Bitgo's Whitepaper: The Gold Standard in Crypto-Assets (English ／ 中文)

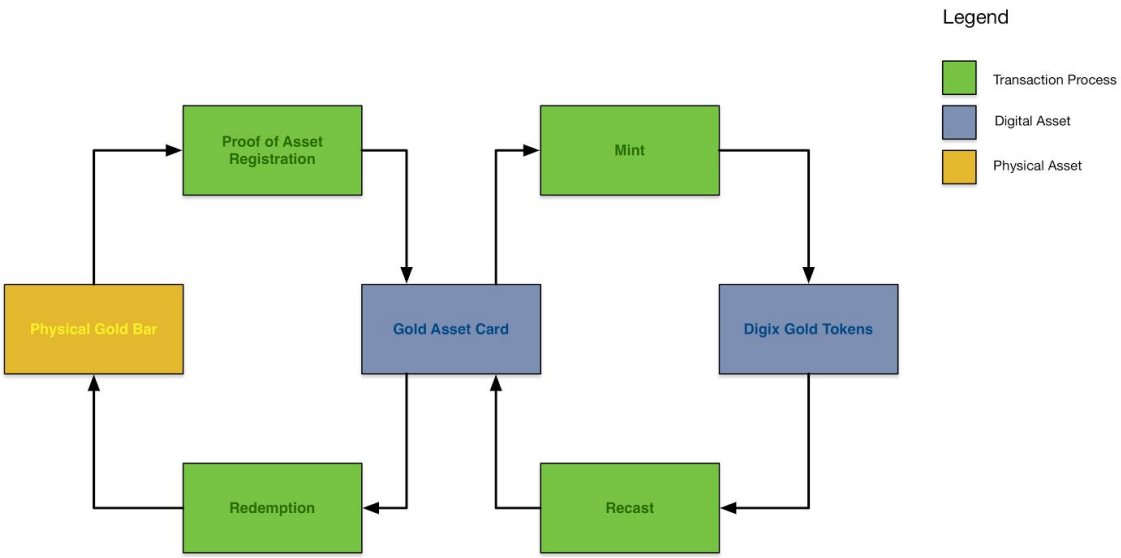
prepared by:
Anthony C. Eufemio <ace@BGC.io>
Kai C. Chng <kcchng@BGC.io>
Shaun Djie <shaundjie@dgx.io>
January 2018
Version 1.03

Abstract

Bitgo provides a use case for the tokenisation and documentation of physical assets through its **Proof of Asset (PoA)** protocol. The PoA protocol utilises Ethereum[1] and the InterPlanetary Files System (IPFS)[2] to track an asset through its chain of custody. This allows for the open and public verification of an asset's existence without a centralised database. Bitgo also offers an API allowing other applications to be built on top of our asset tokenisation service.

Technical Overview:

Product Life Cycle



[1] "[English] White Paper · ethereum/wiki Wiki · GitHub." 2014. 29 Dec. 2015

[2] Benet, Juan. (September 11 2015) "The IPFS Project - How it works". IPFS

Key Products

1. **Proof of Asset (PoA) Asset Cards**

   PoA Asset Cards consist of the below information permanently uploaded onto the decentralised database:

- Time Stamp of card creation
- SKU of the gold bar
- Bar Serial number
- Chain of Custody digital signatures (Vendor, Custodian, Auditor)
- Purchase Receipt
- Audit Documentation
- Depository Receipt
- Storage fees due

   PoA Asset Cards are kept in an Ethereum Wallet.

2. **Bitgo Tokens (BGC)**

   BGC Tokens are minted via a Minter Smart Contract. Each BGC token represents 1g of Gold and divisible to 0.001g. For every PoA Card that is sent to the Minter Smart Contract, BGC tokens will be issued in return. For instance, a 100g PoA Card sent to the Minter Smart Contract returns 100 BGC tokens to the user.

