

# {{PegDollar}}: Decentralized digital money for the masses

---

## Business research whitepaper v0.1 [changing]

Notice: This document is a research proposal, and in no way makes promises about the full functionality of any derived implementation, nor does it represent a commitment or intent to build, deploy or operate such a system. Its sole aim is to envision the process of defining, planning and productizing such a system and product.

Note: Names inside {{}} denote placeholder product names.

### Executive summary

This research proposal describes **{{PegDollar}}**, a **digital money** product **pegged to the US dollar (\$USD)** and **{{PegLoan}}**, the **collateral-backed loan system** that produces it. **{{PegDollar}}**'s **interest bearing** and **natively digital** features differentiate it from existing solutions on the market, while the supporting loan system's **immutability** and **decentralization** differentiate it from existing blockchain based solutions such as MakerDAO's DAI.

**{{PegDollar}}** takes advantage of the low cognitive overhead associated with US dollar as a unit of account. It also yields risk free variable interest for money users, which elevates it over other corporate and government stablecoin offerings. The paper focuses on the **digital money product**, describes its technical and customer facing aspects. It defines the greater "**general-purpose consumer money**" market, categorizes its sub-segments, and describes comparisons with leading products in related categories.

It is important for successful real world implementations of the proposed product, to align their positioning and branding with the hosting blockchain core community. Transitioning to a differently targeted positioning and branding, upon crossing the chasm into widespread adoption, is also crucial to success. Support of the greater ecosystem of partners, such as payment proxies and money protocols, is a significant requirement for wide availability.

The backend system that produces the money product, functions in a complex and distributed ecosystem. A number of entities that benefit from the system as its direct customers/clients, including money users, loan takers, price providers, liquidators and market arbitrageurs, all of which would be provided with sufficient incentives to participate sustainably.

### Vision

A **widely available, dependable** and **easy-to-use digital currency**, that consumers can buy, use, hold and **collect interest** on, without the involvement of banks.

### Business goals

- **Digital money for the masses** - Provide everyday people with a usable (requiring minimal cognitive load) and competitive (interest bearing) digital stablecoin based on blockchain technology.
- **Wide availability** - A currency cannot be easy-to-use if it is not widely accepted by a network of people and businesses, and it is not widely accepted if doesn't grow past a tipping point, where mainstream financial ecosystem players are incentivized to support it.
- **Maximal decentralization** - Eliminate risk of rent-seeking through capture, and minimize the need for third-party trust, with goals of improving conditions of adoption by other businesses, and significantly reducing risk of central failure.
- **Incentivization** - Provide loan takers with sufficient incentives to take loans (open debt positions using collateral), competitively compared to other market solutions. Provide different stakeholders with a competitive but profitable business model that incentivizes and guides them into behavior that benefits the system and other stakeholders.
- **Simplicity** - Minimize operational complexity, such that it is relatively easy for all stakeholders to anticipate the system's automated behavior, and predict future outcomes.
- **Capital efficiency** - Making the flow of capital more efficient through the system unlocks economic value and benefits all stakeholders.

## {{PegDollar}} product basics

{{PegDollar}} is a money product in the form of a cryptocurrency token (representing the US dollar), which is supported by {{PegLoan}}, a loan system available to all on a public blockchain. Anyone can buy, hold and use {{PegDollar}}, as well as store it in a digital savings account and collect interest, all without the involvement of a bank.

There are many other available cryptocurrencies representing the US dollar, however they all depend on some type of central entity for operation, making them more vulnerable to economic rent-seeking or security failure. {{PegLoan}} is ownerless and functions on a never-changing (immutable) secure smart contract. The system allows anyone to take a loan of {{PegDollars}} against their native blockchain assets, specifically default digital token of a given public blockchain (e.g. ETH on Ethereum, BTC on Bitcoin), that happens to be third-party trust-minimal. They can perform this action without giving up ownership of assets at any point, through storing a proportional amount of the collateral asset in a blockchain account.

The money users are not required to be aware of the underlying details, such as the system guaranteeing security of assets, as well as appropriate monetary collateral backing. All other system inter-actors, such as loan takers, price providers and liquidators, have deeper involvement with the details of system and its functionality, and are appropriately incentivized to have ongoing and profitable inter-actions with the system.

