JIBREL NETWORK

MAY 2017

SECOND DRAFT

YAZAN BARGHUTHI
yazan@jibrel.network

VICTOR MEZRIN
victor@jibrel.network

ABSTRACT

the jibrel network aims to facilitate the digitization[1], listing and trading of traditional assets[2] such as currencies, bonds and other financial instruments, on the blockchain. The *jibrel decentral bank* will allow platform users to deposit cash, money market instruments or create their own Crypto Depository Receipts (CryDRs) and benefit from on-chain / off-chain arbitrage. Decentralized organizations and funds that are overexposed in digital currencies can hedge their positions and protect their funding with stable assets. Furthermore, jibrel will provide developers with a complete platform to build tools and applications for transacting, investing and hedging, through leveraging traditional asset-backed tokens.

In addition, jibrel will enable instant, near-zero fee, global payments and remittances in the form of fiat[3] to fiat transactions that can be undertaken through peer to peer, business to business or consumer to merchant channels.

This white paper outlines the core components comprising jibrel, how they interact, and aims to demonstrate how the network can be built-out efficiently using existing infrastructure.

1.INTRODUCTION

Since their introduction with Bitcoin in 2009[1], blockchains have unlocked tremendous value. With this new technology, we can verify and commit transactions in an immutable decentralized ledger, or implemented more broadly, achieve decentralized consensus.

This incredible innovation is currently transforming our world by eroding the need for trusted intermediaries, settlement / clearing offices, and middle-man service providers across a wide range of industries and sectors.

That being said, due to limited adoption at an institutional level, most of the crypto-economy's value remains siloed by use-case or geography. In addition, widespread systemic risk exists due to the bottlenecks imposed by these siloes in the form of challenges and limitations in converting between traditional assets and digital assets.

Given the disconnect between the traditional economy and the cryptoeconomy, the same challenges plaguing the former still persist in the latter. Users wishing to transfer traditional currency between one another still face the time delays and fees imposed by relying on a combination of cryptocurrency exchanges, traditional financial institutions, as well as payment processors.

Moreover, traditional individual and institutional investors, who could facilitate the quick movement of traditional assets off-chain are deterred from participating due to the fundamental incompatibilities that exist - most notably, a lack of transparency and extreme market volatility[2].

Finally, decentralized organizations, who raise funding through crowd sales, as well as decentralized funds and crypto-investors, who are overexposed in digital assets and cryptocurrencies, have limited options to diversify into traditional holdings.

The risks are compounded further by the fact that digital currencies play a multifaceted role, they are used to reward miners for facilitating transactions; as a means of transferring value; as a speculative investment tool; and most recently, to crowdfund and run decentralized organizations and applications (e.g. decentralized computing[3], decentralized storage[4]).

In traditional finance, different instruments are used for these functions and are regulated accordingly. This helps manage systemic risk. Until decentralized regulatory consensus protocols are fully built-out, the cryptoeconomy faces security and fraud risk, in the form of unregulated exchanges; market risks, resulting from extremely volatile currencies that are used beyond their

[1] Conversion to a cryptocurrency or token
[2] Cash, bonds and equities
[3] Government-backed currencies that are declared to be a legal tender without the backing of an underlying physical commodity

architectured purpose; and systemic risks arising from crowd-funds stored in volatile digital currencies and subsequently locked into smart contracts[4].

This paper analyzes the limitations and challenges of the current environment and proposes an approach that leverages existing infrastructure to provide a solution for all stakeholders.

2. TRADITIONAL ASSET-BACKED TOKENS

The core stakeholders in the jibrel ecosystem are; non-investment users, who seek to benefit from the value unlocked by cryptocurrencies and blockchain technology, such as low remittance fees and instant transfers; traditional investors, who seek to benefit from the high returns of the emerging cryptoeconomy; and decentralized organizations / funds and crypto-investors, who seek to diversify their crypto-holdings with stable low-yield assets, on-chain, as to remain transparent to crowd-funders.

The needs of all stakeholders could be successfully met by bringing the stability of traditional financial instruments to the blockchain. This can be accomplished by minting tethered tokens with one-to-one backing of the underlying traditional asset they represent. Using such a method, tethered tokens can be used to denote a currency[5] or even a commodity[6].