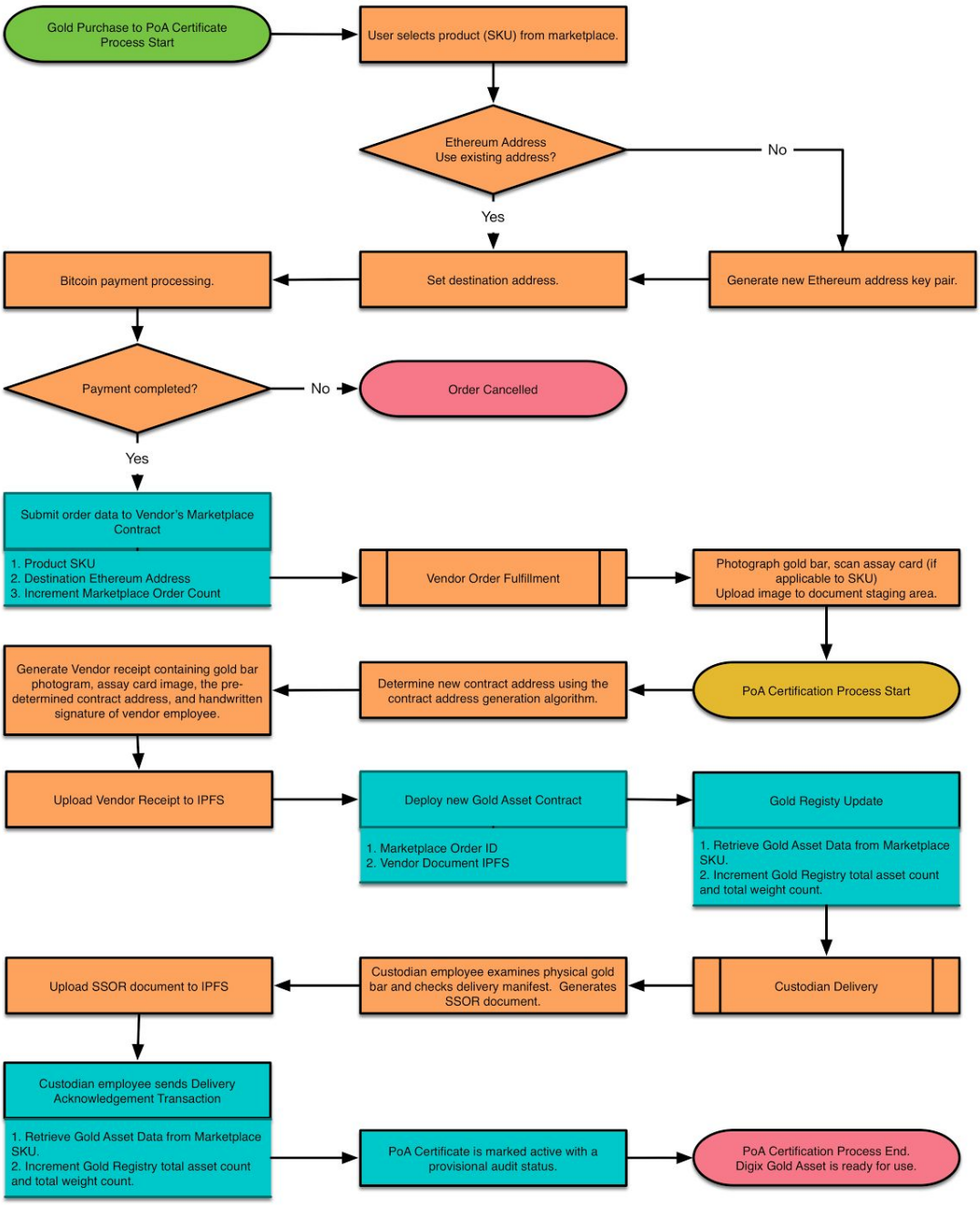
   Bitgo Tokens are held in an Ethereum Wallet.

Key Processes

There are 3 modular processes that Bitgo uses to provide a proof of existence and fungibility for an asset, 1 for redemption of physical assets, and 1 that encourages Ðapp Development. Those processes consist of:

