all active users accounts belonging to the hedge fund and to approve the installation. The administrator can remotely install, remove and update software on all system Blockchain Terminals from this environment.

If the selected application is a Blockchain Terminal contained application, no integrations with other systems or support from a Blockchain Terminal vendor or development partner is needed to help with the installation. Upon approval from the administrator, the selected application is cloned from the Blockchain Terminal Platform application registry to the user's Blockchain Terminal and the application is available for immediate use.

Hypothetical 2 – Audit and Compliance

Hedge fund CCO views private ledger transaction log and annotates CCO logbook – ComplianceGuard assists hedge funds in navigating the complexities of regulatory compliance by bridging the fiduciary requirements of CCOs with the objectivity and neutrality of external auditing authorities. In order to verify transaction activities, CCOs must view and annotate transaction logs using the Blockchain Terminal Platform private ledger. The Blockchain Terminal Platform ensures that CCOs maintain transactional log records on a private ledger and then provides the means for external auditors to validate using hashed data journaled to the global ledger.

For example, the manager of a hedge fund takes a number of employees and the CEO of another company out to dinner. The next day, the hedge fund's CCO opens ComplianceGuard's Compliance Officer Log Book and enters all the entertainment expenses.

By using ComplianceGuard to enter the receipt and declaration into the Blockchain Terminal Platform private ledger, the CCO ensures that the data trail has been entered into the Blockchain Terminal Platform ledger. If no alerts are generated, the CCO can be sure that internal standards are not breached and that the gifts to this particular CEO do not surpass a certain limit.

External auditor is notified of compliance alerts – There are intended to be three alert levels in ComplianceGuard, the most serious of which is also sent outside the fund, prompting an external audit. The Blockchain Terminal tools for a retrospective review of a firm's financial records in response to a compliance alert provide oversight that maydetect (and even prevent) fraud or malfeasance. The auditor is required to document whether or not the event that triggered the alert was determined to be an issue of Critical Accounting Matters ("CAM").

For example, an algorithm used by ComplianceGuard flags a trade as having breached a compliance issue. An alert is sent to the CCO. Since the volume of the trade was large, the issue is serious and an alert notification is also sent to the hedge fund's auditing partner. The auditing partner contacts the hedge fund's CCO requesting information about the potential compliance breach. The Blockchain Terminal alert system helps ensure that issues are reviewed for compliance.

External auditor can be granted access and use the double attestation method to verify the integrity of notarized data – ComplianceGuard is designed to verify the integrity of data in a way that is similar to the double attestation method commonly used by external auditors. In the standard method of double attestation, an auditor assesses the authenticity of a document and then declares its authenticity by attaching the document to the signature of the verifying personnel. The process requires submitting original documents, along with copies, to authorized employees who verify and sign/stamp.

ComplianceGuard facilitates double attestation with exactitude. When an external auditor arrives on the site, the CCO grants access to execute a function in ComplianceGuard that compares the hashes stored in the CCO's hard drive to the hashes stored on the ledger that the external auditor has access to.

Finding that the two sets of hashes align properly, the auditor can be certain that the hedge fund's private ledger transaction log data is valid. The auditor is then able to proceed with confidence that the fund's data has not been tampered with or altered.

References

Aite: Is blockchain a good fit?: A disciplined approach in post-trade, 2017. Available at: https://aitegroup.com/report/ blockchain-good-fit-disciplined-approach-post-trade.

Andersen, Nicolai: Blockchain technology: A game changer in accounting?, 2016. Available at: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/ Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf.

Araoz, Manuel: Proof of existence, 2013. Available at: https://proofofexistence.com/. AutonomousNext.

BarclayHedge: Fundmanagersurvey, 2017. Available at: https://www.barclayhedge. com/research/hedge-fund-manager-survey/2017/2017-10a.html?btg_trk=BH-HOMEPAGE.

Brown, Tom: Real use cases for blockchain and distributed ledger technologies in the asset management sector, 2017. Available at: https://assets.kpmg.com/content/dam/ kpmg/xx/pdf/2017/07/blockchain-brochure.pdf.

Cachin, Christian: Architecture of the hyperledger blockchain fabric, 2016. Available at: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf.

Castro, Miguel; Liskov, Barbara, et al. : Practical byzantine fault tolerance. In OSDI, volume 99, pages 173–186, 1999.

CME-Group: Cme clearport api - fixml message specification, 2017. Available at: https://www.cmegroup.com/confluence/display/EPICSANDBOX/CME+ClearPort+ API+-+FIXML+Message+Specification.