## {{PegLoan}} product basics

{{PegLoan}}, the system behind {{PegDollar}}, is a collateral-backed stablecoin system on a public blockchain that only collateralized the native token and has no formal governance process or token. It focuses on one stable currency pegged to the US dollar, given the minimal level of cognitive load required for everyday use of a US dollar digital currency. However, it is possible for anyone to copy the ideas and open source code behind {{PegLoan}} to deploy new instances of the system targeting different currencies or other baskets of assets. In more technical terms, it is a trust-minimized, governance-minimized, capital efficient collateral-backed stablecoin system (See [terms](#) for definitions).

- **Fully decentralized operation**, lowering chance of rent seeking through capture
- **Optimized capital efficiency** due to elimination of governance token
- **Predictable behavior** due to algorithm-based monetary policy governance
- **Simple risk profile** due to native token as exclusive backing collateral asset
- **Open source** with no legal copyright liability due to copying, modification, deployment

## Stakeholders

In this section we will present all of the stakeholders associated with the proposed products, any distinguishing details, as well as their motivations to participate in the greater product ecosystem.

### System customers

- **Money users** - These are *regular consumers* that *use* or *store* the pegged currency in their blockchain-based *savings account*. The notable target groups that could most benefit from such an offering are *the un-banked* and those with limited access to a *stable Store of Value* (SoV) from countries with dysfunctional monetary policies. This could also be used by the *early adopter community* of a public blockchain.
- **Loan takers** - Most commonly, existing *native token holders* who have decided to *take a loan* against their holdings. The main incentive for this group consists of being *long native token*, while being able to *deploy its value* in other profitable transactions. They may also initially be *motivated by the technology* itself, however this is not a long-term sustainable incentive.
- **Price feed providers [maintainer]** - maintain the system by *providing accurate rates* of exchange between naive currency (ie ETH), the reference currency (ie USD) as well as the pegged currency. These providers are expected to compete in *establishing trust* amongst the loan takers, and in return be *monetarily compensated* based on trust level, as well as *avoiding penalties* by adhering to the loan system rules.
- **Loan liquidators [maintainer]** - maintain the system while competing with each other to liquidate undercollateralized loans. They monitor loans and trigger liquidation while speculating on the future collateralization levels of target loans as

judged by the system.

## Ecosystem partners

- **Wallets** - Popular end user apps that provide self-custody, buying, selling, receiving, and sending of digital assets. They would be encouraged to support and showcase {{PegDollar}} as one of their main options.
- **Exchanges** - Popular exchanges, be they centralized, or decentralized, would be encouraged to add ability to trade pairs with {{PegDollar}} as well as encourage liquidity brought in by exchange traders or liquidity providers.
- **Money protocols** - These are smart contract that offer lending, borrowing, decentralized exchange, synthetic assets, prediction markets, amongst others, that would be encouraged to support {{PegDollar}} as an option for payment or liquidity their services.

## Market

{{PegDollar}} and {{PegLoan}} are the product manifestations of the proposed system's two sided market, one focused on consumers and the other on financial investors. Per our driving [vision](#), primary focus will be on the consumer market.

The main market we are considering is the "*general-purpose consumer money*" market segment. We will consider the various properties that determine demand for a given money product in this market, whether they are determined by the consumer's desired traits, features of that money product, or by environmental factors such as jurisdictional regulation. We will also categorize the market and define sub-segments, in order to better show the optimal positioning of {{PegDollar}}.

We will also briefly and separately touch on the "Digital asset backed loan" market, and discuss optimal positioning of {{PegLoan}} for the system's other stakeholders such as loan takers, price feed providers, liquidators, and market arbitragers.

## Desired product traits

In general, a good money product candidate should demonstrates a good level of the following properties to the end-consumers:

1. **Store of Value (SoV)** - the consumer wants assurance that the value they hold in a money product is not lost.
2. **Medium of Exchange (MoE)** - the consumer likes to be able to use a money product in a wide array of markets for a wide array of economic transaction types.
3. **Unit of Account (UoA)** - The consumer's mental accounting of sending and receiving money is least costly when most of the economic transactions they participate in, use the same stable unit of account. This makes exchange across different markets predictable and less mentally exhausting.