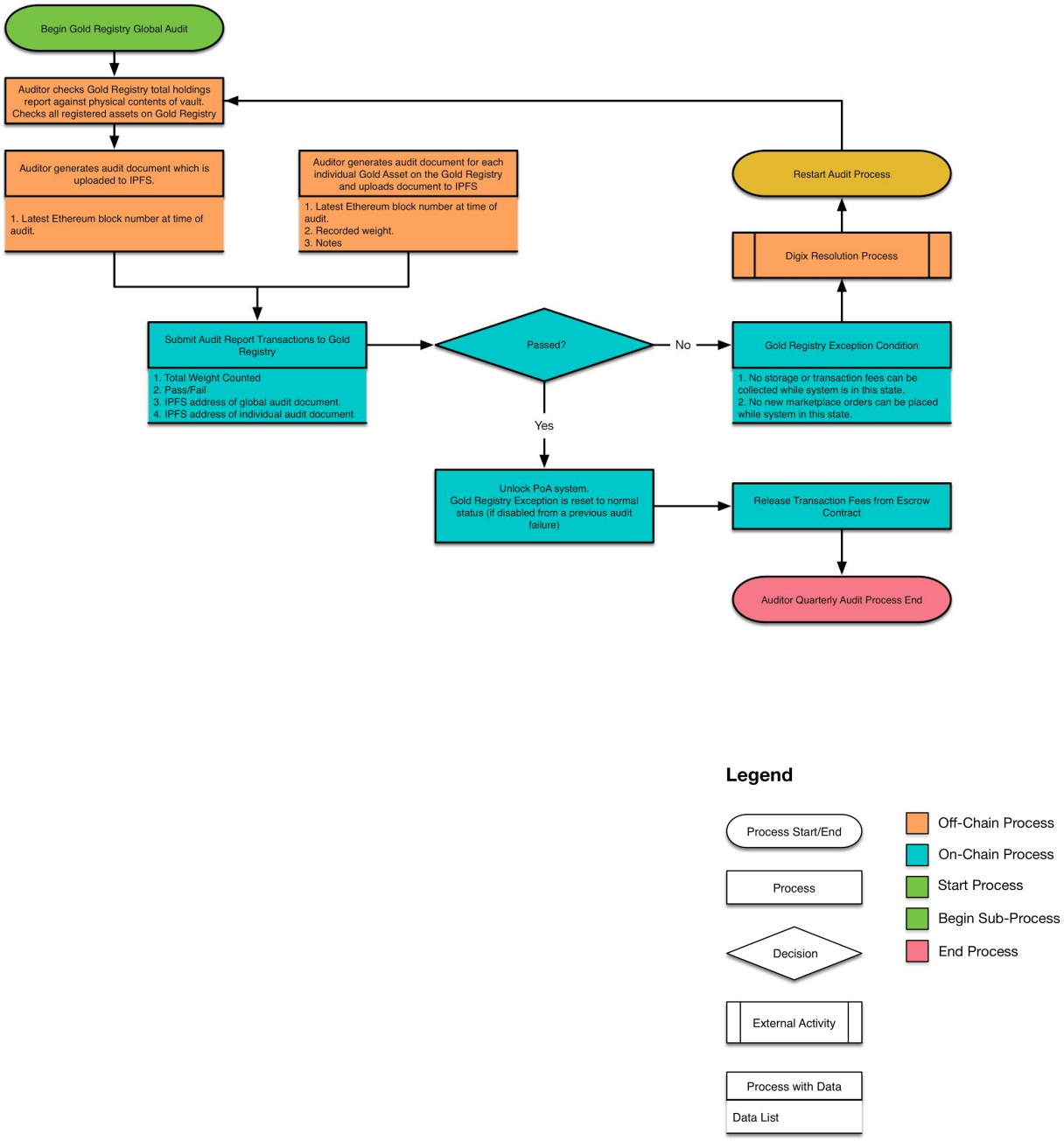
1. **Proof of Asset (PoA) Verification** process which records and provides an audit trail of an asset on Ethereum to create PoA Asset Cards. The asset cards are certified using sequential digital signatures from the entities in the chain of custody, namely, the **Vendor, Custodian**, **Auditor**, which are further validated with proof of purchase and depository receipts provided and uploaded onto IPFS for permanent record (Fig i).