Crawford and Meadows: Blockchain technology as a platform for digitization, 2017. Available at: http://www.ey.com/Publication/vwLUAssets/EY-blockchain-technology-as-a-platform-for-digitization/$FILE/EY-blockchain-technology-as-a-platform-for-digitization.pdf.

Crypto fund list segmentation, 2017. Available at: https://next.autonomous.com/ cryptofundlist.

Czaban, Peter: Proof-of-authority chains, 2017. Available at: https://github.com/paritytech/ parity/wiki/Proof-of-Authority-Chains.

Diemers and Koster: Five propositions to transform the financial services sector, 2016. Available at: https://www.pwc.ch/en/publications/2016/ tp_blockchain_5_theses_en.pdf.

FpML: Financial products markup language, 2015. Available at: http://www.fpml.org/.

Green, Matthew: Zero knowledge proofs: An illustrated primer, 2014. Available at: https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/.

Green, Matthew: Zero knowledge proofs: An illustrated primer part 2., 2017. Available at: https://blog.cryptographyengineering.com/2017/01/21/zero-knowledge-proofs-an-illustrated-primer-part-2/.

Hearn, Mike: Corda: A distributed ledger, 2016. Available at: https://docs.corda.net/_static/ corda-technical-whitepaper.pdf.

Kaal: Blockchain innovation for private investment funds, 2017. Available at: https://papers. ssrn.com/sol3/papers.cfm?abstract_id=2998033.

Merkle, Ralph: Protocols for public key cryptosystems. In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122–133. IEEE Computer Society, 1980.

Nakamoto, Satoshi: Bitcoin: A peer-to-peer electronic cash system, 2008. Available at: https:// bitcoin.org/bitcoin.pdf.

Thompson and Associates: Technology solutions for hedge funds, 2010. Available at: http: //www.thompson-and-associates.com/end-to-end.htm.

IMPORTANT INFORMATION FOR POTENTIAL CONTRIBUTORS

THIS WHITEPAPER DOES NOT CONSTITUTE A PROSPECTUS OR OFFERING DOCUMENT AND DOES NOT AND IS NOT INTENDED TO CONSTITUTE AN OFFER TO SELL, NOR THE SOLICITATION OF ANY OFFER TO BUY, AN INVESTMENT, A SECURITY OR A COMMODITY, OR AN OPTION ON OR ANY OTHER RIGHT TO ACQUIRE ANY SUCH INVESTMENT, SECURITY OR COMMODITY. THIS WHITEPAPER HAS NOT BEEN REVIEWED BY, PASSED ON OR SUBMITTED TO ANY U.S. FEDERAL OR STATE AGENCY OR SELF-REGULATORY ORGANIZATION OR TO ANY OTHER FOREIGN AGENCY OR SELF-REGULATORY ORGANIZATION. THIS WHITEPAPER DOES NOT CONSTITUTE ADVICE TO PURCHASE ANY BCT TOKEN NOR SHOULD IT BE RELIED UPON IN CONNECTION WITH ANY CONTRACT OR CONTRIBUTION DECISION.

THE BCT TOKENS HAVE NOT BEEN AND WILL NOT BE REGISTERED UNDER THE SECURITIES ACT OF 1933, AS AMENDED (THE “SECURITIES ACT”), OR ANY OTHER LAW OR REGULATION GOVERNING THE OFFERING, SALE OR EXCHANGE OF SECURITIES IN THE UNITED STATES OR ANY OTHER JURISDICTION. THE OFFERING OF BCT TOKENS WILL BE MADE (1) INSIDE THE UNITED STATES TO “ACCREDITED INVESTORS” (AS DEFINED IN SECTION 501 OF THE SECURITIES ACT) IN RELIANCE ON REGULATION D UNDER THE SECURITIES ACT TO U.S. PERSONS (AS DEFINED IN SECTION 902 OF REGULATION S UNDER THE SECURITIES ACT) AND (2) OUTSIDE THE UNITED STATES TO NON-U.S. PERSONS IN RELIANCE ON REGULATION S. SUBJECT TO CERTAIN LIMITED EXCEPTIONS, PERSONS PURCHASING AS U.S. ACCREDITED INVESTORS WILL BE REQUIRED TO MAINTAIN THEIR BCT TOKENS UNTIL THE FIRST ANNIVERSARY OF THE ISSUANCE OF THE BCT TOKENS. PERSONS PURCHASING AS NON-U.S. PERSONS WILL ONLY BE ENTITLED TO RESELL THEIR BCT TOKENS AFTER 90 DAYS FROM THE ISSUANCE DATE TO OTHER NON-U.S. PERSONS IN AN OFFSHORE TRANSACTION (AS DEFINED IN RULE 902 OF THE SECURITIES ACT).

