DLC.Link: Enabling Bitcoin in Applications

Aki Balogh, Jesse Eisenberg, Matt Bombard, Grayson Lucas

Abstract

What is Bitcoin? We review the five characteristics of money with a particular focus on Bitcoin's scarcity. We then define conditional payments, smart contracts, and Bitcoin's lack of interoperability.

This leads to the core question: Why doesn't Bitcoin possess smart contract functionality? What are the current "solutions" (i.e., wrapping, bridging, CeFi) and what are the risks to each solution.

We then provide our novel solution, Discreet Log Contracts (DLCs), a self-wrapped, self-bridged, self-custodied solution. We learn the technical components of DLCs, the key improvements to existing solutions, and how DLCs bring much-needed smart contract functionality to Bitcoin. We also learn about DLC.Link's core technological components and how DLCs are used to move native Bitcoin securely from Smart Contracts on other chains.

We quickly define oracles, a decentralized Bitcoin Oracle Network (TM), the "oracle problem", and DLC.Link's unique solution to this problem.

We discuss use cases and provide real-world examples of DLC.Link in action.

Last, we conclude the DLC.Link whitepaper.

I. What is Bitcoin?

According to Bitcoin's pseudonymous founder, Satoshi Nakamoto, Bitcoin is a "peer-to-peer electronic cash system".[1] Satoshi's vision for Bitcoin was to become the next evolution in money. Bitcoin inherently possesses the five key characteristics of money. These are durability, portability, divisibility, fungibility, and acceptability.[2] As a brand-new cash system, Bitcoin combines the core characteristics of the modern monetary system with a novel distributed peer-to-peer computer network secured by energy. This unique combination resulted in the birth of the crypto industry.

[1] https://bitcoin.org/bitcoin.pdf

[2] https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-9-functions-of-money#:~:text=The%20characteristics%20of%20money%20are,%2C%20limited%20supply%2C%20and%20acceptability.

Before Bitcoin, previous experiments to “democratize” money were attempted with each one ultimately ending in failure.[3] Bitcoin, however, solved the “reversibility problem” by eliminating the need for trusted third parties that could willingly or unwillingly reverse transactions. In place of trusted third parties, Satoshi developed a chain of cryptographically signed transactions secured by a proof-of-work consensus in order to validate payments.[4]

Another well-known core characteristic of Bitcoin is its limited supply. Satoshi famously encoded a hard cap of 21 million Bitcoin that could ever be in existence. Bitcoin’s built-in scarcity manifested a powerful narrative, “Digital Gold.” In addition to its characteristics as an electronic money, Bitcoin is perceived by many as a store of value and hedge against monetary debasement. Legendary macro investor, Paul Tudor Jones, believes the 2020’s decade will be a period of fiscal retrenchment and that Bitcoin will have [significant] value at some point.[5] This idea of Bitcoin as digital gold is so strong that United States Senator, Cynthia Lummis, termed BTC the “hardest money ever created” moments after unveiling the country’s first ever bi-partisan cryptocurrency bill.[6]

As robust and decentralized as the Bitcoin network has become, it possesses significant technical limitations. Bitcoin has been widely criticized for its inability to scale. As a result, the Bitcoin network can only process a limited number of transactions per second, which leads to slow transaction speeds and high fees during periods of increased network activity. Each Bitcoin block can only realistically store 2MB of data, which is approximately 4,000 transactions per block.[7][8] Depending on the weight and type of transaction performed, data availability limitations may further restrict the number of transactions per block. As a result, data heavy smart contract transactions have never been able to scale on Bitcoin. The recent NFT ordinals development is a recent example of Bitcoin’s data storage limitations.[9] Last, Bitcoin the network, is highly inflexible. Bitcoin’s unique design favors security and simplicity which makes it cumbersome, if not impossible, to introduce new or innovative features to the Bitcoin Script.

Since its inception, Bitcoin developers have repeatedly attempted to build functionality directly on the base layer. Many brilliant programmers, including Ethereum’s Vitalik Buterin, worked to bring smart contract functionality to Bitcoin. The Bitcoin community, however, is legendarily known for its aversion to change. Any improvement proposal takes years of debate, modeling, and code audits before final implementation. As a result, repeatedly unsuccessful attempts to update the Bitcoin code precipitated a developer exodus to rival smart contract blockchains. Vitalik Buterin’s Ethereum, in particular, has seen tremendous success and is jockeying with Bitcoin for the top blockchain by market capitalization.[10]

[3] https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/#:~:text=Key%20Takeaways,very%20influential%20in%20Bitcoin's%20creation.

