Digix's Whitepaper: The Gold Standard in Crypto-Assets

prepared by:
Anthony C. Eufemio <ace@dgx.io>
Kai C. Chng <kcchng@dgx.io>
Shaun Djie <shaundjie@dgx.io>
January 2016
Version 1.02

Abstract

Digix 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. Digix also offers an API allowing other applications to be built on top of our asset tokenisation service.

Technical Overview:

Product Life Cycle

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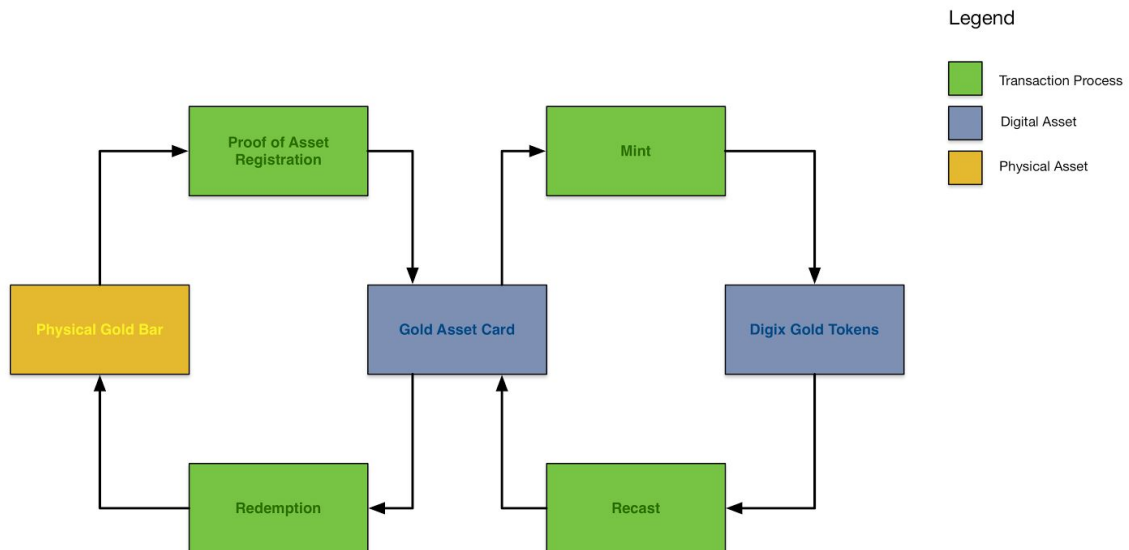
[1] "[English] White Paper · ethereum/wiki Wiki · GitHub." 2014. 29 Dec. 2015

[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. **Digix Tokens (DGX)**

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

   Digix Tokens are held in an Ethereum Wallet.

Key Processes

There are 3 modular processes that Digix 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:
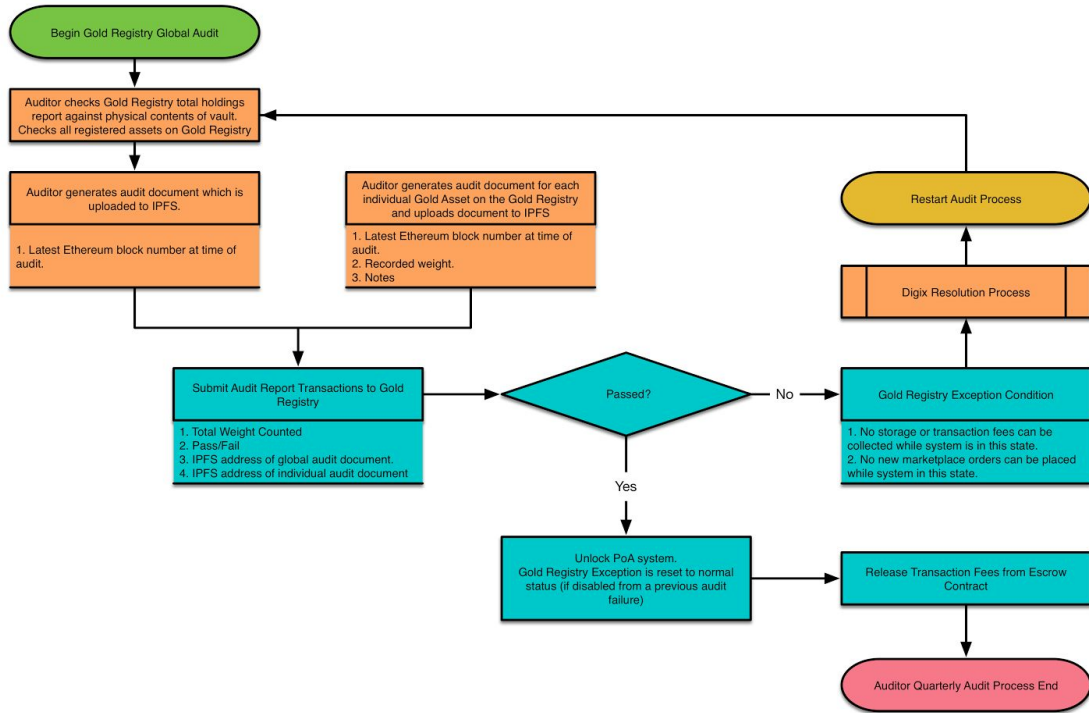
1. **Proof of Asset (PoA) Verification** process which records and provides an audit trail of an asset on Ethereum to create PoA Asset Cards. The asset cards are certified using sequential digital signatures from the entities in the chain of custody, namely, the **Vendor, Custodian**, **Auditor**, which are further validated with proof of purchase and depository receipts provided and uploaded onto IPFS for permanent record (Fig i).
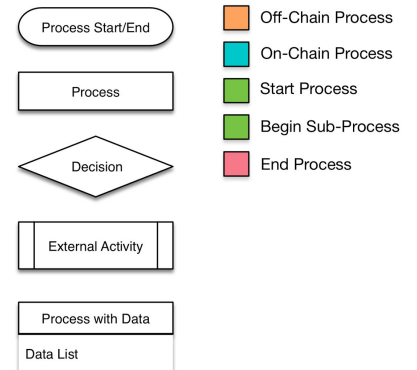
Figure i: Digix Asset Registration Process