By developing a 'guarantor' that houses traditional assets and issues tokens representing ownership of the underlying assets, one can enable a wide-range of currencies, commodities, money market instruments and other financial tools, to be openly traded on-chain.

3. SYSTEM ARCHITECTURE

The following section outlines the key components of the jibrel network and what is required to facilitate putting traditional assets on-chain.

3.1 Public Blockchain

While reliance on another blockchain imposes a long-list of new challenges and limitations, a public and secure blockchain is required for early versions of jibrel, until full cross-chain communication is feasible.

3.2 Cryptocurrency Exchanges

Cryptocurrency exchanges provided end-users with fiat accounts in their local currency and digital wallets to hold cryptocurrencies. User can buy, trade or transmit digital currency, easily converting between crypto and fiat currencies.

3.3 Tethered Tokens

Tethered tokens will be required to create traditional asset-backed tokens. For every traditional asset held a tethered token is minted. Upon the underlying asset being sold, the token is destroyed. .

3.4 Guarantor

In order to ensure tethered tokens hold their respective value, a guarantor is needed. The guarantor will hold traditional assets and issue their respective tethered tokens, as well as redeem and destroy tokens in return for the release / transfer of ownership of the underlying traditional asset.

3.5 Application Layer, Libraries & Templates

Once tethered tokens are established, an array of applications that leverages their capabilities can be developed, including payment processors, remittance wallets and trading platforms. To facilitate rapid application development, a dedicated application layer with user-friendly libraries and code templates will be required.

3.6 Ownership Transfers

Once a tethered token is issued, the underlying asset can be easily traded similar to any cryptocurrency. The high-level process is outlined below:

1. User sends FIAT to guarantor
2. Guarantor returns jFIAT
3. User pays merchant in jFIAT
4. Merchant redeems jFIAT
5. Guarantor sends FIAT to merchant account

With a guarantor backing the tethered token, with the promise to redeem for the underlying asset at a future point in time, the token can stay in the system and be used for on-chain and off-chain payments.

3.7 Fees & Charges

Transferring ownership of both digital and traditional assets have associated fees and charges that will need to be accounted.

3.8 Oversight / Regulation

Any on-chain transaction representing an off-chain transfer of ownership or value must satisfy international and local regulation and must be managed accordingly.

Regulatory protocols / governance tools should be put in place to ensure proper governance and oversight.

All transactions must satisfy KYC / AML regulations.

4 Projects are at risk of not materializing if their funding is reduced due to market downswings, potentially leading to insolvency

4. JIBREL NETWORK IMPLEMENTATION

This section outlines how each component will be implemented in the jibrel network.

4.1 Ethereum Blockchain

The selected blockchain must decouple mining rewards and the underlying transactions between the participants of the system. For this reason, Ethereum is well suited to form the foundation of jibrel's underlying architecture. Mining rewards will be in the form of Ethereum 'gas', while any tethered token will not be part of the mining process[7].

While jibrel is also suited to be built on Bitcoin's Omniprotocol, that approach is beyond the scope of this paper.

4.2 Crypto Depository Receipts (CryDR)

CryDRs are tethered tokens that represent ownership of an underlying traditional asset held by jibrel. In this paper, they are denoted as jAsset (e.g. jUSD, jEUR, jGBP). On release, jibrel will support six fiat currencies and two money market instruments, with plans to add additional financial instruments in the future.

4.2.1 Currencies / Fiat

The first iteration of the jibrel network aims to support USD, EUR, GBP, RUB, CNY, AED with additional currency support gradually added as strategic exchange partners are integrated.

4.2.2 Money Market Instruments

Stable low-yield assets are jibrel's core offering, crypto-investors will be able to purchase tokens tethered to US Treasury Bills and Zero-Coupon Certificates of Deposits. For the first iteration of the jibrel network, all money market instruments will incorporate an *automatic rollover* or *accrual* mechanism. Meaning, fiat received from matured investments, will be automatically redeployed in similar assets. Similarly, dividend or interest will be accrued until the underlying asset matures or is sold. In future versions, money market instruments will be configurable.