THIS WHITEPAPER CONTAINS FORWARD-LOOKING STATEMENTS THAT ARE BASED ON THE BELIEFS OF CG BLOCKCHAIN, AS WELL AS CERTAIN ASSUMPTIONS MADE BY AND INFORMATION AVAILABLE TO CG BLOCKCHAIN. THE PROJECT AS ENVISAGED IN THE WHITEPAPER IS UNDER DEVELOPMENT AND IS BEING CONSTANTLY UPDATED, INCLUDING BUT NOT LIMITED TO KEY GOVERNANCE AND TECHNICAL FEATURES. ACCORDINGLY, IF AND WHEN THE PROJECT IS COMPLETED, IT MAY DIFFER SIGNIFICANTLY FROM THE PROJECT SET OUT IN THIS WHITEPAPER. NO REPRESENTATION OR WARRANTY IS GIVEN AS TO THE ACHIEVEMENT OR REASONABLENESS OF ANY PLANS, FUTURE PROJECTIONS OR PROSPECTS AND NOTHING IN THIS WHITEPAPER IS OR SHOULD BE RELIED UPON AS A PROMISE OR REPRESENTATION AS TO THE FUTURE.

OWNERSHIP OF BCT TOKENS WILL CARRY NO RIGHTS, WHETHER EXPRESS OR IMPLIED, OTHER THAN A LIMITED POTENTIAL FUTURE RIGHT OR EXPECTATION TO USE BCT TOKENS AS SET FORTH IN THIS WHITEPAPER AND IN THE DISTRIBUTION TERMS AND CONDITIONS. BCT TOKENS WILL BE MADE AVAILABLE TO CONTRIBUTORS SOLELY IN ORDER TO PROVIDE OR RECEIVE SERVICES ON THE BLOCKCHAIN TERMINAL AND TO SUPPORT THE DEVELOPMENT, TESTING, DEPLOYMENT AND OPERATION OF THE BLOCKCHAIN TERMINAL. BCT TOKENS ARE NOT INTENDED FOR INVESTMENT, SPECULATIVE OR OTHER FINANCIAL PURPOSES. BCT TOKENS DO NOT REPRESENT OR CONSTITUTE:

- ANY OWNERSHIP RIGHT OR STAKE, SHARE, EQUITY, SECURITY, COMMODITY, BOND, DEBT INSTRUMENT OR ANY OTHER FINANCIAL INSTRUMENT OR INVESTMENT CARRYING EQUIVALENT RIGHTS;

- ANY RIGHT TO RECEIVE FUTURE REVENUES, PROFITS, DIVIDENDS, INTEREST, SHARES, EQUITIES, SECURITIES OR ANY OTHER FORM OF PARTICIPATION, ECONOMIC OR OTHERWISE, OR ANY GOVERNANCE RIGHT IN OR RELATING TO BCT TOKENS, BCT INC, OR ANY AFFILIATE OF BCT INC;

- ANY FORM OF MONEY OR LEGAL TENDER IN ANY JURISDICTION NOR DO THEY CONSTITUTE ANY REPRESENTATION OF MONEY (INCLUDING ELECTRONIC MONEY);

- THE PROVISION OF ANY GOODS OR SERVICES PRIOR TO THE DATE ON WHICH BCT TOKENS MAY BE DELIVERED TO CONTRIBUTORS; OR

- ANY FUTURE RIGHT TO SELL BCT TOKENS, OR TRADE BCT TOKENS TO OR WITH ANY OTHER PARTY.

BCT TOKENS WILL BE DISTRIBUTED IN ACCORDANCE WITH THE TERMS AND CONDITIONS SET FORTH IN THE DISTRIBUTION TERMS AND CONDITIONS, AS PUBLISHED ON BCT INC'S WEBSITE FROM TIME TO TIME. CG BLOCKCHAIN AND ITS AFFILIATES MAY DECIDE IN THEIR SOLE DISCRETION, TO ABANDON THE BLOCKCHAIN TERMINAL AND TO FOREGO ISSUING ANY ADDITIONAL BCT TOKENS.