Figure i: Bitgo Asset Registration Process



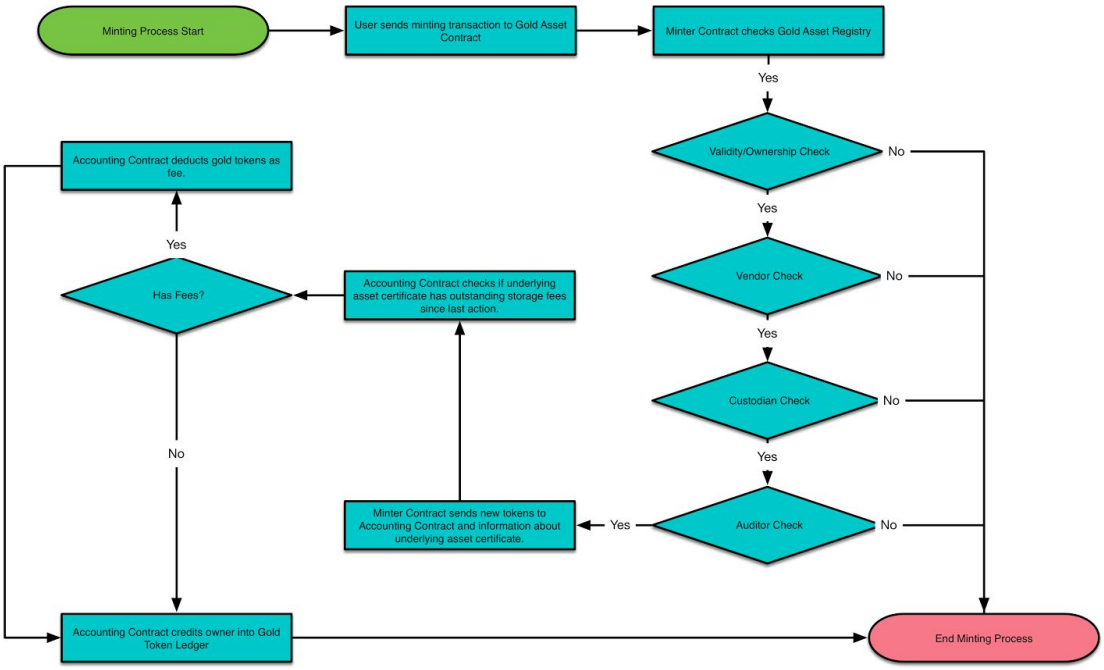
The PoA Verification contains a sub process for regular audits as shown in (Fig ii).

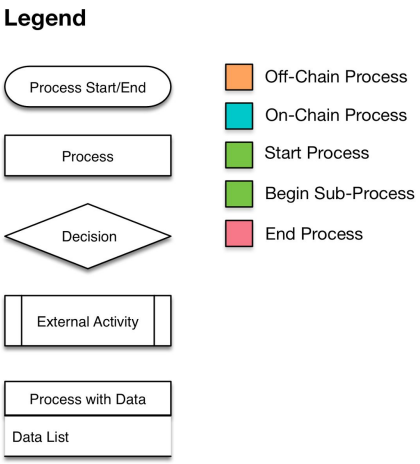
Figure ii: Audit Process



2. **Minter Smart Contract** to create fungible BGC tokens, that accepts or holds PoA Asset Cards in exchange for BGC tokens (Fig iii).

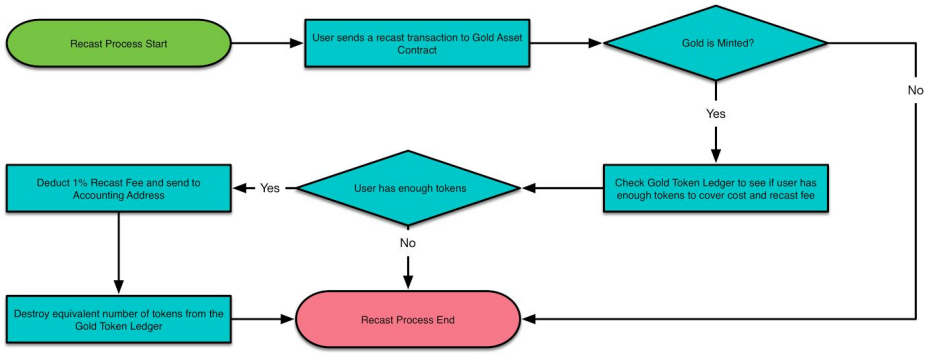
Figure iii: Minting Bitgo Gold Asset Cards into Bitgo Gold Tokens





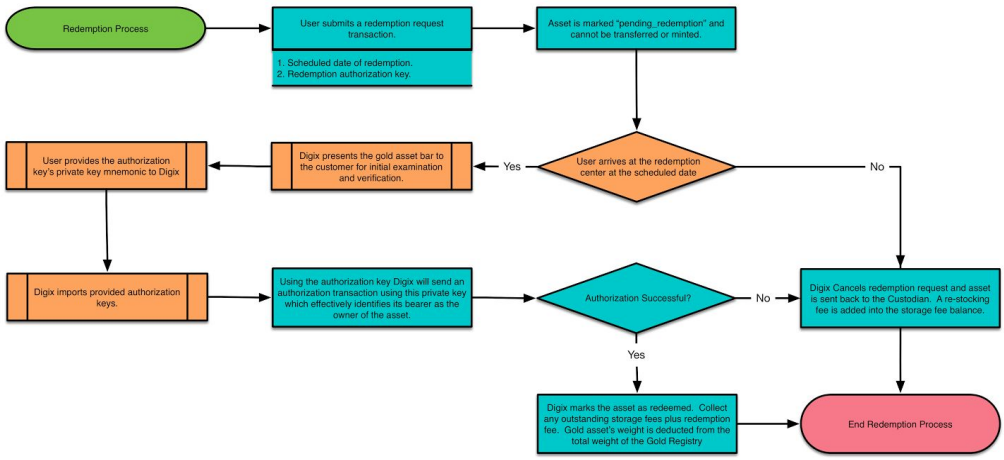
3. **Recaster Smart Contract**, which is used to exchange BGC tokens back into PoA Asset cards. (Fig iv).

Figure iv: Recasting Bitgo Gold Tokens into Bitgo Gold Asset Cards



4. **Redemption Process**, for redeeming physical gold bar with PoA Asset cards. (Fig V).

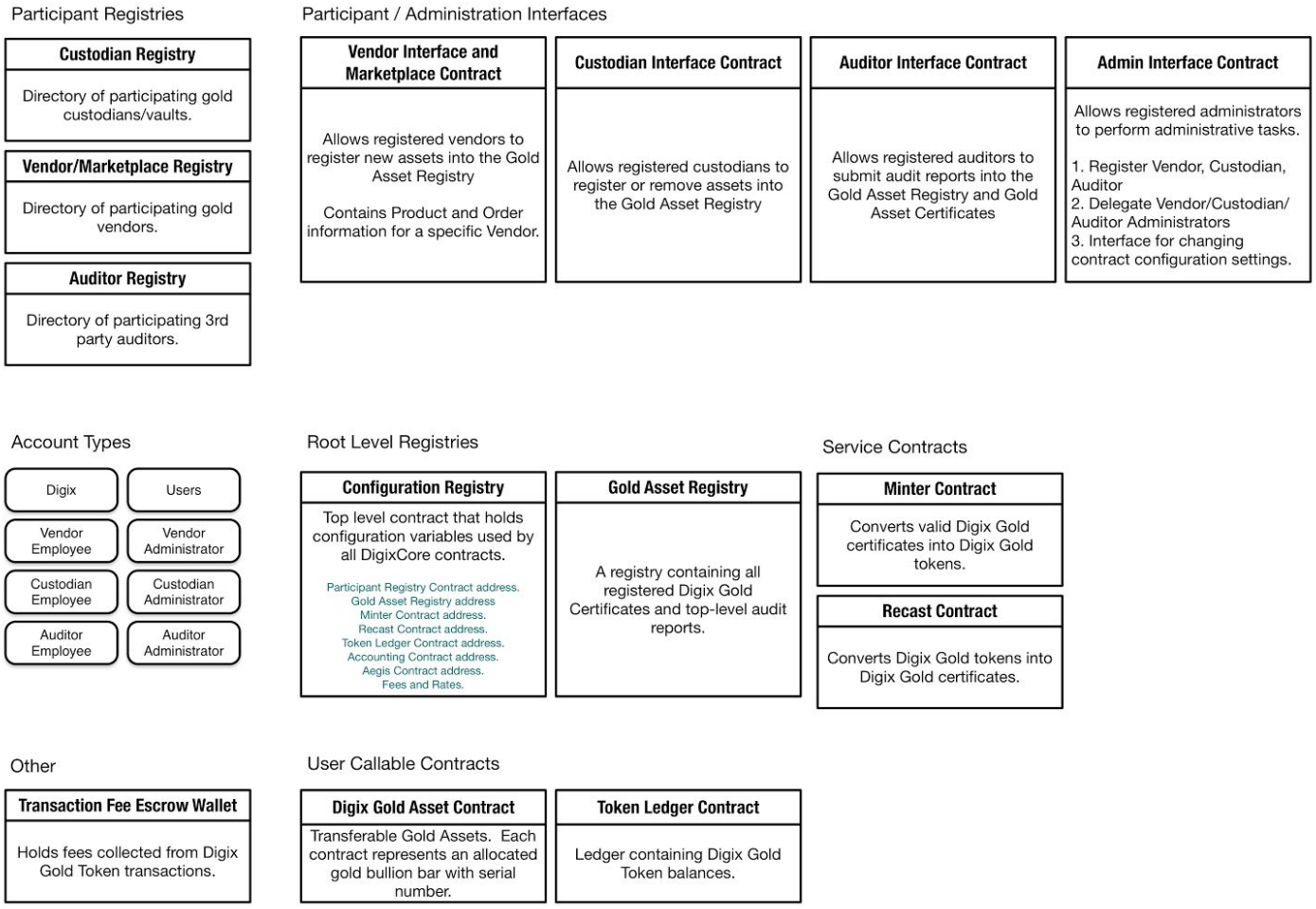
Figure V: Bitgo Gold Redemption and Token Based User Identification