4.2.3 Other Financial Instruments

In the future, as traditional financial institutions are integrated into the jibrel platform, full support of other financial instruments can be rolled out, including listed and private equity.

4.2.4 Smart Compliance

Since CryDRs are fully programmable they can be embedded with regulation. Fiat currencies will be unrestricted, however the purchase and resale of other assets will need to be restricted by class and geography to be fully compliant. This logic is embedded in each CryDR.

4.3 Jibrel 'Decentral' Bank (JDB)

The JDB will receive / hold traditional assets on behalf of their owners and issue their respective CryDRs. Uponsends it to the owner's wallet. Upon redemption of a token, the token is destroyed and the underlying asset is transferred to the token holder.

While the JDB aims to be fully decentralized, until full on-chain integration of traditional financial institutions, large components of the system will need to be off-chain. Off-chain activity will require the input and oversight of local and international regulators.

For this reason, stakeholder interaction must be properly managed to ensure full regulatory compliance without sacrificing transparency and reliability. This will be achieved through *asset portals*, dedicated entities operating with full compliance in their respective geographies.

4.4 Asset Portals

Asset portals are used to undertake the necessary legal and financial steps to convert traditional assets into on-chain digital assets.

Fiat portals will be simple cryptocurrency exchanges. Strategic partnerships can be formed with existing exchanges while a dedicated jibrel exchange network with sufficient geographic reach can be built-out. In addition, by housing a portion of jibrel's fiat reserves in existing exchanges, transfer times and fees are significantly reduced whilst simultaneously providing exchanges with much needed liquidity.

Non-fiat portals will require off-chain presence to undertake the necessary due diligence and take ownership of non-fiat deposits.

In most geographies, asset portals will require brokerage and money transmitter licenses. In cases involving heavily regulated jurisdictions or more nuanced financial assets, full regulator involvement and oversight might be required.

As regulation evolves, asset portals will be able to decentralize and become community driven. Institutional investors and other financial institutions will be able to list their own traditional assets on-chain, using the jibrel platform.

4.5 Jibrel Network Token (JNT)

While non-fiat portals will charge *offline fees* in fiat currencies, the JDB's on-chain fees and commissions will be levied in the form of Jibrel Network Tokens (JNT).

JNT will be listed on ERC-20 compatible exchanges.

5. INFRASTRUCTURE

Critical data, such as user balances and transactions, will be stored on the blockchain while all other data is hosted on development servers.

Several development environments, tools and frameworks have already been developed to enable the rapid development of decentralized applications[8]. Jibrel will need to develop similar developer components, tools and frameworks to enable the widespread adoption and distribution of CryDRs.

Infrastructure will be required across two main dimensions, on-chain APIs and off-chain APIs / Utils.

5.1 On-chain Infrastructure

Only four key smart contracts will be required for the network to operate effectively.

5.1.1 CryDR Smart Contracts

Each asset registered with the JDB will have a CryDR issued in the form of a smart contract. CryDR smart contracts will be ERC-20 compliant. Forwarding CryDRs between user accounts is similar to forwarding other ERC-20 tokens between wallets.

5.1.2 Jibrel Decentral Bank Smart Contract

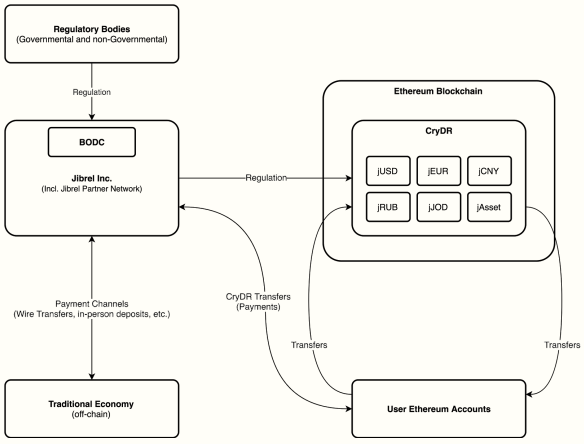
A dedicated JDB smart contract will regulate the work of CryDR Smart Contracts.

5.1.3 Board of Directors Smart Contract (BODC)

The Board of Directors smart contract (BODC) is the only mechanism to interact / influence the Jibrel Decentral Bank Contract.