- Gold Purchase to PoA Certificate Process Start
- User selects product (SKU) from marketplace.
- Ethereum Address Use existing address? — No → Generate new Ethereum address key pair.
- Yes → Set destination address.
- Bitcoin payment processing.
- Payment completed? — No → Order Cancelled
- Yes →

Submit order data to Vendor's Marketplace Contract
1. Product SKU
2. Destination Ethereum Address
3. Increment Marketplace Order Count

Vendor Order Fulfillment

Photograph gold bar, scan assay card (if applicable to SKU) Upload image to document staging area.

PoA Certification Process Start

Determine new contract address using the contract address generation algorithm.

Generate Vendor receipt containing gold bar photogram, assay card image, the pre-determined contract address, and handwritten signature of vendor employee.

Upload Vendor Receipt to IPFS

Deploy new Gold Asset Contract
1. Marketplace Order ID
2. Vendor Document IPFS

Gold Registy Update
1. Retrieve Gold Asset Data from Marketplace SKU.
2. Increment Gold Registry total asset count and total weight count.

Custodian Delivery

Custodian employee examines physical gold bar and checks delivery manifest. Generates SSOR document.

Upload SSOR document to IPFS

Custodian employee sends Delivery Acknowledgement Transaction
1. Retrieve Gold Asset Data from Marketplace SKU.
2. Increment Gold Registry total asset count and total weight count.

PoA Certificate is marked active with a provisional audit status.

PoA Certification Process End. Digix Gold Asset is ready for use.

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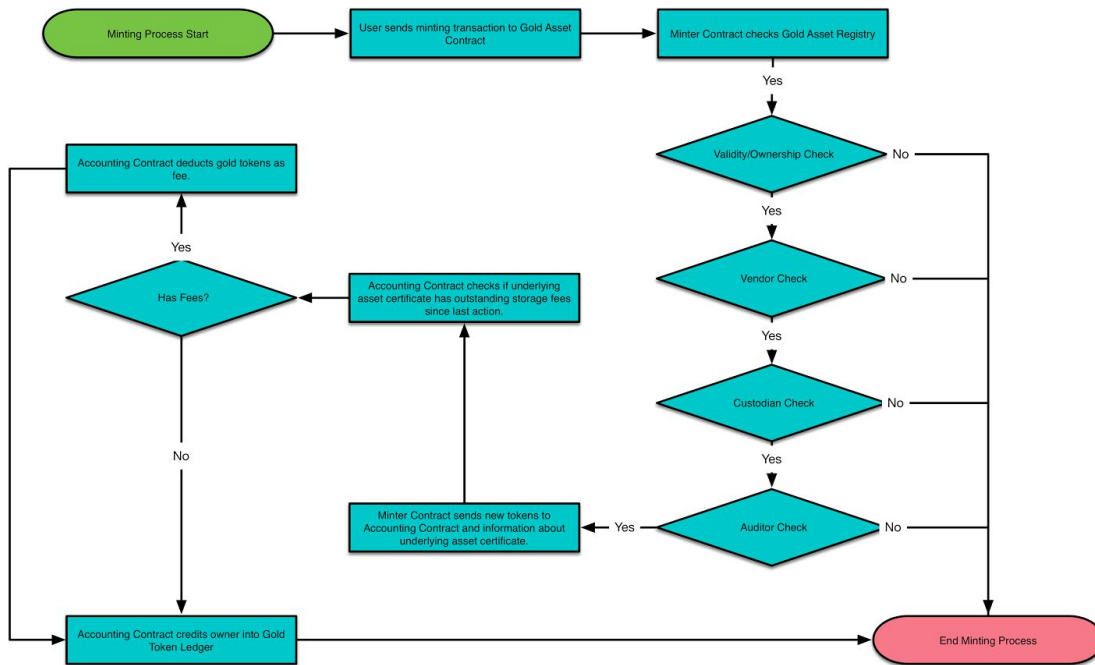
Figure ii: Audit Process