## Product features

Any money product offers specific technical features tuned to its target market. These could vary across dimensions such as reference value, backing assets, and supporting payment networks.

### Reference value

Money products track a commonly accepted concept of unit of account, which may vary in value through time. In a global setting, and assuming minimal regulatory limitations, using US dollar (\$USD) as reference value, results in optimal SoV and UoA properties of money. In specific jurisdictional settings however, using national currency is most common. Selecting a national currency as reference value, adds a centralization factor around value-setting, that could potentially be exploited by the national government, by inflating its value through printing money excessively.

### Interest bearing

A money product that can earn risk free interest, while not in use, is superior to one that does not. Bank deposit money does earn small amounts of interest when stored in a traditional savings accounts, that also subjects the money to some restrictions

around withdrawal. MakerDAO's DAI token and {{PegDollar}} offer considerably higher variable interest, which makes them a better in terms of SoV. Not only are they less likely lose value, their value is likely to increase with time compared to inflation.

## Payment network

This is a network of payment senders and receivers, backed by underlying payment infrastructure. In order for a money product to be a good Medium of Exchange (MoE) it has to be widely available through markets that consumers want to participate in. Low cost of access, as well as merchant and consumer desire to participate in a money payment network, determine the extent of the money's desirability as a MoE.

## Collateral backing

In order to ensure their long term value, money products are fully or partially backed by other assets. The mechanisms of this backing and the type of assets used determine many of the technical risk parameters of such a money product. Some common examples of this are Gold (ie for US dollar), digital assets (ie BTC, ETH for algorithmic stablecoins), or national currencies like US dollar (\$USD), Euro, or Chinese Yuan (ie corporate or national stablecoins).











The backing assets of a money product are the least visible to consumers, however they affect and are heavily dependent upon regulatory factors. In case of {{UniDollar}} backed by {{UniLoan}}, the specific selection of backing assets as digital assets, mainly affects the other side of the market, namely the "digital asset backed loan" market.

## Competition




For the greater market segment please see [market categorization](#) breakdown, based on features and desired properties, for more information.

If we focus on direct competitors, the stablecoin market segment is what we should consider. Stablecoin competitors currently range from centrally issued ones, to automated/algorithmic ones (ie MakerDAO's DAI). We believe all of these competitors have positioned themselves to have a lower level of optimizations around trust minimization, risk minimization, capital efficiency, and governance minimization, that significantly lowers their potential for long-term success. These other options, either depend on a centralized entity for issuance, or for governance, and often do not efficiently flow capital through the system.

Below is a tabular representation of the product's extended competition, as represented by market categories, category leaders and other notable examples:

Product	Market segment	Reference value	Asset backing	Interest bearing	Payment network	SoV rating	MoE rating	UoA rating
US dollar (\$USD) bills	Physical cash money (bank notes)	US dollar (\$USD)	Gold, National credit and rep	No	Physical commerce	 High	 High	 High
Argentine peso bills	Physical cash money (bank notes)	Argentine peso	Gold, National credit and rep	No	Physical commerce	 Low	 High	 Medium
Any US credit card	Credit card money	US dollar (\$USD)	Consumer credit	No	Digitized commerce	 Medium to  High	 High	 High