BODC will be managed through a voting system, where members of the board can use their Ethereum accounts to vote on BODC actions. Storing and using private keys will be the responsibility of members. Ideally, the board will be composed of crypto thought-leaders and financial services experts.

Figure 1. Crypto Depository Receipts - General Workflow



5.1.4 Helpers / Utils (Auxiliary Smart Contracts)

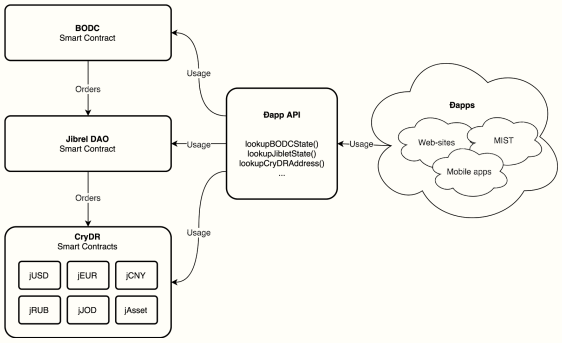
We will also need to create several auxiliary smart contracts to enable auxiliary functions such as switching between contracts running different versions and enabling additional API features.

Their detailed description is beyond the scope of this document.

5.2 Off-chain Infrastructure

In order to facilitate the widespread adoption of CryDRs as a transaction, investment and hedging tool, user-friendly libraries and code templates for application developers will be released.

Figure 2. Jibrel DApp API Workflow



5.2.1 Libraries & Templates

We expect that developers will use existing libraries to interact with Ethereum Blockchain (for example, JS web3). We will release wrappers for this library and code samples that will simplify the interaction with the JDB and CryDR smart contracts.

5.2.2 CryDR Explorers

Open-source explorers will be created, allowing users to view CryDR metadata and interact with the BODC as well as manually verify ownership of the underlying asset by the JDB.

5.2.3 Board of Director Tool-kit

Tools will be created to interface the internal IT infrastructure of CryDR Ltd with Ethereum blockchain. In particular, for the organization of interaction of the members of the board of directors with BODC and for operative monitoring of the state of the system.

6. SMART REGULATION IMPLEMENTATION

This section outlines in the implementation of CryDRs, Smart Regulation and Compliance

6.1 CryptoDepository Receipt (CryDR) Architecture

CryDRs themselves are smart contracts deployed to the Ethereum blockchain. To facilitate a robust and scalable system, CryDRs should satisfy multiple requirements:

High Compatibility: Should employ an ERC20 interface to be compatible with existing token management tools
Updatable Business Logic: Should be easily upgradable to keep up with evolving real-world rules and regulations
Immutability: Should be immutable once deployed
Migratable: Events and Storage should be stored separately
Interactivity: CryDRs should be able to interact with each other

6.2 Existing Methodologies

These technical requirements are difficult to achieve using the current Ethereum ecosystem.

Upgradable smart contracts implementations are quite complex, and while certain tools and methodologies exist, they each have their own limitations.

6.2.1 EVM *DELEGATECALL*

The first potential approach leverages opcode `DELEGATECALL` in Ethereum Virtual Machine (EVM).

While this is a powerful tool to update business logic, it has several drawbacks. Specifically, once deployed, the storage structure of the original smart contract must be maintained throughout updates. For this reason, this approach can only be employed in simple upgradable contract implementations and cannot be used for Jibrel's use-case.

6.2.2 Smart Contract Pruning

Another potential solution is the pruning of the contract and deploying another new contract to the same address, preserving Events and State. While this would be an ideal solution for the Jibrel Network, it has yet to be implemented in EVM.

6.3 Jibrel Network Approach

In building Jibrel, we leverage a more tedious but holistic solution - we deconstruct the whole system into multiple sophisticated smart contracts that interact with one another, but can provide seamless upgrades and updates.

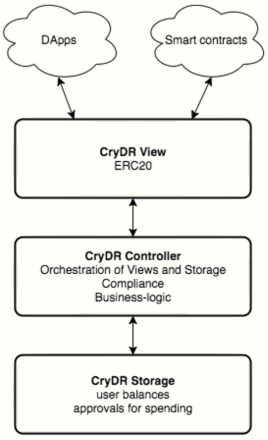
While more complex to implement, it provides a powerful backend for Jibrel DApps.