[4] https://medium.com/@lightcoin/the-problem-bitcoin-solves-8b3944ea77a7#:~:text=With%20Bitcoin%2C%20Nakamoto%20solved%20the,to%20order%20and%20validate%20payments.

[5] https://twitter.com/SquawkCNBC/status/1579460717752684546

[6] https://finbold.com/u-s-senator-lummis-calls-bitcoin-the-hardest-money-ever-been-created/

[7] https://www.bitstamp.net/learn/crypto-101/what-is-block-size/

[8] https://bitcoinmagazine.com/guides/what-is-the-bitcoin-block-size-limit

[9] https://www.theblock.co/post/207086/what-are-bitcoin-nfts-ordinals-and-how-do-they-work

[10] https://medium.com/coinmonks/the-flippening-what-it-is-and-why-it-matters-63e22486ca44

II. What are conditional payments?

Conditional payments are payments made with specific conditions or embedded logic. These conditions can be specified in the contract or agreement, and can be triggered by a variety of factors, such as the completion of a specific task, the passage of a certain amount of time, or the occurrence of a particular event. Conditional payments can be used in a wide range of contexts, including financial transactions, employment agreements, or even personal contracts. Many conditional payments use cases are finding a home on smart contract blockchains. The size of the conditional payment market is likely in the tens of trillions of dollars. The blockchains, applications, and infrastructure providers that successfully unlock this heretofore untapped value will likely come to dominate the 21st century.

III. What are smart contracts?

> [Smart contracts are] self-executing contracts with the terms of the agreement between buyer and seller, or multiple parties, being directly written into software as code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.[11]

IV. Bitcoin's lack of interoperability

The creation of smart contracts has led to a Cambrian explosion of innovation on decentralized blockchain networks. From Decentralized Finance ("DeFi") to Nonfungible Tokens ("NFTs") to Decentralized Autonomous Organizations ("DAOs"), a growing series of startup economies have sprung into existence. Bitcoin's limited scripting language severely limits its ability to interact with smart contracts. As a result, the tremendous capitalization of Bitcoin ("BTC") the asset remains untapped. Bitcoiners in need of productive BTC capital are forced to look elsewhere.

V. Problem: Bitcoin lacks smart contract functionality. Bitcoin cannot move without wrapping, bridging or 3rd party custodianship

This leads to a deeper review into Bitcoin's smart contract limitations. Why doesn't Bitcoin have smart contract functionality similar to its rival smart contract blockchains? The short answer, Bitcoin was never intended to support fully-functioning smart contracts. Bitcoin's programming language, Bitcoin Script, is a simple, stack-based Turing-incomplete language. This type of language makes it very difficult to reason about large-scale programs. Operations such as token creation, statefulness, and leveraging data from other transactions or contracts are extremely difficult or impossible, and go against the ethos of Bitcoins original design. As a result, many Bitcoiners have migrated to rival smart contract platforms while others have taken their BTC capital to the traditional financial system.

[11] https://www.investopedia.com/terms/s/smart-contracts.asp

Wrapping

In today's blockchain economy, gas assets like ETH, SOL, and AVAX power smart contract economies. In order to transact on a specific blockchain one must possess network-compatible assets. Due to code incompatibility, smart contract blockchains are unable to transact with native Bitcoin in the same ways that they can interact with their own native assets. As a result, software programmers developed a solution that allowed for native BTC to be "wrapped" and repackaged into a synthetic Bitcoin.

What are wrapped assets and what is wBTC? Wrapped Bitcoin operates similarly to a Bitcoin IOU. Wrapped Bitcoin (wBTC), for example, is backed 1:1 with native BTC and custodied by an independent 3rd party entity, Bitgo. Custodians promise to safekeep the BTC, however, as many CeFi firms recently demonstrated in the 2022 crypto bear market (i.e., Blockfi & Celsius), this is not guaranteed. Wrapped Bitcoin's custodian risk particularly suffers from a number of risks including blackbox, censorship, and regulatory risk.

Blackbox risk occurs when an entity withholds key information regarding the strategy, controls, and risk management of its assets. Customers are required to trust the entity does not possess hidden risk. Further, customers rely upon the entity to not deviate from its own stated objectives. Additionally, censorship risk occurs when customers give up their anonymity in order to satisfy Know-Your-Client ("KYC") laws. Custodians such as Bitgo require their depositors to KYC in order to officially onboard as clients. Bitcoin, known for its censorship resistance properties, loses one of the core benefits when wrapping. Last, regulatory risk occurs if a state or supra-national actor criminalizes or restricts crypto assets and transactions. Custodians must follow the law or suffer financial or criminal consequences. In each scenario, the BTC may be lost forever, leaving the user holding worthless synthetic BTC tokens. The adage, "not your keys, not your coins" is appropriate when letting a 3rd party custody your assets.