Product	Market segment	Reference value	Asset backing	Interest bearing	Payment network	SoV rating	MoE rating	UoA rating
Any US deposit bank w/ debit card	Deposit and debit card money	US dollar (\$USD)	Yes	Consumer deposit, bank credit	Digitized commerce	High	High	High
Venmo	Corporate digitized money	US dollar (\$USD)	Consumer deposit, corporate credit	No	Money app	High	Medium	High
PayPal	Corporate digitized money	US dollar (\$USD)	Consumer deposit, corporate credit	No	Money app, payment provider	High	High	High
WeChat Pay	Corporate digitized money	Chinese Yuan	Consumer deposit, corporate credit	No	Money app, payment provider	High	High++	High
Tether	Corporate stablecoin money	US dollar (\$USD)	Corporate deposit and credit (<100%)	No	Public blockchains	Medium+	Medium	High
Coinbase USDCoin (USDC)	Corporate stablecoin money	US dollar (\$USD)	Corporate deposit (100%)	No	Public blockchains	High	Medium	High
Digital US dollar (\$USD)	State backed stablecoin money	National currency	Gold, National credit	No	Public blockchains	High	Medium	High
Digital Chinese Yuan	State backed stablecoin money	National currency	Gold, National credit	No	Public blockchains	High-	Medium-	High
DAI	DAO-governed asset-backed stablecoin money	US dollar (\$USD)	Digital assets >100% (ETH)	Yes	Public blockchains	High	Medium	High
<b>{{PegDollar}}</b>	<b>Trust-minimized asset backed stablecoin money</b>	<b>US dollar (\$USD)</b>	<b>Digital assets &gt;100% (commonly ETH)</b>	<b>Yes</b>	<b>Public blockchains</b>	<b>High+</b>	<b>Medium</b>	<b>High</b>

Product	Market segment	Reference value	Asset backing	Interest bearing	Payment network	SoV rating	MoE rating	UoA rating
Imaginary product {{PegWTF}}	asset backed stablecoin money	US dollar (\$USD)	Digital assets >100% (commonly ETH)	Yes	Public blockchains	 High++	 Medium	 High

## Market categorization

Numerous sub-segments exist in the greater "*general-purpose money for consumers*" segment, some of which are already seeing very large scales of market activity. Some of these include our daily use of cash, credit/debit cards, money apps and bank transfers. We categorize the market sub-segments as follows:

- **Physical cash money (bank notes)** - Provided and backed by national governments. The most prominent of these globally are US dollar bills (\$USD). Current estimate for current money supply (M2) is above \$1.5 trillion.
- **Digitized consumer money**
  - **Debit and credit card money** - facilitated by payment processing companies that connect credit card transactions to consumer credit accounts or debiting directly from the consumer's bank deposit account.
  - **Bank digitized money** - network of bank deposit accounts and transfers facilitated by Automated Clearing House (ACH) - Examples: Chase, Wells Fargo, Bank of America, etc.
  - **Corporate digitized money** - Money apps - For example Venmo, PayPal, ApplePay
- **Digital stablecoin money**
  - **Corporate stablecoin money** - Examples: USDCoin (USDC) backed by Coinbase, Tether dollar (USDT) backed by Tether, Gemini dollar (GUSD) backed by Gemini.
  - **State backed stablecoin money** - Example: digital Yuan or potential digital dollar
  - **Asset backed stablecoin money**
    - **DAO-governed asset-backed stablecoin money** - Example DAI backed by MakerDAO
    - **Trust-minimized asset backed stablecoin money** - Example: {{PegDollar}} backed by {{PegLoan}} system
      - [Imaginary product] **Trust minimal asset backed stablecoin money** - See Imaginary product {{PegWTF}}.

## Notable exclusions

- **Digital assets money** - Bitcoin, ETH, not suitable for general-purpose consumer use due to large volatility, and speculative use.
- **Currency exchange assets** - For example US dollar, Euro, Yuan etc held on currency exchanges used for currency trading. Used mainly for speculation and not for everyday use in commerce.
- **Equities (stocks, bonds) and commodities (Gold)** - not suitable for general-purpose consumer use due to large volatility, and speculative use.

## Jurisdictional considerations

In many jurisdictional sub-segments, due to regulatory enforced limitations, most everyday economic transactions can only be denominated in the national currency. This, most viable money candidates have no choice but to use that jurisdiction's national currency as their reference value, as well their backing asset.

Unfortunately, in many cases this occurs even if the national currency does not represent good characteristics for Store of Value (SoV), due to consistently large inflation, and volatility. Some examples like Argentinian Peso and Iranian Rial demonstrate the extent of this problem.

## Branding

Branding is essential to success of a consumer-based money product. As a result, any potentially successful implementation of this research proposal needs to at least have a set of consistent brand guidelines, that establish it as a reasonable alternative to all the money product options out there. A few options are discussed below:

## 1. PegLoan and PegDollar

The more generic branding can be used for any public blockchain, and is consistent with the terminology used.

- `{{PegLoan}}` = PegLoan
- `{{PegDollar}}` = PegDollar
- `{{PegDollar}}` symbol: ₪\$

In case of use on the Ethereum blockchain, this generic branding is a fallback to the more compelling option below. Of course the Ethereum community can effectively reject the branding below, based on the sentiment that the product does not sufficiently align itself with Ethereum, or it is attempting to illegitimately appropriate the community's identity.

## 2. UniLoan and UniDollar

Preferred option for Ethereum.

- `{{PegLoan}}` = Uniloan
- `{{PegDollar}}` = UniDollar
- Brand = 🦄
  - UniDollar - 🦄 \$
  - UniLoan - 🦄 🏠

The brand symbology and emoji representation is inherently "meme-able", adding to the velocity of the product brand's awareness and eventual adoption.

The innovators and early adopter market segment, who have significant community influence, and believe in the Ethereum community's value of maximal decentralization, have already been exposed to this symbology and can be recruited to spread the word about Uniloan and UniDollar.

Of course adoption of this branding mainly depends on the community's effective permission to use it, based on their sentiment of how aligned the product is with the Ethereum ideals.

### 2.a. Unicorn dollar

This would be the preferred currency symbol for at least the initial stages of the product (before crossing the chasm), when the innovators and early adopter market segment would likely prefer to use this notation in their apps, as it reinforces a sense of community.

- Unicorn dollar symbol: 🦄 \$

Referred to as Unicorn dollars.

### 2.b. Uni dollar

Mass users of UniDollar will more likely be part of the early and late majority market segments. They will likely not be familiar with the Unicorn symbology mentioned above. In their case, it is more desirable to have a more conventional representation of the brand, as opposed to one that is playful. This will help establish the trust required to use the currency for everyday commerce, and increase the level of comfort for both consumers and by merchants. For example, one can imagine this symbol being used in payment applications, spreadsheets or accounting software user interfaces.

- Uni dollar symbol: ₪\$

`{{PegLoan}}` market



The "Digital asset backed loan" market is one that is separate from the "consumer money" market. We will discuss the optimal positioning of {{PegLoan}} for the system's other stakeholders such as loan takers, price feed providers, liquidators, and market arbitragers.

## Business models

The system protocol itself is immutable and thus maximally decentralized. No one entity can profit from operating the central system. However the various stakeholders of the ecosystem created by the system protocol have their own incentive systems and business models.

It is important to mention however, that wide adoption of the products representing this system will likely have a significant positive impact in value capture by the native blockchain asset that implements it. This is a notable point, as it strongly aligns the system's success to the hosting public blockchain.

In this section we discuss likely business models governing each of these players, as well as a few others:

- **Research organization**
- **Specific public blockchain community**
- **Price feed provider organizations:**
  - **Non-profit foundation or organization(s)**
  - **Reputation-centric financial organization**
  - **For profit financial organizations**
- **Loan takers** - Can be individuals or organizations, business model not applicable
- **Money users** - Can be individuals or organizations, business model not applicable
- **Liquidators** - Entities dedicated to pursuing and capturing arbitrage opportunities

### Research organization

This is the initial entity responsible for vetting and introducing the idea of this research proposal to the world. It would operate as a non-profit and take in revenues in the form of grants from other entities interested in developing public blockchain ecosystems they focus on. See the research organization section of [roadmaps](#) for more details.

### Public blockchain community

This is the decentralized community of individuals who contribute to a specific public blockchain, and as such it does not have a conventional business model. Like the research organization it would operate on grants from entities interested in developing the public blockchain's ecosystems. The individuals in these communities operate more on ideals of communism than that of transactional self-interest, or chain of command. They contribute when they can, ask for help when they need, and consider gaining community recognition as their main reward objective. See the community section of [roadmaps](#) for more details.

### Non-profit organization(s) or foundation

Such organizations or foundations are dedicated to contributing to a specific implementation of the idea introduced by this research proposal. The dedicated nature of such a foundation's mission, will likely garner a special level of support and trust from that blockchain's existing community of contributors. Success of such a foundation would also be beneficial to the blockchain's native token.