6.3.1 CryDR 3-Layer System

CryDRs are deconstructed into their critical components:

Storage - Houses all the data
View: Interface for third-party contracts and web-apps
Controller: Implements compliance and business logic, orchestrates storage and view contracts

Figure 3. Tiered Architecture

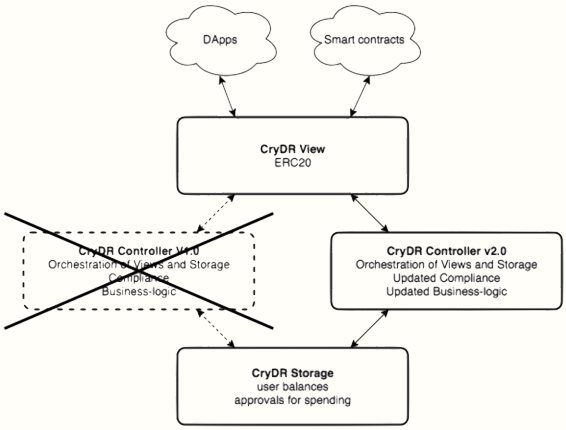


6.3.1.1 Updating Compliance

With this structure, we can easily deploy a new CryDR controller contract and configure view and storage contracts to use this new controller.

Effectively, this allows us to easily update the underlying compliance and business-logic powering CryDRs, what we refer to as Smart Regulation.

Figure 4. Controller Updates

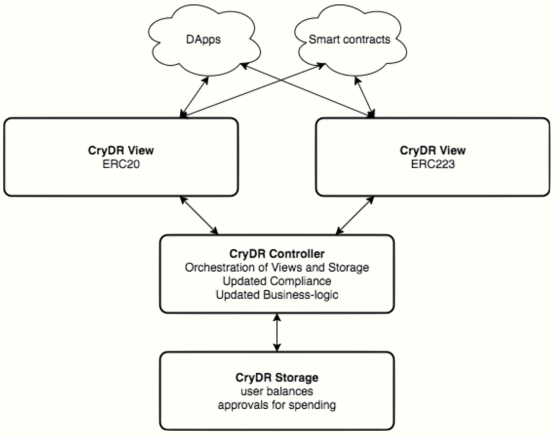


By facilitating a process that allows for business logic to be updated, the Jibrel Network ensures tokens can remain fully compliant by evolving with changes in real-world regulation.

6.3.1.2 Upgrading Interfaces

Using this architecture, we can also upgrade token interfaces seamlessly, such as providing additional support for new token standards (e.g. ERC223)

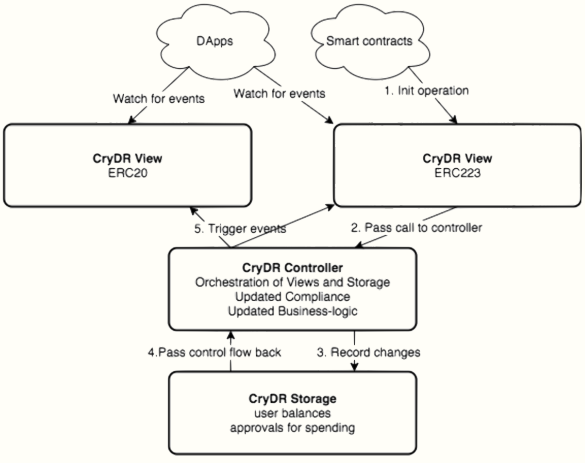
Figure 5. View Upgrades



When conducting such upgrades, CryDR storage remains unchanged / unaffected.

Since Views act as a tiered layer ahead of the controller, all Events remain intact during updates. A well implemented controller will trigger all connected views, so clients can receive all events.

Figure 6. Trigger Events



6.3.2 Smart Regulation Architecture

Implementing KYC/AML measures require strict and detailed account permissioning controls.
Smart contracts have inherited limitations, primarily, they are only able to access on-chain data, with calls to third-party services prohibited by design.