The risks to wrapping Bitcoin are many and well understood. Even with the above risks, more than 185,000 wBTC trade on the Ethereum blockchain (Solana also holds approximately 16,000 now-defunct wrapped soBTC).[12][13] For comparison, the much-ballyhooed Bitcoin Lightning Network only holds 5,000 BTC in total.[14] The fact that Ethereum's wrapped Bitcoin holds more than 37x the quantity of the Lightning Network's Bitcoin demonstrates the demand for advanced smart contract blockchains.

Bridging

Blockchain programmers have developed cross-chain crypto infrastructure called bridges. So, what is a bridge? A bridge is a piece of software allowing users to interact between different blockchain networks in a decentralized manner. Bridges allow for an entity or individual to transfer assets from one blockchain to another regardless of the code's compatibility. Typically, a user sends ("locks") their native token(s) to a bridge and in exchange receives newly minted "wrapped" tokens that are compatible with the destination blockchain.[15]

[12] https://www.coingecko.com/en/coins/wrapped-bitcoin as of december 20 2022.
[13] https://www.coingecko.com/en/coins/wrapped-bitcoin-sollet as of December 20, 2022.
[14] https://cointelegraph.com/news/bitcoin-lightning-network-capacity-strikes-5-000-btc
[15] https://worldcoin.org/articles/crypto-bridge-hacks

While bridges solve many of the issues trustlessly moving Bitcoin between blockchains, they do not come without risk. According to an August 2022 Chainalysis report, approximately $2 billion in crypto was stolen across 13 bridge hacks. This resulted in an estimated 70% of the funds stolen in 2022. Bridges are an extremely attractive target as they typically feature a central storage point for the funds bridged between blockchains[16]. In 2022 alone, the Nomad Bridge hack fetched $190 million in exploited crypto assets while the Ronin Bridge hack stole an eye-popping $600 million in bridged assets.[17][18]

Centralized Finance

Bitcoiners are no different than other investors. Many expect their BTC capital to be put to productive use. For the less technically inclined, centralized financial ("CeFi") firms offer many of the same services as their DeFi smart contract competitors. Centralized crypto exchanges, lenders, and custodians provide services similar to those found in the traditional financial world. As a result, a considerable number of Bitcoiners place their BTC with CeFi entities.

CeFi firms share all of the same custodian risks as their wrapped Bitcoin alternatives. Additionally, CeFi firms suffer from counterparty risk. Many "on-chain" transparencies provide real-time audit mechanisms such as Proof of Reserves or Proof of Liabilities.[19][20] Counterparty risk, however, is always present with firms that operate off-chain. [21] Trust in leadership, ownership, and the institution itself are the minimum requirements to custody assets. Even then, fraud and financial mismanagement occur as seen with the spectacular implosions of FTX, Blockfi, Voyager, and Celsius earlier this year. Each of the aforementioned CeFi firms suffered from fraud, financial mismanagement, or a combination of the two.

The dust is still settling but the amount of destroyed crypto wealth is in the tens, if not, hundreds of billions of dollars. Whether wrapped, bridged, or CeFi, Bitcoiners face a considerable number of risks putting their BTC to productive use. After 2022's devastation, it would be hard not to exclusively HODL in cold storage while walking away from the industry entirely. Thankfully, the cavalry has arrived. Enter Discreet Log Contracts, a self-wrapped, self-bridged, self-custodied solution to put BTC to productive use.

VI. Solution: Bitcoin smart contracts via Discreet Log Contracts. A self-wrapped, self-bridged, & self-custodied Bitcoin solution

Tadge Dryja, the Bitcoin Lightning Network co-inventor and renowned research scientist at the MIT Digital Currency Initiative, published a seminal whitepaper titled "Discreet Log Contracts." Dryja states,

[16] https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/

[17] https://decrypt.co/106459/crypto-bridge-nomad-exploited-190m-frenzied-free-for-all

[18] https://cointelegraph.com/news/the-aftermath-of-axie-infinity-s-650m-ronin-bridge-hack

[19] https://blog.chain.link/proof-of-reserves/?_ga=2.204404560.1370862830.1671726988-1493302761.1668108969&_gac=1.221998826.1671726988.CjwKCAiAnZCdBhBmEiwA8nDQxSl2NT918vUjEamefLNPZaD_B0LgGumfRR6kOTYAS8YO1ztPJN-hKRoCoBsQAvD_BwE

[20] https://niccarter.info/proof-of-reserves/

[21] https://www.reuters.com/technology/binances-books-are-black-box-filings-show-crypto-giant-tries-rally-confidence-2022-12-19/

> Smart contracts are an often touted feature of cryptographic currency systems such as Bitcoin, but they have yet to see widespread financial use. [One] of the biggest hurdles to their implementation and adoption have been **scalability** of the smart contracts, and the difficulty in getting data external to the currency system into the smart contract. **Privacy** of the contract has been another issue to date. Discreet Log Contracts are a system which addresses the scalability and privacy concerns and seeks to minimize the trust required in the oracle which provides external data. The contracts are discreet in that external observers cannot detect the presence of the contract in the transaction log. They also hinge on knowledge of a *discrete* logarithm, which is a plus.[22]

In short, discreet log contracts ("DLCs") acting as escrow contracts enable conditional payments between two or more parties. The parties can be users, institutions, even smart contracts – any entity with a Bitcoin address. The DLC uses discrete log contracts and the parties' information is kept private, so it is a pun in that it's both "discrete" and "discreet."

How does a DLC work?

An "event" (i.e., wager) dictates the DLC's outcome. That event consists of an **announcement** which sets up the details for a set of predetermined potential outcomes (i.e., win/lose/other) and an **attestation** which identifies one of the outcomes as the official one. An oracle builds and signs the event announcement and attestation. Technically, DLCs function similar to a 2-of-3 multisig wallet in that two signatures are required to execute a transaction.[23] The DLC is created with two parties and a third-party oracle. The oracle participant (i.e., single oracle or multi-oracle setup) attests to the observed reality and referees the transaction.

This oracle is often referred to as a DLC Oracle, but we prefer to use the term Bitcoin Oracle™for wider communities not familiar with the details of the technology, and will thus use that naming convention going forward.

The key to a DLC is the Bitcoin Oracle itself. Unlike a data feed oracle such as Chainlink's that serves prices or other external data, the DLC oracle only has two functions:

(1) At contract creation, the Bitcoin Oracle generates pre-signatures using the users' keys, its own private key and its nonce. A pre-signature is built for each potential contract outcome. For example, a binary outcome (win/lose) will generate two pre-signatures, whereas a more complex outcome will generate *n* pre-signatures or may even generate a formula for computing pre-signatures (i.e., following a continuous distribution).

(2) At contract close, the DLC oracle views the observed outcome and attests to the signature corresponding with that result. This completed signature lets the winning party execute the contract.

[22] https://adiabat.github.io/dlc.pdf

[23] https://support.bitpay.com/hc/en-us/articles/360032618692-What-is-a-Multisignature-Multisig-or-Shared-Wallet-

In addition to DLC data scalability improvements, DLC.Link possesses numerous security improvements, providing highly desirable alternatives to the existing solutions. These include:

Facilitates non-custodial escrow functionality. The parties involved in a contract, including any third party, cannot steal nor compromise the contract since the funds are held in decentralized vaults. This restriction prevents the mismanagement of the underlying BTC collateral. Practically speaking the BTC collateral is held in an escrow wallet. As the possible set of outcomes are predefined and signed by both parties prior to contract setup, a basic misdirection or theft of funds becomes impossible.

Minimizes online attacks. DLCs act as multisig wallets where finality is achieved through an unbiased decentralized oracle network. DLC.Link leverages oracle signatures of transactions as private keys to achieve finality and, by default, only permits the assets in the contracts to be spent.

Eliminates central points of failure. DLCs hold the BTC collateral across multiple escrow accounts, preventing the creation of central points of failure. This removes the single point of failure or vulnerability hackers so routinely exploit with bridges – even when one account is compromised, however, the other accounts can still achieve consensus.

Provides Bitcoin Base-Level Security. Since DLC.Link is built on Bitcoin, all applications, assets, and transactions inherit Bitcoin's base-level security.

The result is a self-wrapped, self-bridged, self-custodied solution for Bitcoin smart contract transactions.

Why now?

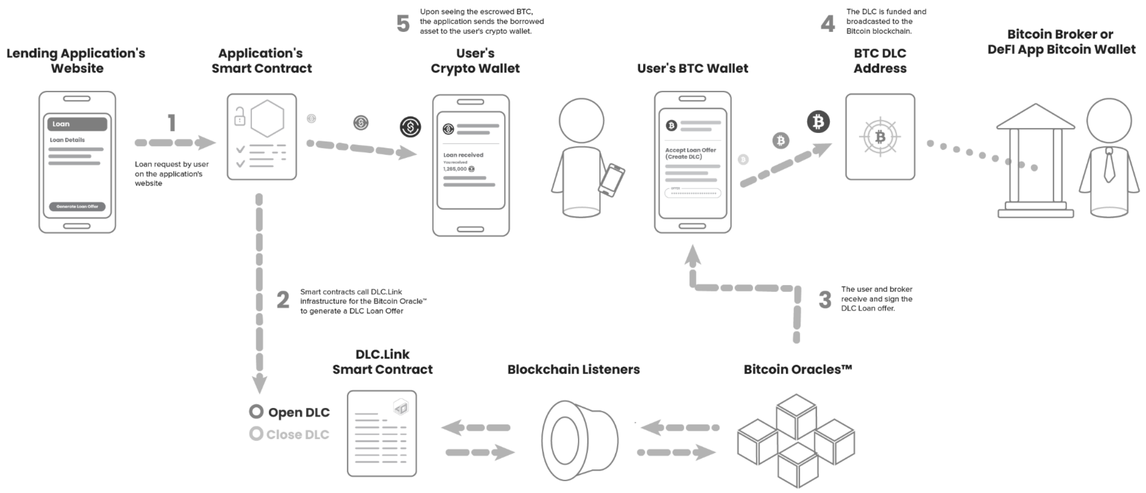
DLCs have been in use for years so why do we care about them now? In fall 2021, Bitcoin received a major update, Taproot, which added support for Point Time Locked Contracts (PTLCs) and Schnorr Signatures. Both of these enable more powerful and streamlined DLCs.[24][25][26][27] An improvement from their predecessor Hash Time Locked Contracts (HTLCs), PTLCs lock Bitcoin to a public key (a point on its elliptical curve) and are unlocked by providing a signature from a satisfied signature adaptor. HTLCs can unwittingly create a link between multiple payments whereas PTLCs can use different keys and signatures, which improves safety while eliminating the risk of correlation. The addition of Schnorr signatures also allows PTLCs to take zero bytes of block space, which significantly reduces its footprint and improves real-world applicability.

VII. Components of DLC.Link

The DLC.Link platform consists of a combination of three main component technologies: The Bitcoin Oracle™, the smart contract layer on a secondary platform (optional), and the wallets that sign the Bitcoin DLC transactions.

[24] https://cointelegraph.com/bitcoin-for-beginners/a-beginners-guide-to-the-bitcoin-taproot-upgrade
[25] https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki
[26] https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki
[27] https://river.com/learn/terms/p/point-timelocked-contract-ptlc/

Setup Loan - Simple Flow



1 Loan request by user on the application's website

2 Smart contracts call DLC.Link infrastructure for the Bitcoin Oracle™ to generate a DLC Loan Offer

3 The user and broker receive and sign the DLC Loan offer.

4 The DLC is funded and broadcasted to the Bitcoin blockchain.

5 Upon seeing the escrowed BTC, the application sends the borrowed asset to the user's crypto wallet.

The Bitcoin Oracle™

The Bitcoin Oracle™ plays the role of mediator by confirming the outcome for DLC participants. Often multiple oracles will be involved in a single contract (DLC), which can require an m-of-n consensus among the selected oracles. This is the primary engine powering DLC.Link's infrastructure. The Bitcoin DLC Oracle™ cryptographically attests to the outcome of events happening in the real world or on other blockchains. Every DLC needs an oracle. The success of DLC.Link's DLC infrastructure will be determined by a vibrant ecosystem of high-quality oracles attesting to outcomes of events outside the Bitcoin blockchain.

The **attestation** of the Bitcoin Oracle, what data it signs and thus picks the winning outcome from the set of possible outcomes in the DLC, is the most critical piece of data in the process. This is why it is recommended, as is a core tenant of web3 infrastructure and theory in general, that a consensus model is used, with multiple Bitcoin Oracles agreeing on an outcome. Any design for determining this outcome via on-chain or off-chain data can be supported by our open-source Bitcoin Oracle model.

In the next section, we will detail our current smart contract solution, which allows for complex smart contracts to generate outcomes, which automatically feed into Bitcoin Oracles and become attested outcomes.

The reader should keep in mind that although we receive outcomes from fully-featured smart contracts on various chains, the DLC paradigm means that DLCs aren't made vulnerable to the highest risk profile of those smart contracts. This is because the possible outcomes in a DLC are predetermined, and once that BTC is locked, only the two participants in the DLC are able to receive those funds, regardless of the form of the data feed used to close the DLC.

DLC.Link will provide open-source software enabling organizations to easily and safely run their own Bitcoin Oracle and participate in the network.

Learn more about this topic in the section What is the Oracle problem? below.

Smart Contracts

Smart contracts are the backbone of the complex thriving ecosystem of DeFi and general web3 development. They communicate between various on-chain sources, including data oracle systems, DeFi/Dapp contracts, and the DLC.Link Management Contract.

Smart contracts on other blockchains such as Ethereum and Stacks are not necessary for running DLCs or powering the Bitcoin Oracles, as that can be done by any automated data source. But when it comes to programmatically moving currency, the decentralized web is usually the best choice.

DLC.Link has launched a smart contract on Ethereum and Stacks, and will soon do the same on other chains. The DLC.Link contract acts as a communication layer between Bitcoin Oracles and smart contracts, and functions similarly to Chainlink's direct-request contracts. This contract allows for interaction with other contracts which wish to leverage DLCs to move and manage native Bitcoin directly from these other chains.

By having a DLC management contract, DLC.Link makes moving BTC powerful and accessible from various chains, while still private and low-fee by keeping the BTC transaction extremely simple and anonymous via DLC technology.

Wallet integration library

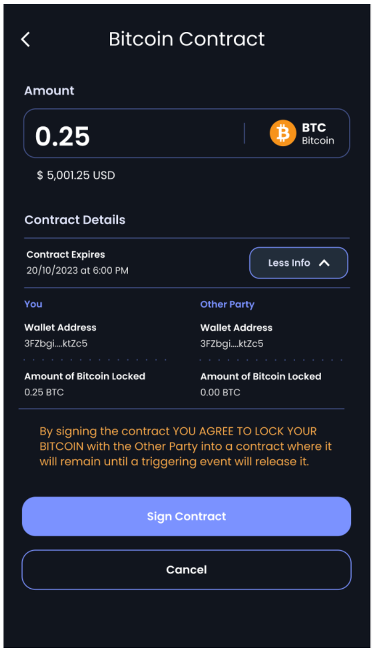
Signing a DLC requires functionality not always present in existing Bitcoin wallets on the market. Therefore, DLC.Link will provide open-source libraries and step-by-step guides for easily integrating DLC signing into existing Bitcoin wallets. Current libraries, based on other public development, are available in the Rust and JavaScript programming languages.

In order to sign a DLC, both participants in the contract need to follow the DLC signing protocol details in the open-source specification[28] found in the footnote below. This process requires the creation of outcomes, and the schorr signature of those by each party. Therefore the DLC.Link library or other similar tool is needed to support DLC signing in a Bitcoin wallet.

The involved Bitcoin wallet need not know any complex details that may be behind the DLC, such as details of the DeFi loan on Ethereum, for example. However, the DLC itself has a minimal set of information, such as the possible outcomes and amount of BTC being locked in the DLC, which should be shown to the user during contract signing.

We have imagined a few mobile app screens to give an idea to the reader about what this DLC signing interface could look like. See below:

[28] https://github.com/discreetlogcontracts/dlcspecs



Bitcoin Contract

Amount

0.25 BTC Bitcoin

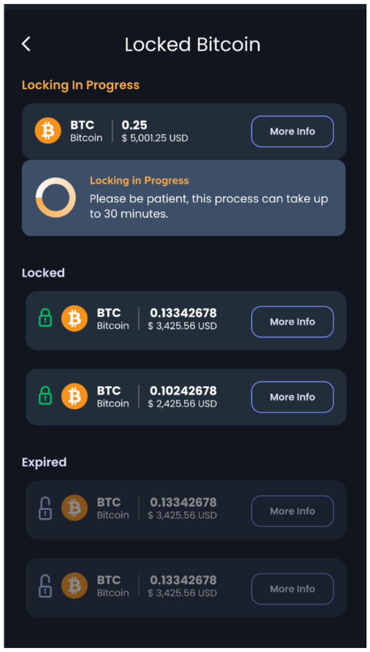
$ 5,001.25 USD

Contract Details

Contract Expires
20/10/2023 at 6:00 PM

You	Other Party
Wallet Address 3FZbgi...ktZc5	Wallet Address 3FZbgi...ktZc5
Amount of Bitcoin Locked 0.25 BTC	Amount of Bitcoin Locked 0.00 BTC

By signing the contract YOU AGREE TO LOCK YOUR BITCOIN with the Other Party into a contract where it will remain until a triggering event will release it.



Locked Bitcoin

Locking In Progress

BTC Bitcoin | 0.25 $ 5,001.25 USD

Locking in Progress
Please be patient, this process can take up to 30 minutes.

Locked

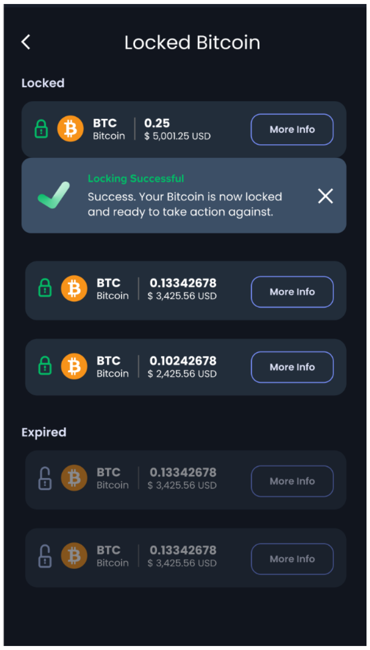
BTC Bitcoin | 0.13342678 $ 3,425.56 USD

BTC Bitcoin | 0.10242678 $ 2,425.56 USD

Expired

BTC Bitcoin | 0.13342678 $ 3,425.56 USD

BTC Bitcoin | 0.13342678 $ 3,425.56 USD



Locked Bitcoin

Locked

BTC Bitcoin | 0.25 $ 5,001.25 USD

Locking Successful
Success. Your Bitcoin is now locked and ready to take action against.

BTC Bitcoin | 0.13342678 $ 3,425.56 USD

BTC Bitcoin | 0.10242678 $ 2,425.56 USD

Expired

BTC Bitcoin | 0.13342678 $ 3,425.56 USD

BTC Bitcoin | 0.13342678 $ 3,425.56 USD

Deposit Token

Bitcoin deposited in a DLC can be represented on another chain via a token. This can be implemented as an NFT, a soulbound token, semi-fungible token, or another specification.

Representing native Bitcoin non-custodially on another blockchain as a token allows for the representation of the asset in the native format on that chain, granting the freedom and power of the contracts on that network. For example, the NFTs can be bought and sold on various NFT marketplaces, and their ownership can be easily transferred.

When the NFT is burned, the corresponding DLC is unlocked and the value flows to the right participant based on who burned the NFT. A simple standard example would include two outcomes. If the NFT is owned/burned by the original participant it pays out fully to that participant. However if it's burned by another wallet, the money flows to the other participant, like a bitcoin broker, who has a payment agreement with the burner.

The metadata details of a deposit token representing Bitcoin in a DLC should include the UUID of the DLC in the Bitcoin Oracle network, the addresses of the participants in the original DLC, and the amount of BTC locked in the DLC.

Cloud Storage for DLCs

One final component of the DLC architecture is a storage platform for the contract execution transactions (CETs) of the DLCs from the various wallets. These are the set of possible outcomes agreed to between the participating wallets. As the CETs are not trivially small (~100KB-5MB per DLC), they are best saved off-chain for privacy and fee reduction, but are nevertheless important to be stored in a robust manner as losing them has implications for a participant being able to sign and close a DLC.

Therefore, a system will be designed to store the CETs for a given transaction securely in the cloud against a hash of a user's bitcoin key, preventing the problem of a potential loss of CETs if a participant was to lose their wallet.

Similar solutions are being designed for Lighting Network node data, and can likely be combined into a similar product.

VIII. What are oracles? What is the difference between a Chinlink and a DLC.Link enabled Bitcoin Oracle? What is the role of a Bitcoin Oracle?

The word "oracle" comes from the Latin verb ōrāre, "to speak" and is usually in reference to a priest or priestess through whom a god is believed to speak. Most notably, oracles have had their place in Greek mythology and been predictors of the future. In the crypto space, Blockchain oracles are entities that connect blockchains to external systems, thereby enabling smart contracts to execute based upon inputs and outputs from the real world.

At the most fundamental level, oracles allow parties to open and execute transactions that settle on a blockchain network. The most well-known oracle provider, Chainlink, offers a decentralized network of nodes that provide data and information to the blockchain. Data feeds can be in the form of any data that isn't natively found on the blockchain, such as the outcome of a sports match, asset price feeds, or historical weather data. DLC.Link offers its own unique decentralized Bitcoin Oracle Network ("BON")™ focused exclusively on Bitcoin. DLC.Link is to Bitcoin what Chainlink is to all smart contracts.

What is a Bitcoin oracle? Bitcoin oracles solve a fundamental constraint of the Bitcoin network - interoperability. The safety and resiliency of the Bitcoin network exists today, partially because it is closed and contained from non-Bitcoin data and components. A Bitcoin oracle communicates with off-chain systems, but still allows for the movement of Bitcoin natively on-chain. In this way, logic that sits either on a decentralized network such as Ethereum or a centralized server is now able to escrow and settle Bitcoin. The practical reality is a decentralized Bitcoin Oracle Network ™ bringing smart contract functionality to Bitcoin.

As we have shown, oracles are an integral element to most applications built on blockchains. They act as bridges passing data back and forth between a blockchain and off-chain real-world systems. Without them, blockchains become siloed systems incapable of change and unable to respond to external events. In addition to simple integrations of public data sources, more interesting use cases emerge when Bitcoin oracles relay information from complex smart-contract systems on other blockchains.

Bitcoin oracles enable countless use cases for transactions requiring non-custodial escrow (trustless 3rd party middleman) and the movement of Bitcoin (capital). Their capacity to allow trustless deposits as well as to integrate with any outside data feed brings an entire new world to Bitcoin's functionality. While oracles enable blockchains to interact with off-chain data sources, they do not, however, come without risks. One well-known risk is the oracle problem.

IX. What is the Oracle problem?

The oracle problem refers to the issue of integrating off-chain data into on-chain smart contracts. Bitcoin transactions, one of the simplest forms of smart contract, typically leverage limited data, including public keys, signatures, timestamps and block sizes. This is reliable as its validity is objective and trustlessly verifiable through the blockchain. Integrating data, for example, like the score of a football match, into a smart contract in a trustless way has proven challenging. Currently, there are no established methods for ensuring the data provided by either the counterparty or the intermediary is authentic.

The core question remains how can off-chain data be trusted? As oracle attestations often come from off-chain sources this is a major concern. If there is only one oracle for a network, this presents a single point of failure. This undermines the true purpose of decentralized applications. This is the crux of the oracle problem. If the Bitcoin oracle goes offline, then data stops flowing on-chain which prevents final settlement on Bitcoin. Worse yet, if the Bitcoin oracle is manipulated, the data sourced from off-chain systems may be compromised. An oracle that publishes incorrect outcomes allows for fraudulent Bitcoin payments to occur defeating the entire purpose of a trustless system.

DLC.Link has developed a solution to this problem. DLC.Link designed a decentralized network of oracles that listen to events from numerous other blockchains which leverages the trustless and decentralized nature of the greater blockchain ecosystem. DLC.Link combines DLCs with proven oracle solutions like Chainlink in order to unlock Bitcoin liquidity without the need for a trusted third party. To successfully bridge the gap between the strongest, decentralized asset, Bitcoin, and other smart contract blockchains, requires numerous Bitcoin oracles to mitigate data inaccuracy, collusion, and downtime. DLC.Link is building the infrastructure for anyone to set-up and run a Bitcoin oracle. As the Bitcoin Oracle Network ™ matures, this will further empower developers and applications on any blockchain or system to accept Bitcoin collateral without any of the implications, restrictions, or risk of using a third-party. Said another way, the combination of DLCs and a Bitcoin Oracle Network ™ remove the need to wrap, bridge, or use CeFi for any BTC related transactions. The DLC.Link infrastructure will serve anyone willing to use BTC as capital for any smart contract conforming to the Bitcoin principle of a trustless monetary system.

X. Who are the parties involved in a DLC transaction? What are some use cases?

[Betting] A simple example of a DLC-enabled escrow contract. Bitcoiners Alicia & Frank want to wager on the outcome the World Cup final. Alicia, an Argentinian, and Frank, a Frenchman, each bet 1 BTC their team wins the World Cup. Alicia & Frank each send one BTC to a DLC-enabled escrow wallet. The escrow wallet securely holds the BTC sent by Alicia & Frank. Additionally, the escrow wallet interacts with a DLC Bitcoin Oracle network to sign the wager transaction. At the end of the game, the DLC Bitcoin Oracle network confirms the final score through an attestation through off-chain data sources (i.e., ESPN, Yahoo Sports, and CNN Sports). After 2 of the 3 “official” news sources confirm the World Cup winner, the Oracle communicates with the escrow contract, triggering a release of 2 BTC to the winner of the wager.

XI. Conclusion

The DLC.Link platform provides essential infrastructure for scalable Bitcoin smart contracts. Discreet log contracts solve each of the problems plaguing today’s custody, bridging, and CeFi solutions. DLCs self-wrap, self-bridge, and self-custody native Bitcoin in trust minimized ways that bolster decentralization and allow for greater self-sovereignty. As a result, DLC.Link expects to usher in a Bitcoin renaissance.