BCT INC AND ITS AFFILATES INTEND TO OPERATE IN FULL COMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS AND OBTAIN THE NECESSARY LICENCES AND APPROVALS AS MAY BE REQUIRED IN THEIR OPINION IN KEY MARKETS. THIS MEANS THAT THE DEVELOPMENT AND ROLL-OUT OF ALL THE FEATURES OF THE BLOCKCHAIN TERMINAL AS DESCRIBED IN THIS WHITEPAPER ARE NOT GUARANTEED. REGULATORY LICENCES OR APPROVALS MAY BE REQUIRED IN A NUMBER OF RELEVANT JURISDICTIONS IN WHICH RELEVANT ACTIVITIES MAY TAKE PLACE. IT IS NOT POSSIBLE TO GUARANTEE, AND NO PERSON MAKES ANY

ASSURANCES, THAT ANY SUCH LICENCES OR APPROVALS WILL BE OBTAINED WITHIN A PARTICULAR TIMEFRAME OR AT ALL. THIS MEANS THAT BCT TOKENS AND OTHER FEATURES OF THE BLOCKCHAIN TERMINAL MAY NOT BE AVAILABLE IN CERTAIN MARKETS, OR AT ALL. THIS COULD REQUIRE THE RESTRUCTURING OF THE BLOCKCHAIN TERMINAL OR RESULT ITS UNAVAILABILITY IN ALL OR CERTAIN RESPECTS.

BCT INC AND ITS AFFILIATES, INCLUDING CG BLOCKCHAIN, HAVE BEEN USING PROCEEDS OF THE SALE OF BCT TOKENS IN THE FURTHERANCE OF THE DEVELOPMENT OF THE BLOCKCHAIN TERMINAL, COMPLIANCEGUARD AND OTHER APPLICATIONS THAT MAY BE USED ON THE BLOCKCHAIN TERMINAL, AND IN THE FURTHERANCE OF A BUSINESS INFRASTRUCTURE TO SUPPORT SUCH DEVELOPMENTS. THERE CAN BE NO GUARANTEE THAT BCT INC WILL SELL A SUFFICIENT NUMBER OF BCT TOKENS TO RAISE ENOUGH CAPITAL TO REASONABLY SUPPORT THE CONTINUED DEVELOPMENT OF THE BLOCKCHAIN TERMINAL, AND ASSOCIATED PRODUCTS, AND SUPPORT THE DELIVERY THEREOF, OR THAT EVEN IF THE MAXIMUM NUMBER OF BCT TOKENS AVAILABLE FOR SALE IS SOLD THAT BCT INC AND AFFILIATE MANAGEMENT WILL DEPLOY THE PROCEEDS IN A SUFFICIENT MANNER TO SUPPORT THE CONTINUED DEVELOPMENT OF THE BLOCKCHAIN TERMINAL AND ASSOCIATED PRODUCTS.

CG BLOCKCHAIN AND ITS AFFILIATES RESERVE THE RIGHT TO REVISE THIS WHITEPAPER FROM TIME TO TIME IN THEIR SOLE DISCRETION. ANY REVISIONS TO THIS WHITEPAPER WILL BE MADE AVAILABLE ON BCT INC’S WEBSITE.

BEFORE AN INVESTOR ACQUIRES BCT TOKENS, BCT INC MAY (IN ITS SOLE AND ABSOLUTE DISCRETION) REQUEST THAT SUCH POTENTIAL INVESTOR PROVIDE CERTAIN INFORMATION AND DOCUMENTATION FOR THE PURPOSES OF COMPLYING WITH ANY “KNOW YOUR CUSTOMER” ANTI-MONEY LAUNDERING OR SIMILAR OBLIGATIONS TO WHICH BCT INC MAY BE SUBJECT; AND DETERMINE THAT IT IS NECESSARY TO OBTAIN CERTAIN OTHER INFORMATION ABOUT SUCH INVESTOR IN ORDER TO COMPLY WITH APPLICABLE LAWS AND REGULATIONS IN CONNECTION WITH THE SALE OF BCT TOKENS. POTENTIAL INVESTORS SHALL BE SUBJECT TO SUCH OTHER DUE DILIGENCE AS BCT INC DEEMS NECESSARY OR APPROPRIATE IN ITS SOLE AND ABSOLUTE DISCRETION. FURTHER, BCT INC RESERVES THE RIGHT IN ITS SOLE AND ABSOLUTE DISCRETION TO REFUSE TO SELL TO ANY POTENTIAL INVESTOR BCT TOKENS.