In order to access off-chain data, the data must first be pushed onto the blockchain in form of transactions.

Put simply, this means all compliance measures must be implemented on-chain via smart contracts.

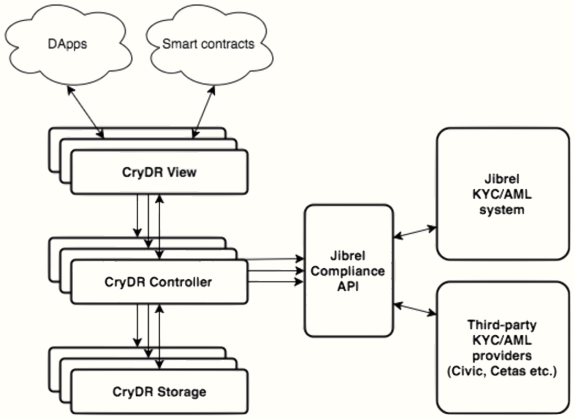
In order to implement KYC/AML measures we need to implement two solutions:

Data storage: To store user data on-chain
Rule Implementation: Apply KYC / AML rules on each transaction

Many projects address the first task. Such as Civic, and uPort. However, these solutions are built to be adaptive and versatile, as a result, these solutions are only able to store generic user information that does not sufficiently meet the need of institutional grade KYC / AML processes.

For this reason, Jibrel will build out a dedicated compliance API that will liaise with both a dedicated Jibrel KYC / AML module as well as third-party solutions available today.

Figure 7. Jibrel Compliance API



6.3.3 Role of Jibrel Network Token (JNT)

A key business requirement of the Jibrel Network is that all CryDRs must remain tethered to an underlying asset. In order to achieve this, off-chain assets must first be securitized, which is why a virtual exchange currency is required. Both to transact with the network, as well as facilitate the payment off-chain fees.

An existing currency (e.g. BTC, ETH) is not suitable as the price movements of these currencies are unrelated to utility in the Jibrel Network. This disconnect imposes market and credit risk. In addition, if the Jibrel Network aims to provide a dedicated chain in the future, a dedicated token will be required to facilitate a seamless migration process.

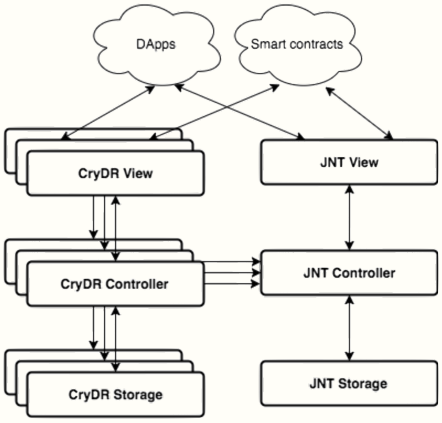
CryDRs themselves are unsuitable for this solution, as they must remain tethered to real-world assets, leveraging them as part of payment causes another

disconnect to emerge, unbalancing the system.

Jibrel Network Token (JNT) will act as the 'fuel' or 'gas' of the network. JNT will provide universal access to all features provided by the Jibrel Network and the relevant Jibrel DApps.

JNT ensures all CryDRs remain tethered to their respective underlying assets at all times, adding an additional layer of compliance.

Figure 8. Jibrel Network Token Interaction



7. FULLY DECENTRALIZED OPERATIONS

In the short to medium term, off-chain activities will be needed to undertake the necessary legal and financial due diligence to convert physical assets to digital assets. In addition, the BOD members will be needed to oversee the JDB to ensure full transparency and regulatory compliance.

In the longer-term, it is expected that regulation will evolve to facilitate on-chain verification of asset ownership, enabling jibrel to become a decentralized autonomous organization.

7.1 Self-service Portals

Once the technological limitations such as on-chain computational capability and the feasibility of implementing complex zero-knowledge proofs[5][9]; as well as the regulatory hurdles of obtaining the relevant licensing, are overcome, jibrel could operate self-service portals (i.e. traditional exchange platforms hosted on-chain, communicating with the jibrel network).

The build-out of these portals is critical to jibrel achieving full decentralization.