5. **Generic I/O Contracts,** allowing developers to utilize PoA Cards or BGC tokens for Đapp development.

Ethereum Smart Contracts Stack

The diagram below shows the individual Bitgo smart contracts deployed on the Ethereum



Bitgo's Proof of Asset Participants
(Blockchain Oracle Entities)

Asset Vendor

ValueMax Singapore, a publicly listed company, supplies London Bullion Market Association (LBMA[3]) certified gold bullion bars through the Bitgo Marketplace. Established in 1988, they provide pawnbroking services, retail and trading of pre-owned jewellery, gold and luxury timepieces.

Independent Auditor

Bureau Veritas Inspectorate will carry out quarterly checks on the quality and quantity at our custodian vault to ensure accounting is upheld. They are a multinational group with capabilities in an extensive range of commodities, providing independent inspection, sampling and testing services of precious metals.

Every gold bullion is rigorously tested with precision instruments at Audit. We perform such measurements using Ultrasonic Gauge Measurements (UTM) and densometers. UTM is a method of performing non-destructive measurement (gauging) of the local thickness of a solid element basing on the time taken by the ultrasound wave to return to the surface. Densometers are devices that measure the density of objects with water displacement.

Participating Custodian Vault

Malca-Amit's state of the art facility near Singapore Changi International Airport is located in the Le Freeport of Singapore, a 25,000 sqm high-security and climate-controlled facility featuring cutting edge security technologies enhanced by green building engineering.

Multi-party Trust Mechanism

The Bitgo system relies on multiple independent participants to provide a transparent platform for the tokenization of physical assets. We can assume that miners in a Proof of Work based crypto-currency system will act rationally, that is, that they would act in a way to maximize and protect their long term profits by performing their role of transaction verification. We assume that a cartel of rational miners would not collude to perform double spending attacks as such attacks would cause reputational damage to the entire system. We must therefore assume that in the Bitgo system which is the tri-party system consisting of asset providing vendors, the asset custodian in charge of storing and securing the asset from theft, and the auditor in charge of

[3] "LBMA - FAQs". The London Bullion Market Association.

ensuring the authenticity of the reported assets in custody are all acting in a rational manner who are trying to maximize their profits from the fees that they collect for their service.

Mitigating Potential Points of Failure with Real World Governance

Dishonest Entities and collusion in the chain of custody

Bitgo works with entities in jurisdictions that provide stringent regulatory oversight and corporate governance. The entities we have engaged with are either publicly listed or well known in the industry for providing their niche service. Each entity that we have engaged with performs a separate function to prevent cheating. For instance, the asset vendor for physical assets cannot also be the asset custodian. The interest in the service has to be independent of one another. While the risk of collusion is a real possibility, it is at the cost of severe reputational and legal damages to the colluding participants. As these entities provide similar other services to other customers and such reputational and legal damages to their core business would be detrimental to their business, we can make a fair assumption that they will act in a rational manner.