For example, one can foresee a specific Foundation dedicated to the establishment of a pegged loan system on Ethereum, partly by promoting the system itself, as well as the pegged dollar currency that it produces. The Ethereum community is likely to generally support such a foundation in spirit, as its goals will likely be well aligned with that of the greater community, and its success will benefit Ether (ETH) in value.

### Reputation-centric financial organization

An entity that forgoes profiting from conventional financial activities in favor of revenue from high trust requiring activities, such as auditing or rating. They have established trust across social subsections of users, that they will report prices truthfully.



Comparable organizations in other industries may include rating agencies, auditing firms, etc.

## For profit financial organizations

These are entities that already offer financial services, and are also trusted to offer truthful price information. In the DeFi space, a foreseeable candidate for such a role would be *DeFi aggregators*. DeFi aggregators provide users with desirable experience, on mobile and web, targeted to specific jurisdictions, while allowing users to access a range of backend financial services, and to switch between them in some cases.

## Liquidators

Are generally proficient in programmatic automation and capital allocation and likely require little overhead investment in the form of organizational management or marketing. As such, and as already observable in the DeFi market, they are expected to be run by one or few programmatically and financially skilled individuals, with high margins when successful. The space is however expected to become more competitive in the long run, likely costing existing liquidators but benefiting the ecosystem as a whole.

# Appendix

## Assumptions

### Long term trend assumptions

- **Disruption of finance** - Financial assets and processes would increasingly be digitized and decentralized, through use of blockchain technology, due to the significant efficiency unlocked in building and operating financial systems.
- **Collateral-backed stablecoins** - Using smart contracts to offer a stable-value token by collateralizing other digital assets, is the optimal method for creating decentralized blockchain-based stablecoins.

### Market assumptions

In this section we provide some background on the key concepts and assumptions that drive the reasoning behind the product choices made in this research proposal.

- **Good money** - The best digital money for the masses is a US dollar (\$USD) stablecoin, that returns interest, has high liquidity, and is widely accepted across a variety of different financial ecosystems. The following are properties consumers look for in good money:
  - **UoA** - Unit of Account - In the world today, the most usable Unit of Account (UoA) is the US dollar (\$USD with over \$1 trillion circulation), partly due to the low cognitive load associated with understanding and using it.
  - **MoE** - Medium of Exchange - High liquidity and network effects (availability throughout the financial system) of an asset are pre-requisites for it becoming a good Medium of Exchange (MoE).
  - **SoV** - Store of Value - Functional stablecoins, especially ones bearing interest are considered good Stores of Value (SoV).
- **Interest** - An interest bearing stablecoin has significant competitive advantage compared to real world stable currencies, and is on par with other on-chain alternatives such as MakerDAO's DAI token. A money product that bears interest is a better Store of Value (SoV), given that the value actually increases in time.
- **Achieving decentralization** - In general, decentralization is best achieved through [permission-less-ness](#), [censorship-resistance](#), and minimized involvement of third-party actors. It improves the SoV aspect of the product by reducing its long term value risks and capital efficiency.
- **Default collateral** - ETH is currently the most trust minimized programmable digital asset available, and is supported by a considerably decentralized Ethereum blockchain that is permission-less, censorship-resistant, relatively secure, and with a high promise of wide adoption.
  - Bitcoin currently does not fit the easy programmability requirement, however it offers higher security, as well as many other superior qualities. At the same time, it has not built up considerable momentum in developing

financial ecosystem network effects. That said, learning more about the Bitcoin space remains a top research priority.

- Other blockchains lack most of above required features, and in rare cases where they do, they are not even as secure as Ethereum, and lack network effects. That said, this proposal remains open to sharing ideas with other chains or considering them for further research.
- **Governance and tokens** - Completely replacing off-chain and on-chain governance with an on-chain incentive systems, significantly reduces risk of capture as well, increases operational complexity, and significantly reduces capital efficiency. This is especially true when a governance token is used (ie MakerDAO's MKR token).
- **Long term value risks** - This type of risk, such as the risk of inadequate collateral backing, increases the likelihood that a money product would eventually fail by losing its value. Everyday consumers however do not perceive this type of risk as easily.