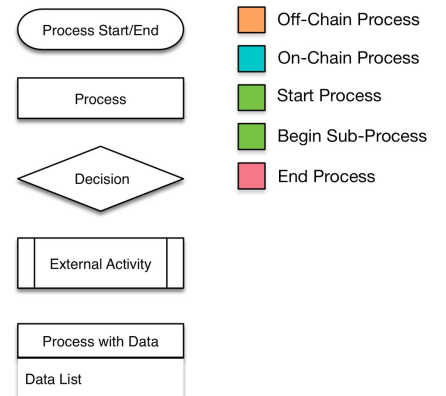Begin Gold Registry Global Audit

Auditor checks Gold Registry total holdings report against physical contents of vault. Checks all registered assets on Gold Registry

Auditor generates audit document which is uploaded to IPFS.

1. Latest Ethereum block number at time of audit.

Auditor generates audit document for each individual Gold Asset on the Gold Registry and uploads document to IPFS

1. Latest Ethereum block number at time of audit.
2. Recorded weight.
3. Notes

Restart Audit Process

Digix Resolution Process

Submit Audit Report Transactions to Gold Registry

1. Total Weight Counted
2. Pass/Fail
3. IPFS address of global audit document.
4. IPFS address of individual audit document

Passed?

No

Gold Registry Exception Condition

1. No storage or transaction fees can be collected while system is in this state.
2. No new marketplace orders can be placed while system in this state.

Yes

Unlock PoA system.
Gold Registry Exception is reset to normal status (if disabled from a previous audit failure)

Release Transaction Fees from Escrow Contract

Auditor Quarterly Audit Process End

Legend

Process Start/End

Process

Decision

External Activity

Process with Data
Data List

Off-Chain Process

On-Chain Process

Start Process

Begin Sub-Process

End Process

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

Figure iii: Minting Digix Gold Asset Cards into Digix Gold Tokens
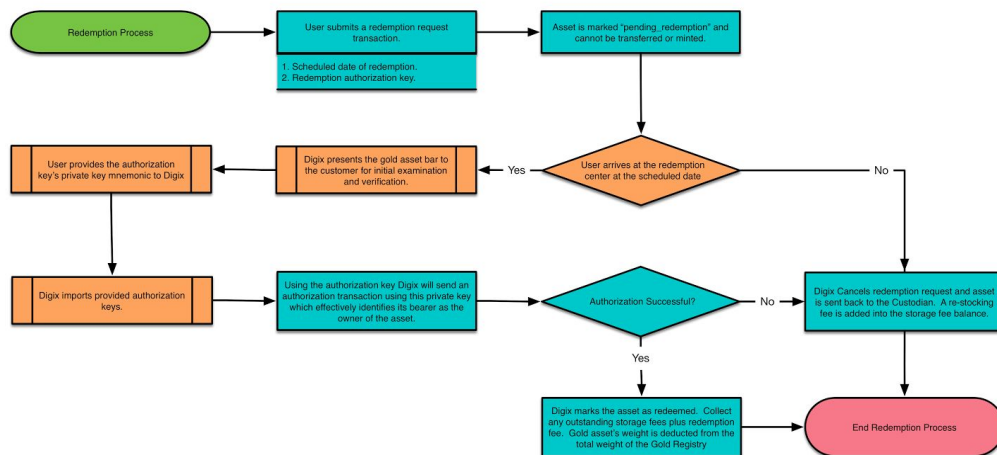
3. **Recaster Smart Contract**, which is used to exchange DGX tokens back into PoA Asset cards. (Fig iv).

Figure iv: Recasting Digix Gold Tokens into Digix Gold Asset Cards
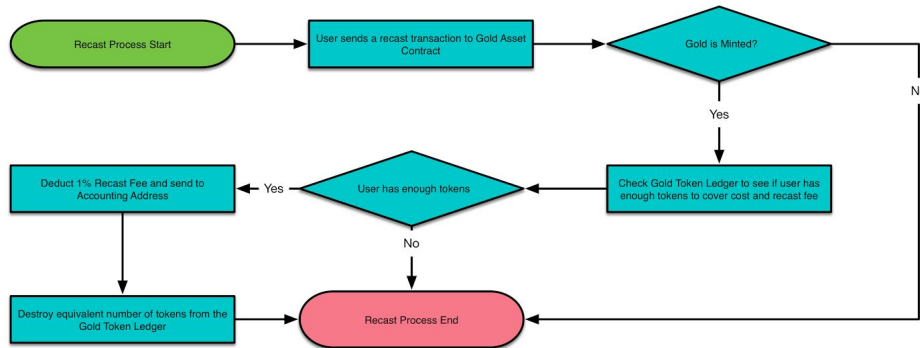
4. **Redemption Process**, for redeeming physical gold bar with PoA Asset cards. (Fig V).

Figure V: Digix Gold Redemption and Token Based User Identification

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

Ethereum Smart Contracts Stack

The diagram below shows the individual Digix smart contracts deployed on the Ethereum blockchain that make up the core processes above.

Participant Registries

Custodian Registry
Directory of participating gold custodians/vaults.

Vendor/Marketplace Registry
Directory of participating gold vendors.

Auditor Registry
Directory of participating 3rd party auditors.

Participant / Administration Interfaces

Vendor Interface and Marketplace Contract
Allows registered vendors to register new assets into the Gold Asset Registry

Contains Product and Order information for a specific Vendor.

Custodian Interface Contract
Allows registered custodians to register or remove assets into the Gold Asset Registry

Auditor Interface Contract
Allows registered auditors to submit audit reports into the Gold Asset Registry and Gold Asset Certificates

Admin Interface Contract
Allows registered administrators to perform administrative tasks.

1. Register Vendor, Custodian, Auditor
2. Delegate Vendor/Custodian/ Auditor Administrators
3. Interface for changing contract configuration settings.

Account Types

Digix	Users
Vendor Employee	Vendor Administrator
Custodian Employee	Custodian Administrator
Auditor Employee	Auditor Administrator

Root Level Registries

Configuration Registry
Top level contract that holds configuration variables used by all DigixCore contracts.

Participant Registry Contract address.
Gold Asset Registry address
Minter Contract address.
Recast Contract address.
Token Ledger Contract address.
Accounting Contract address.
Aegis Contract address.
Fees and Rates.

Gold Asset Registry
A registry containing all registered Digix Gold Certificates and top-level audit reports.

Service Contracts

Minter Contract
Converts valid Digix Gold certificates into Digix Gold tokens.

Recast Contract
Converts Digix Gold tokens into Digix Gold certificates.

Other

Transaction Fee Escrow Wallet
Holds fees collected from Digix Gold Token transactions.

User Callable Contracts

Digix Gold Asset Contract
Transferable Gold Assets. Each contract represents an allocated gold bullion bar with serial number.

Token Ledger Contract
Ledger containing Digix Gold Token balances.

<div align="center">

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

</div>

Asset Vendor

ValueMax Singapore, a publicly listed company, supplies London Bullion Market Association (LBMA[3]) certified gold bullion bars through the Digix 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.

<div align="center">

Multi-party Trust Mechanism

</div>

The Digix 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 Digix 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

Digix 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 Digix. 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

Digix'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 Digix 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.

Digix receives its revenues through the collection of transaction fees paid in the form of Digix 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 Digix allows developers to utilize PoA Asset Cards or Digix tokens for Đapp development and event logging. Our vision is to create an ecosystem for developers to utilize DGX 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 Digix system.

Gamification

In legal jurisdictions, DGX 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

DGX 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 Digix allow video gamers ..." IB Times.

Crowdfunding

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

Gold Backed Crypto Currency Developments

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

Crypto Exchanges and Wealth Management Đapps

When exchanges integrate DGX 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 DGX 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 DGX 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

Digix 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.