Key Benefits

No centralised database management of Crypto Asset records

All chain of custody information is fully managed by the Ethereum blockchain. This blockchain ledger is immutable with data upload taking significantly less time than on the Bitcoin blockchain.[4]

No Web-based log-in

There is no web form log-in. Users will download desktop clients from Bitgo. The application itself can also be compiled from source on Github and is publicly auditable.[5] There is significantly less chance of a Man in the Middle attack compared to traditional user web-based log-in.[5]

Secure Cold Storage of Crypto-Assets

Bitgo's Aegis Vaults is a cold storage wallet custodial service for crypto-assets and crypto currencies on Ethereum.

Perpetual Existence of Digital Assets

---

[4] CryptoBond. (September 16, 2015) Why Is Ethereum Different to Bitcoin. CryptoCompare
[5] Hjemlvik, Erik. (March 27, 2011) Network Security Blog. "Network Forensic Analysis of SSL MITM Attacks". NETRESEC

All asset data is recorded on the blockchain and exists indefinitely. Even if Bitgo folds, every proof generated can be verified and are admissible in a court of law in the applicable jurisdiction.

Ex post facto Incentivization Mechanism

The Proof of Asset process requires that regular quarterly or more frequent audits to be performed by a 3rd party auditor on the entire collection of gold assets held at the custodian vaults. The auditor performs a complete audit of each gold bar which includes verification of its authenticity, weight, and physical examination to detect anomalies or defects. The auditor submits a record on the Gold Registry contract for each and every single bar that has been audited, which contains an IPFS reference to a signed paper documentation, the auditor's Ethereum identity, and a pass or fail result.

Bitgo receives its revenues through the collection of transaction fees paid in the form of Bitgo gold tokens. These tokens are held in an escrow contract which can only release the tokens to a specified address after the successful completion of a 3rd party audit.

Generic I/O Contracts and Đapp Development Opportunities

The generic I/O contract provided at Bitgo allows developers to utilize PoA Asset Cards or Bitgo tokens for Đapp development and event logging. Our vision is to create an ecosystem for developers to utilize BGC tokens as a framework for various Đapp developments. Code samples will be provided on our Github.

Wealth Inheritance

Dead man's switch can be built as a service to allow wealth to be passed on in the form of Crypto Assets to the mentioned Ethereum address under the Bitgo system.

Gamification

In legal jurisdictions, BGC tokens can be used like bitcoin to facilitate in game currency or as gaming tokens.[6] The PoA protocol can also be used for the issuance of digital gaming assets.[7]

Escrow

BGC tokens can provide a better and less volatile store of value for Escrow services on the blockchain.

---

[6] Farivar, Cyrus (January 22, 2013). "Bitcoin-based casino rakes in more than $500,000 profit in six months". Ars Technica.

[7] Addison, Ian. (December 22, 2015) "Game-changers FreeMyVunk and Bitgo allow video gamers ..." IB Times.

Crowdfunding

A Đapp can provide crowdfunding opportunities with crypto-currencies and crypto-assets, or offer convertibility of cryptocurrencies to BGC tokens as a hedge to price volatility.

Gold Backed Crypto Currency Developments

Cryptocurrencies can stake a portion of its value with BGC Gold tokens and Gold Assets, backing its value with Gold.

Crypto Exchanges and Wealth Management Đapps

When exchanges integrate BGC tokens as a cryptocurrency pair, they will be able to offer a gold hedge to cryptocurrencies as part of their service offering. Wealth management services that adjusts your cryptocurrency / crypto asset holdings can be developed to manage an individual's crypto financial risk profile.

P2P Lending and Microfinance

Đapps can utilize BGC Gold for peer to peer lending. A borrower can call for funding through a Đapp based on his risk profile and reputation and negotiate a rate of return on the borrowed funds. Interest / yield payments can be serviced at regular intervals with a penalty system in place for late payments. This has already been done with bitcoin[8], but due to the price volatility of cryptocurrencies, lenders may lose more of their asset value than what can be earned from the interest during the period of the loan. The price stability of BGC Gold Tokens can facilitate the adoption rate of such services.

Collateral services

Privately held assets can be safely and efficiently used as collateral without going through lengthy verification process to ascertain an asset's existence and authenticity.

Conclusion

Bitgo will provide a transparent, audit friendly, safe protocol that leverages the full potential of Ethereum's decentralized consensus ecosystem and IPFS to facilitate crypto assets on the blockchain.

[8] Shieber, Jonathan (June 5, 2014). "BTCJam Brings Its Bitcoin-Based Lending Service To Emerging Markets". TechCrunch.