## Acknowledgements

### Ode to Uniswap

Even though {{PegLoan}} provides a different financial service compared to Hayden Adams' Uniswap, some of its properties around trust-minimization and decentralization are in fact inspired by Uniswap. It also attempts to stay true to the brand essence of Uniswap, which also happens to overlap with the values of the greater Ethereum community, and its [Unicorn symbology](#).

Uniswap is a maximally decentralized exchange smart contract, that is permission-less, censorship-resistant and unstoppable (See [terms](#) for definitions). After the contract's finalization and deployment by original author, no one (not even the author) has any control over its operation. The contract will run as long as Ethereum 1.0 continues to operate, and has been available to anyone with an internet connection, to be used in performing token exchanges or profiting by providing liquidity.

{{PegLoan}} and its default US dollar stablecoin {{PegDollar}}, would have most or all of the important properties of Uniswap, including its level of decentralization. After deployment and finalization, the {{PegLoan}} smart contract, should no longer be controlled by anyone, and should be available to all blockchain users.

### Tip of the hat to MakerDAO

This proposal recognizes standing on the shoulder of Rune Christensen, the MakerDAO team, the Maker community, and the world changing impact they have had. Keeping in mind that ideas and progress are not beholden to any one group or person, the proposal uses learnings from the remarkable experiment they have run, and shares in the common goal of evolving digital finance.

### PegWTF

{{PegWTF}} is an imaginary money product and successor to {{PegDollar}}, based on the imaginary WTF (World Trade Francs) Unit of Account, defined and maintained by the also imaginary {{WTF Foundation}}, as a universally agreed-upon and stable basket of goods, assets and/or currencies. {{PegWTF}} is based on the same {{PegLoan}} system as described in the current research proposal, though it uses WTF as its reference currency.

See [WTF](#) for reference. Seriously though, WTF!?!

### Terms

**Stable-coin** - A fully digital token whose value that is stable relative to a reference pegged asset with high level of historical stability. The reference pegged asset could be anything from a national currency like the US dollar (\$USD), to a basket of stable and uncorrelated assets, such as basic commodities, or currencies.

**Digitized** commerce/money - Commerce or money that is represented and operated in digital form in order to achieve efficiencies offered by digital automation. The digitization is however not with full fidelity, and relies on a mechanism to tie the digital representation to physical representation of value, through legal and operational processes representing overhead.

**Digital commerce/money** - Commerce or money that is backed, represented and operated fully in digital form in order to achieve even higher efficiencies offered by digital automation.

**Permission-less-ness** - is the property of a system that allows anyone to interact with it and to participate in its offered economic transactions, without permission or requiring verification or validation of their identity. For example the internet is permission-less because anyone can access information or post information for others to see.

**Censorship-resistance** - is the property of a system that makes it very difficult for any gatekeepers to prevent users from interacting with the system, and participate in offered economic transactions. For example, the internet is censorship-resistant because censoring it is very difficult, even by governments and organizations that try to control the actions of their populations or members.

**Unstoppable** - is the property of a system that is owner-less and cannot be disrupted by any entities. For example Uniswap is unstoppable because it has no owners that can modify the original contract in any way, and it cannot be disrupted, because it runs on the Ethereum blockchain which has been, and will very likely be running perpetually into the future.

**Native token** - Is the default value token provided by any given public blockchain, one that is used to pay for transactions performed on the blockchain platform level. For example on the Bitcoin blockchain, native token is Bitcoin (BTC), and on Ethereum, the native token is Ether (ETH).

## Legal considerations

If successful, the proposed system and products would be adopted at high scale, raising a possibility of becoming pulled into significant disputes. In this section we attempt to explore a few potential disputes and discuss possible mitigations.

### General Jurisdictional regulation

The {{PegLoan}} system and its {{PegDollar}} money product virtually function on the neutral and decentralized internet and blockchain spaces. In this context, there are no specific jurisdictional enforcements outside the functionality of the hosting blockchain, and the smart contract rules that make up the system. However the effects of these products' functionality extend into the real world, and into real jurisdictions where the stakeholders reside.

Most notable concern by local, state and national government regulatory bodies are related to preventing financial crime or using money in prohibited activities by requiring reporting of large and/or suspicious financial activity to the authorities. A few examples of these requirements are the Know Your Customer(KYC) and Anti Money Laundering (AML) rules enforced by most western governments. Also at the international level, Financial Action Task Force (FATF), sets [specific rules](#) for combating "terrorist financing, the financing of proliferation, and other related threats to the integrity of the international financial system."

### US jurisdictional regulation

Amongst the many financial regulatory bodies in the US government, Financial Crime Enforcement Network (FinCEN) is the most relevant body that deals with legal matters related to money. According to a recent [press release](#) FinCEN states that "administrators of stablecoins have to register as MSBs with FinCEN."

This stance is demonstrably inconsistent with realities of how permissionless blockchains work. For example the definition of "administrator" in the existing cases of algorithmic stablecoins (like MakerDAO) and real world backed stablecoins (like USDC) is legally questionable as it is vastly different from traditional administration. However, the statement does demonstrate intent, political will, and the possibility of FinCEN enforcing specific interpretations of the existing rules, even if that interpretation is inaccurate. This presents a notable inherent legal risk for any parties intending to operationalize the proposed system. It should also be noted that this proposal only aims to envision the final system and products, and will require full legal review and mitigation of the above risks before forming an intention to proceed any further than described.

### Stakeholder disputes

The system is designed to ideally operate in a stable manner, with all stakeholders following the spirit of the smart contract system and ecosystem rules around reporting of truthful prices. There is however always the very small chance of things not working out as designed. In such cases, it is important not to rule out the role of off-chain dispute resolution at the societal level. Resorting to off-chain dispute resolution is of course largely a result of the immutable and decentralized nature of the proposed system.

The system enforces hard rules on stakeholder behavior on-chain through the use of smart contracts. This is designed to incentivize constructive behavior and reduce coordination costs by reducing the chances of costly disputes, and by offering less-costly dispute resolution mechanisms. For example, the system's on-chain algorithms for collecting and aggregating reported prices, make it costly for any minority of price providers to cheat. They also provide for an ongoing process for resolving disputes in price reporting and to almost always arrive at a stable conclusion in time.

In very rare cases however, the on-chain dispute resolution mechanism may be insufficient in bringing about desired results, ones that are in accordance to spirit of commonly agreed upon beliefs. For example, there is a small possibility that a large group of existing feed providers attempt to capture the system, despite incurring short term penalty costs, in order to abuse and profit from the system long term. In such a case, or in case the ecosystem anticipates the approaching of such a case, it is perfectly reasonable to resort to off-chain dispute resolution mechanisms, in order to minimize costs to all good-faith stakeholders.

The system and ecosystem rules around price reporting for example, rely on off-chain trust relationships that establish top trusted feed providers' through loan allocations in the on-chain system. It is perfectly reasonable therefore, that any violation of these trust relationships, is disputable off-chain in addition to on-chain. Existence of such societal dispute resolution options, only strengthens functionality of system and ecosystem as a whole.

### **Smart contract risks**

As demonstrated by the DAO hack, there is always a non-zero probability of smart contracts not behaving as originally intended. The goal should be to minimize this probability as close to zero as possible by taking effective mitigating steps.

The probability of smart contract malfunction is higher for more complex smart contracts. This probability decreases significantly as a result of formal verification, auditing and other code quality assurance processes. For the {{PegLoan}} system, the complexity level is relatively higher than previously established immutable smart contract systems like Uniswap, and so the mitigating steps mentioned above become essential.

The immutable nature of a smart contract system may eliminate a class of attacks on centralized system administrators, however it does introduce the issue of not being able to correct any code issues in the short term, when compared to more centralized designs. As a result, if such malfunctions expose the system to attacker harm, the impact of such malfunctions could be significant, despite the extremely small probabilities. As such, the main stakeholders of the system should be aware of all such known and unknown risks in terms of their probability, and potential impact.

For any entities providing an interface into the {{PegLoan}} system, it is responsible behavior, to inform their interface users of the said potential risks at least at a high level.