7.2 On-chain Digital Identity / KYC / AML

While many on-chain digital identity and KYC solutions exist today, they are limited in functionality. More advanced identification solutions will be required to achieve self-service portals.

7.3 Board of Directors DAO

Once operations have reached steady state, the Board of Directors can be dissolved and replaced with a autonomous regulatory entity, charged with overseeing the operations of the JDB.

8. USE-CASES

Traditional asset-backed tokens that are easily exchangeable provides a wide range of use-cases

8.1 Traditional / Digital Asset Exchange

By allowing traditional assets and digital assets to be freely traded between one another, a platform is inherently developed that facilitates low-risk, high returns for institutional investors through the wholesale of traditional investment instruments to investors and entities seeking stable digital assets.

8.1.1 Investment Platform

An investment bank can deposit money market instruments or commodities into the JDB and then sell those products (CryDRs) to decentralized organizations and funds at a premium, benefiting from *on-chain / off-chain arbitrage*.

8.1.2 Hedging Tokens

Decentralized Autonomous Organizations and funds can purchase money market CryDRs and store them on-chain, with full transparency, reassuring investors that their funding is safe. Decentralized Autonomous Funds can choose from a wide range of traditional assets to complement their digital portfolios and protect against cryptoeconomy downturns.

8.2 Global Transfers

By providing asset-backed tokens, the platform is able to provide tokens that possess all the desirable qualities of both, traditional assets - in particular, stability and global adoption, and digital assets - immutability, ease of transfer and reliability.

With these tokens, payment gateways, remittance channels and other money transfer use-cases can be implemented.

5 While significant work has been undertaken to improve the efficiency of probabilistically checkable proofs, they still remain highly impractical

8.2.1 Remittances

Jibrel can enable remittances by enabling fiat to fiat transfers that use crypto-infrastructure to execute transactions. Users can add funds and transfer them to anyone in the world, leveraging the low fees provided by digital currencies while still maintaining the stability, security and safety of traditional currencies.

8.2.2 Universal Wallet

Currency agnostic wallets can be created that allow users to freely convert between currencies and make transfers to anyone, anywhere in any currency, without the exorbitant fees usually associated with such transactions.

8.3 Cross-border Payments

Similarly, jibrel can enable cross-border payments.

8.3.1 Currency API

With the underlying tokens, jibrel can provide a currency API that allows users to convert freely between currencies.

8.3.2 Merchant API

Jibrel can provide merchants with a simple easy to use payment gateway that can accept payments in any currency and pay-out in the local currency. Without incurring exchange or transfer fees.

Once the network is established, merchants will be able to set-up currency agnostic payment gateways using jibrel's user-friendly libraries and API.

9. REFERENCES

[1] Nakamoto, Satoshi, *Bitcoin: A peer-to-peer electronic cash system*, 2008 - URL - {https://bitcoin.org/bitcoin.pdf}

[2] Brennan and Lunn, Credit Suisse Equity Reports - *Blockchain - The trust disruptor: Shared ledger technology and the impact on stocks*, 2016 - URL {http://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf}

[3] Golem, *The Golem Project: Crowdfunding White Paper*, 2016 - URL {http://golemproject.net/doc/DraftGolemProjectWhitepaper.pdf}

[4] Wilkinson, Shawn, *Storj Project: A Peer-to-Peer Cloud Storage Network*, 2014 - URL {https://storj.io/storj.pdf}

[5] Tether Ltd, *Tether: Fiat currencies on the Bitcoin blockchain*, 2016 - URL {https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf}

[6] Eufemio, Chng and Djie, *Digix: The Gold Standard in CryptoAssets*, 2016 - URL {https://dgx.io/whitepaper.pdf}

[7] Buterin, Vitalik, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2013 - URL {http://ethereum.org/ethereum.html}

[8] Solidity, *Solidity: A contract-oriented, high-level language for the Ethereum Virtual Machine*, Release 0.4.10 Documentation - URL {http://solidity.readthedocs.io/en/v0.4.10/}

[9] Ben-Sasson, Chiesa, Garman, Green, Miers, Troma and Virza, *Zerocash: Decentralized Anonymous Payments from Bitcoin*, 2014 - URL {http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf}