

Bitcoin Lending Protocol

Product Requirements Document

Phase 1: Stacks Mainnet Launch

Version: 1.2 (Multi-Stablecoin Support)

Date: January 2026

Status: Draft for Review

Author: Jamie (Project Lead)

Change Log: - v1.0: Initial draft with incorrect descending auction - v1.1: Corrected to competitive bidding auction mechanism - v1.2: Added multi-stablecoin support (USDA, USDC, xUSD)

Table of Contents

1. Executive Summary
 2. Problem Statement
 3. Solution Overview
 4. User Personas
 5. Feature Requirements
 6. User Interface Requirements
 7. Non-Functional Requirements
 8. Success Metrics
 9. Phase 1 Deliverables
 10. Technical Constraints
 11. Out of Scope
 12. Risk Assessment
 13. Timeline and Budget
-

1. Executive Summary

The Bitcoin Lending Protocol is an open-source, decentralized lending platform that enables Bitcoin holders to borrow against their BTC collateral without selling, while providing stablecoin holders with attractive yield opportunities. Phase 1 delivers a production-ready protocol on Stacks using sBTC collateral, featuring an innovative oracle-free **competitive bidding auction** mechanism that eliminates price manipulation risks inherent in traditional DeFi lending.

Multi-Stablecoin Support

Supported Stablecoins (Phase 1): - **USDA** (Primary) - Arkadiko's native Stacks stablecoin - **USDC** (Secondary) - Bridged USD Coin, institutional stan-

ard

- **xUSD** (Optional) - Additional stablecoin options

Borrowers choose their preferred stablecoin, lenders provide liquidity in that specific stablecoin, giving users flexibility while maintaining the protocol's oracle-free innovation.

Key Innovation

Competitive bidding auctions where lenders compete by bidding lower total repayment amounts, ensuring transparent market-driven pricing without requiring external price oracles. Borrowers set their maximum repayment in their chosen stablecoin, and lenders compete to offer better terms - the lowest bid wins when the auction ends.

Phase 1 Targets

Metric	Target
Launch Timeline	Q2 2026 (7 months)
Initial Loan Volume	\$1M+ in first 3 months
Target Users	Bitcoin miners (borrowers) + DeFi lenders
Active Borrowers	10+ miners in first quarter
Active Lenders	50+ lenders providing liquidity
Average Bids per Auction	3-5 competitive bids
Supported Stablecoins	USDA (primary), USDC, xUSD
Total Budget	\$308,000
Security Audit	Complete before mainnet launch

Strategic Positioning

Phase 1 establishes the protocol on Stacks as the first Bitcoin-native lending platform with oracle-free competitive bidding and flexible multi-stablecoin support. This foundation enables future phases to add native Bitcoin custody (Phase 2) and multi-chain liquidity (Phase 3), positioning the protocol as the definitive solution for Bitcoin-backed lending.

2. Problem Statement

2.1 The Bitcoin Liquidity Challenge

Bitcoin represents over \$2 trillion in market capitalization, yet this capital remains largely idle. Bitcoin holders face an impossible choice: sell their appreciating asset to access liquidity, or hold while missing out on capital deployment opportunities.

This is particularly acute for **Bitcoin miners** who need working capital for:
- Monthly electricity bills (\$20,000-\$100,000+) - Equipment purchases and upgrades - Facility expansion - Operational reserves during price downturns

Current borrowing options force miners to: - Sell BTC at potentially unfavorable prices, crystallizing losses - Use traditional banks (lengthy approval, extensive KYC, no BTC collateral accepted) - Risk custody with centralized lending platforms (Celsius, BlockFi bankruptcies) - Accept unfavorable terms from specialized crypto lenders

2.2 Limitations of Existing DeFi Solutions

Current DeFi lending protocols suffer from critical limitations:

Centralized Wrapped Bitcoin

- **WBTC dependency:** Platforms like Aave and Compound require wrapped BTC
- **Custody risk:** BitGo holds underlying Bitcoin (single point of failure)
- **Regulatory vulnerability:** Centralized custodian subject to seizure/freeze
- **Trust requirement:** Users must trust BitGo won't be compromised

Oracle Dependency Traditional DeFi lending relies on price oracles (Chainlink, Band, etc.) to determine: - Collateral ratios - Liquidation thresholds - Interest rate curves

Oracle risks: - Manipulation during low liquidity periods - Flash loan attacks exploiting price feeds - Centralization through oracle provider dependency - Additional protocol complexity and attack surface - Ongoing costs for oracle subscriptions

Geographic and Regulatory Barriers

- Centralized platforms (BlockFi, Celsius, Genesis) require KYC
- Jurisdictional exclusions (US, China, others)
- Regulatory pressure on centralized entities
- Systemic risks demonstrated by 2022-2023 collapses

2.3 Market Gap

No protocol currently offers: - Bitcoin collateral without wrapped tokens - Oracle-free interest rate discovery - Permissionless, trustless operation - Tradeable loan positions for liquidity - Competitive market-driven rates - Multiple stablecoin options (user choice)

This gap represents our opportunity.

3. Solution Overview

3.1 Core Innovation: Oracle-Free Competitive Bidding

The Bitcoin Lending Protocol eliminates oracle dependency through a **competitive bidding auction mechanism**. Rather than using external price feeds to set interest rates, we let the market discover rates through lenders competing to offer the best terms to borrowers.

How It Works

1. **Borrower** locks sBTC collateral and specifies:
 - Requested loan amount (e.g., \$50,000)
 - **Preferred stablecoin** (USDA, USDC, or xUSD)
 - **Maximum total repayment amount** they're willing to pay (in that stablecoin)
 - Loan duration (e.g., 30, 60, 90 days)
 - Auction duration (e.g., 24 hours for bidding period)
2. **Auction begins** with borrower's maximum repayment as the starting point
 - Example: Borrow \$50,000 USDA, max repayment \$53,500 USDA
 - Implied maximum rate: ~7% APR over 60 days
3. **Lenders compete** by placing bids during the auction period
 - Each bid is a **total repayment amount in the borrower's chosen stablecoin**
 - New bids must be **lower** than the current lowest bid
 - Multiple lenders can bid during the auction window
 - Example bid progression: \$53,500 → \$52,800 → \$51,200 → \$50,500
 - Competition drives the borrower's cost down
4. **Auction ends** after the specified duration (e.g., 24 hours)
 - **Lowest bid wins** the auction
 - Winning lender provides the loan amount in the specified stablecoin
 - Effective interest rate calculated from winning bid
 - Example: \$50,500 repayment on \$50,000 loan over 60 days = 6.17% APR annualized
5. **Loan finalizes** when auction ends with at least one valid bid
 - Stablecoin (USDA/USDC/xUSD) transfers from winning lender to borrower
 - Collateral remains locked in smart contract
 - NFTs minted for both parties (tradeable positions)
 - If no bids received: collateral returns to borrower, auction cancelled

Why This Auction Design Works **Market-Driven Pricing:** - Lenders reveal their true minimum acceptable return through competitive bidding - No artificial rate curves or pre-determined pricing - Borrowers benefit from genuine competition among lenders - Transparent price discovery visible on-chain

Oracle-Free: - No external price feeds required for any part of the system - Interest rates emerge organically from supply and demand - No manipulation vectors through price feeds - No dependency on off-chain data sources

Fair for Both Sides: - Borrowers set their maximum acceptable cost (ceiling) - Lenders compete to win the loan at attractive rates - No one forced to accept unfavorable terms - Either party can walk away (borrower cancels if no bids, lender doesn't bid if rate too low)

Simple and Secure: - No complex liquidation mechanisms needed - No need for real-time price oracles - Straightforward time-based auctions - Lowest bid wins = simple, understandable rule

Example Auction with USDA Borrower Creates Loan Request: - Locks: 1.5 sBTC (worth ~\$150,000 at current prices) - Requests: \$50,000 USDA (chosen stablecoin) - Max repayment: \$53,500 USDA (7% APR equivalent over 60 days) - Loan duration: 60 days (8,640 blocks) - Auction duration: 24 hours (144 blocks)

Lenders Bid During 24-Hour Window:

Time	Lender	Bid (Total Repayment)	Implied APR	Status
Hour 2	Alice	\$53,500 USDA	7.00%	Leading
Hour 8	Bob	\$52,800 USDA	5.60%	Leading
Hour 14	Carol	\$51,200 USDA	2.40%	Leading
Hour 20	Dave	\$50,500 USDA	1.00%	Winner

After 24 Hours: - Dave's bid of \$50,500 USDA is the lowest - Dave wins and provides \$50,000 USDA to borrower - Borrower owes \$50,500 USDA at maturity (60 days) - Effective rate: **1.00% APR** (borrower got excellent terms!) - Dave will earn \$500 profit (\$50,500 - \$50,000)

At Maturity (60 days later): - Borrower repays \$50,500 USDA to Dave - Borrower reclaims 1.5 sBTC collateral - Both NFTs burned, loan complete

3.2 Multi-Stablecoin Flexibility

Supported Stablecoins:

Stablecoin	Type	Key Features	Target Users
USDA	Native Stacks	Deepest liquidity on Stacks, STX-collateralized	DeFi natives, Stacks ecosystem users
USDC	Bridged	Institutional standard, 1:1 USD reserves	Institutions, conservative investors

Stablecoin	Type	Key Features	Target Users
xUSD	Various	Alternative options, diversification	Existing xUSD holders, experimenters

Why Support Multiple Stablecoins?

User Choice: Borrow in stablecoin you already hold (no forced conversion)

Market Fit: Institutions prefer USDC, DeFi users prefer USDA

Flexibility: Protocol adapts as Stacks ecosystem evolves

Risk Diversification: Not dependent on single stablecoin success

Competitive Advantage: More flexible than single-stablecoin protocols

How It Works: - Smart contract maintains whitelist of approved stablecoins - Each loan specifies its stablecoin asset - Lenders must provide liquidity in that specific stablecoin - Market naturally gravitates to most liquid options (likely USDA) - Protocol can add new stablecoins as ecosystem grows

Implementation:

```
;; Borrower creates loan in USDA
(create-loan-auction
  sBTC                ;; collateral
  1.5                 ;; amount
  .usda-token         ;; borrow in USDA
  50000               ;; amount
  53500               ;; max repayment in USDA
  ...)

;; Lender bids in USDA
(place-bid loan-id 51200) ;; Bid 51,200 USDA

;; Winner provides USDA, borrower repays in USDA
```

3.3 Technical Architecture

Phase 1 deploys on **Stacks**, Bitcoin's smart contract layer, using **sBTC** (1:1 Bitcoin-backed asset) as collateral and **multiple stablecoins** (USDA/USDC/xUSD) for loans.

Why Stacks?

- **Bitcoin finality:** Proof of Transfer consensus anchors to Bitcoin
- **Clarity language:** Decidable smart contracts with no reentrancy
- **sBTC integration:** Native 1:1 BTC representation
- **Stablecoin availability:** USDA, USDC, xUSD already on Stacks
- **Lower costs:** ~\$1-5 per transaction vs Ethereum's \$10-100

- **Growing ecosystem:** Mature developer tools and infrastructure

Core Components

Frontend (React)

- Wallet connection (Hiro, Leather, Xverse)
- Stablecoin selection (USDA/USDC/xUSD)
- Auction browsing and bidding interface
- Portfolio management dashboard
- NFT marketplace for trading positions

Stacks.js SDK

Clarity Smart Contracts (Stacks)

Loan Contract	Auction Logic
- Collateral	- Competitive
- Escrow	- Bid handling
- Repayment	- Finalization
- Multi-stable	- Per coin

NFT Contract	Marketplace
- Borrower NFT	- List positions
- Lender NFT	- Purchase
- Transfer	- Price discovery

SIP-010 Token Calls

Asset Contracts

sBTC	USDA	USDC
Collateral	Token	Token

xUSD

Token

Smart Contract Architecture **Core Contract:** `loan-protocol.clar` (all-in-one design) - Collateral locking (sBTC) - **Stablecoin whitelisting** (USDA, USDC, xUSD) - Auction creation (per stablecoin) - Competitive bidding logic - Loan finalization (transfers specific stablecoin) - Repayment processing (receives specific stablecoin) - NFT minting (borrower and lender positions) - Marketplace functions

Asset Contracts: - **sBTC:** Collateral (Bitcoin-backed, 1:1) - **USDA:** Primary stablecoin (Arkadiko) - **USDC:** Secondary stablecoin (bridged) - **xUSD:** Additional stablecoin options

3.4 Oracle-Free Guarantees

By eliminating oracles, we achieve:

No price manipulation: No external feed to attack

No flash loan risk: Bids are explicit amounts, not calculated from oracle prices

Predictable execution: Clarity guarantees prevent surprises

Lower costs: No oracle subscription fees

Simpler architecture: Fewer dependencies = less attack surface

Transparent pricing: Anyone can see all bids on-chain

True competition: Lenders compete on actual terms, not algorithmic curves

5. Feature Requirements

5.1 Core Lending Features (Must Have - P0)

FR1.1: Collateral Locking **Description:** Borrowers must be able to lock sBTC as collateral through smart contract.

Functional Requirements: - Accept sBTC deposits from connected Stacks wallet - Verify collateral is genuinely locked in protocol contract - Emit blockchain event confirming collateral lock with amount and timestamp - Prevent collateral withdrawal until loan is fully repaid or defaults - Support partial collateral returns if borrower wants to reduce loan amount - Display locked collateral amount in user interface

Acceptance Criteria: - [] User can deposit sBTC from wallet with one transaction - [] Contract verifies sBTC balance before allowing loan creation - [] Locked collateral cannot be withdrawn by user or admin - [] Event emission includes: borrower address, amount, timestamp, loan ID - [] UI reflects locked status within 2 seconds of confirmation

FR1.2: Multi-Stablecoin Selection & Whitelisting **Description:** Borrowers must be able to select their preferred stablecoin from approved options.

Functional Requirements: - **Stablecoin Whitelist Management:** - Protocol maintains list of approved stablecoins - Initial whitelist: USDA, USDC, xUSD - Future: Governance can add/remove stablecoins - Each stablecoin validated as SIP-010 compliant

- **Borrower Selection:**
 - Borrower chooses stablecoin when creating loan
 - UI displays stablecoin options with:
 - * Symbol and name (USDA, USDC, xUSD)
 - * Description and key features
 - * User's current balance
 - * Liquidity available in protocol
 - * Recent usage statistics
- **Stablecoin Enforcement:**
 - Loan stores chosen stablecoin asset
 - All bids must be in that stablecoin
 - Repayment must be in same stablecoin
 - UI prevents wrong stablecoin usage

Stablecoin Properties Display:

For each option show:

- Symbol: USDA / USDC / xUSD
- Description: "Native Stacks stablecoin" / "Institutional standard" / "Alternative option"
- Your balance: 125,000 USDA / 50,000 USDC / 0 xUSD
- Protocol liquidity: \$2.5M USDA / \$800K USDC / \$100K xUSD
- Usage: 65% of loans / 30% of loans / 5% of loans

Acceptance Criteria: - [] Borrower can choose from 3+ approved stablecoins - [] Each loan stores its chosen stablecoin (immutable after creation) - [] Contract validates stablecoin is whitelisted before loan creation - [] Lenders can filter auctions by stablecoin - [] UI prominently displays stablecoin throughout loan lifecycle - [] Clear warnings if user lacks balance in chosen stablecoin - [] Protocol owner can update whitelist (emergency only, transparent)

Technical Notes:

```
;; Stablecoin whitelist
(define-map approved-stablecoins principal bool)

;; Initialize with USDA, USDC, xUSD
(map-set approved-stablecoins .usda-token true)
(map-set approved-stablecoins .usdc-token true)
(map-set approved-stablecoins .xusd-token true)
```

```
;; Validation function
(define-read-only (is-stablecoin-approved (token principal))
  (default-to false (map-get? approved-stablecoins token)))
```

FR1.3: Competitive Bidding Auction (Multi-Stablecoin) Description: Implement oracle-free competitive bidding auctions with stablecoin-specific bids.

Functional Requirements: - Borrower specifies **maximum total repayment amount in chosen stablecoin** - Auction duration configurable (default: 24 hours / 144 blocks) - Lenders place bids as **total repayment amounts in the specified stablecoin** - Each new bid must be **lower** than current lowest bid - **Lenders must have sufficient balance** in the required stablecoin - Multiple bids allowed during auction period - Track current lowest bid in smart contract - **Lowest bid wins** when auction ends - If no bids received: collateral returns to borrower, auction fails

Bid Validation Rules:

First bid:

- bid_amount <= max_repayment
- bidder has balance >= bid_amount in correct stablecoin
- stablecoin matches loan's borrow_asset

Subsequent bids:

- bid_amount < current_lowest_bid.amount
- bidder has balance >= bid_amount in correct stablecoin

Time validation:

- current_block < auction_end_block

Stablecoin validation:

- bid is for correct stablecoin (loan.borrow_asset)

Stablecoin-Specific Logic:

```
(define-public (place-bid (loan-id uint) (amount uint))
  (let ((loan (unwrap! (map-get? loans {loan-id: loan-id}) ERR_LOAN_NOT_FOUND)))

    ;; Verify bidder has sufficient balance in correct stablecoin
    (let ((balance (unwrap!
      (contract-call? (get borrow-asset loan) get-balance tx-sender)
      ERR_BALANCE_CHECK_FAILED)))
      (asserts! (>= balance amount) ERR_INSUFFICIENT_STABLECOIN)
    )
  )
```

```

;; Standard bid validation
(asserts! (< amount (get-current-bid-amount loan-id)) ERR_BID_TOO_HIGH)

;; Store bid
(map-set current-bids {loan-id: loan-id} {
  bidder: tx-sender,
  amount: amount
})

(ok true)
)
)

```

Acceptance Criteria: - [] Auction accepts bids for full duration - [] Each bid must be lower than previous (contract enforces) - [] Bids only accepted in loan's specified stablecoin - [] Balance check performed before accepting bid - [] Clear error if insufficient balance: "Need X USDA, have Y USDA" - [] Anyone can query current lowest bid at any time - [] Finalize-auction can only be called after auction-end-block - [] Expired auctions with no bids return collateral automatically - [] Bid placement is gas-efficient (<1000 gas units)

FR1.4: Multi-Stablecoin Loan Finalization **Description:** Transfer the correct stablecoin from winning lender to borrower when auction ends.

Functional Requirements: - Can only finalize after auction-end-block reached - Identifies winner as lowest bidder - **Dynamically calls the correct stablecoin contract** based on loan.borrow_asset - Transfers loan amount in borrower's chosen stablecoin from winner to borrower - Sets repayment amount to winning bid - Mints borrower position NFT - Mints lender position NFT - Changes loan status from "auction" to "active" - Records loan start time for maturity tracking - Emits loan-finalized event with stablecoin details

Dynamic Stablecoin Transfer Logic:

```

(define-public (finalize-auction (loan-id uint))
  (let (
    (loan (unwrap! (map-get? loans {loan-id: loan-id}) ERR_LOAN_NOT_FOUND))
    (winning-bid (unwrap! (map-get? current-bids {loan-id: loan-id}) ERR_NO_BIDS))
    (stablecoin-contract (get borrow-asset loan)) ;; Get stablecoin for THIS loan
  )
    ;; Verify auction has ended
    (asserts! (>= burn-block-height (get auction-end-block loan)) ERR_AUCTION_ACTIVE)

    ;; Transfer in the CORRECT stablecoin (dynamic call)
    (try! (contract-call? stablecoin-contract transfer

```

```

    (get borrow-amount loan)
    (get bidder winning-bid)      ;; From winner
    (get borrower loan)           ;; To borrower
    none))

;; Update loan status
(map-set loans {loan-id: loan-id} (merge loan {
  status: "active",
  lender: (some (get bidder winning-bid)),
  repayment-amount: (get amount winning-bid)
}))

;; Mint NFTs
(try! (nft-mint? borrower-position loan-id (get borrower loan)))
(try! (nft-mint? lender-position loan-id (get bidder winning-bid)))

;; Emit event with stablecoin info
(print {
  event: "auction-finalized",
  loan-id: loan-id,
  winner: (get bidder winning-bid),
  winning-bid: (get amount winning-bid),
  stablecoin: stablecoin-contract
})

(ok true)
)
)

```

Acceptance Criteria: - [] Finalization fails if auction still active - [] Winner correctly identified as lowest bidder - [] **Correct stablecoin contract called** (USDA/USDC/xUSD based on loan) - [] Stablecoin transfer completes atomically - [] Both NFTs minted in same transaction - [] Loan status updated correctly - [] Event includes: loan ID, winner, borrower, amount, **stablecoin used** - [] UI updates within 10 seconds showing active loan with correct stablecoin

Important Note on Finalization Responsibility

Finalization is **not automatic**. Someone must explicitly call `finalize-auction(loan-id)` after the auction ends. Either the borrower or lender can initiate finalization—whichever calls the function pays the gas cost. **If no one finalizes the auction, the collateral and stablecoins remain locked in the contract indefinitely.**

This is by design for Phase 1: both parties are incentivized to finalize (lender wants to earn interest; borrower wants their funds). If neither party follows

through, both parties forfeit the opportunity. This may be addressed in Phase 2 with automated recovery mechanisms.

FR1.5: Multi-Stablecoin Repayment Processing Description: Borrowers must repay loans in the same stablecoin they borrowed.

Functional Requirements: - Calculate current amount owed (winning bid amount) - **Enforce repayment in same stablecoin as loan** (reject wrong stablecoin) - Transfer repayment from borrower to lender (or current NFT holder) - Release sBTC collateral to borrower (or current NFT holder) - Burn or mark NFTs as completed - Update loan status to “repaid” - Emit repayment-complete event - Support early repayment (before maturity) - Support late repayment (after maturity, before collateral claim)

Stablecoin Validation & Transfer:

```
(define-public (repay-loan (loan-id uint))
  (let (
    (loan (unwrap! (map-get? loans {loan-id: loan-id}) ERR_LOAN_NOT_FOUND))
    (borrower-nft-owner (unwrap! (nft-get-owner? borrower-position loan-id) ERR_NOT_BORROWER))
    (lender-nft-owner (unwrap! (nft-get-owner? lender-position loan-id) ERR_NOT_LENDER))
    (stablecoin-contract (get borrow-asset loan))
    (contract-addr (unwrap-panic (var-get contract-address))))
    ;; Verify loan is active
    (asserts! (is-eq (get status loan) "active") ERR_LOAN_NOT_ACTIVE)

    ;; Verify caller is current borrower NFT owner
    (asserts! (is-eq tx-sender borrower-nft-owner) ERR_NOT_BORROWER)

    ;; Transfer repayment in CORRECT stablecoin (dynamic call)
    (try! (contract-call? stablecoin-contract transfer
      (get repayment-amount loan)      ;; Fixed amount from winning bid
      tx-sender                        ;; From borrower
      lender-nft-owner                 ;; To current lender
      none))

    ;; Return collateral (sBTC)
    (try! (as-contract (contract-call? .sbtc-token transfer
      (get collateral-amount loan)
      contract-addr
      borrower-nft-owner
      none)))

    ;; Burn NFTs
```

```

    (try! (nft-burn? borrower-position loan-id borrower-nft-owner))
    (try! (nft-burn? lender-position loan-id lender-nft-owner))

    ;; Update loan status
    (map-set loans {loan-id: loan-id} (merge loan {status: "repaid"}))

    ;; Emit event
    (print {
      event: "loan-repaid",
      loan-id: loan-id,
      borrower: borrower-nft-owner,
      lender: lender-nft-owner,
      repayment-amount: (get repayment-amount loan),
      stablecoin: stablecoin-contract
    })

    (ok true)
  )
)

```

Error Handling:

```

;; If wrong stablecoin attempted (caught by stablecoin transfer failure)
ERR_INSUFFICIENT_STABLECOIN (u420)
;; Error message: "Repayment must be in USDA (loan stablecoin)"

```

Acceptance Criteria: - [] UI shows exact amount owed **in correct stablecoin** - [] Repayment amount never changes (fixed from auction) - [] Early repayment allowed (borrower can repay anytime) - [] Late repayment allowed (until lender claims collateral) - [] Stablecoin transfer to correct lender (original or NFT buyer) - [] Collateral released to correct borrower (original or NFT buyer) - [] Both NFTs burned atomically - [] **Clear error if attempting repayment in wrong stablecoin** - [] Event emission includes amounts, stablecoin, and participants

UI Error Messages:

Wrong Stablecoin
 This loan requires repayment in USDA.
 You attempted to pay with USDC.

Your balances:
 USDA: \$0 (Need \$50,500)
 USDC: \$50,000

Actions:

- Swap USDC → USDA on DEX
- Transfer USDA to your wallet

- List position for sale

[Go to DEX] [Cancel]

6. User Interface Requirements

6.1 Wallet Integration (Must Have - P0)

FR4.1: Stacks Wallet Connection with Multi-Stablecoin Balances
Support Major Wallets: - Hiro Wallet (browser extension + mobile) - Leather Wallet - Xverse Wallet

Functional Requirements: - One-click wallet connection - Show wallet address (truncated) after connection - Display **all token balances:** - sBTC balance (for collateral) - USDA balance - USDC balance - xUSD balance - Disconnect button - Auto-reconnect on page refresh (session persistence) - Handle wallet switching gracefully - Show network status (mainnet/testnet)

Balance Display UI:

Connected: SP1ABC...XYZ [Disconnect]

Your Balances:

sBTC	2.5000
USDA	\$125,000
USDC	\$50,000
xUSD	\$10,000

Total Value: ~\$390,000

Acceptance Criteria: - ☐ User can connect wallet in <3 seconds - ☐ All token balances (sBTC + 3 stablecoins) update within 5 seconds - ☐ Disconnection clears session properly - ☐ Wallet switching detected and UI updates all balances - ☐ Works on mobile and desktop - ☐ Clear error messages for connection failures - ☐ Real-time balance updates when transactions occur

6.2 Borrower Interface (Must Have - P0)

FR4.2: Create Loan Request with Stablecoin Selection Loan Creation Form with Stablecoin Chooser:

Step 1: Choose Stablecoin (Prominent First Step)

Step 1: Choose Your Stablecoin

USDA (Recommended)

Native Stacks stablecoin

- Deepest liquidity on Stacks
- No bridging required
- Best for DeFi users

Your balance: 125,000 USDA

Available liquidity: \$2.5M

USDC

Institutional standard stablecoin

- 1:1 USD reserves (Circle)
- Best for institutions
- Requires bridge from Ethereum

Your balance: 50,000 USDC

Available liquidity: \$800K

xUSD

Alternative stablecoin option

- Diversification
- Experimental

Your balance: 10,000 xUSD

Available liquidity: \$100K

[Continue]

Step 2: Loan Parameters

Create USDA Loan Request

Stablecoin: USDA [Change]

Collateral (sBTC)

[1.5] sBTC

Balance: 2.5 sBTC

Loan Amount (USDA)

[\$50,000] USDA

Maximum Repayment (USDA)

[\$53,500] USDA

→ Implied max APR: 7.0%

Loan Duration

[60 days]

Auction Duration

[24 hours]

Preview:

You lock: 1.5 sBTC

You receive: 50,000 USDA

You owe (max): 53,500 USDA

LTV: 33% (conservative)

Lenders will compete to offer
better rates than your 7.0% max!

[Create Loan Auction]

Validation & Warnings:

Low Stablecoin Balance Warning

You chose USDC but only have \$50,000 USDC.

If you need to repay early or manage the loan,
you may need more USDC.

Consider:

- Choosing USDA (you have \$125,000)
- Acquiring more USDC before borrowing

[Change to USDA] [Continue Anyway]

Acceptance Criteria: - ☐ Stablecoin selection is first step (prominent) - ☐
Each stablecoin option clearly explained - ☐ User balances shown for each option
- ☐ Available protocol liquidity shown - ☐ Form validates input in real-time
- ☐ All amounts shown in chosen stablecoin throughout - ☐ LTV calculation
accurate and updates live - ☐ Implied max APR calculation correct - ☐ Warning
if user has low balance in chosen stablecoin - ☐ Gas fees estimated before
transaction - ☐ Success message shows: auction ID, stablecoin, countdown

FR4.3: Monitor Active Auctions (Stablecoin-Aware) Auction Dashboard for Borrowers:

Your Active Auctions

AUCTION LIVE - Ends in 14h 23m

Loan #42 (USDA Loan)

Stablecoin: USDA

Your max repayment: 53,500 USDA

Current winning bid: 51,200 USDA (4.8% APR)

Bids placed: 3

Bid History:

- 53,200 USDA by 0xABC... (2h ago)
- 52,100 USDA by 0xDEF... (6h ago)
- 51,200 USDA by 0xGHI... (9h ago)

Great! Lenders are competing.

You're getting better than your max!

[View Full Auction] [Cancel]

AUCTION LIVE - Ends in 8h 42m

Loan #45 (USDC Loan)

Stablecoin: USDC

Your max repayment: 107,500 USDC

Current winning bid: 105,000 USDC (9.5% APR)

Bids placed: 5

[View Full Auction] [Cancel]

Acceptance Criteria: - ☐ Dashboard shows all user's auctions - ☐ **Stablecoin prominently displayed** for each auction - ☐ All amounts in correct stablecoin - ☐ Bid updates in real-time - ☐ Timer counts down smoothly - ☐ New bid triggers notification - ☐ Cancel works only before any bids - ☐ Transition to "Active Loan" after auction ends

FR4.4: Manage Active Loans (Multi-Stablecoin) Loan Management Dashboard:

Your Active Loans

USDA Loans (2)

Loan #42 (USDA)

Borrowed: 50,000 USDA
Owe: 50,500 USDA (fixed)
Interest: 500 USDA (1.0% APR)
Due in: 32 days
Collateral: 1.5 sBTC

Your USDA Balance: 125,000 Sufficient

[Repay Now: 50,500 USDA]
[List Position for Sale]

USDC Loans (1)

Loan #45 (USDC)

Borrowed: 100,000 USDC
Owe: 105,000 USDC (fixed)
Interest: 5,000 USDC (9.5% APR)
Due in: 18 days
Collateral: 2.5 sBTC

Your USDC Balance: 45,000 Insufficient
Need: 60,000 more USDC

[Get USDC] [List Position for Sale]

Insufficient Balance Warning:

Insufficient USDC for Repayment

This loan requires: 105,000 USDC
Your USDC balance: 45,000 USDC
You need: 60,000 more USDC

You have in other stablecoins:

- USDA: 125,000 (can swap to USDC)
- xUSD: 10,000

Options:

- Swap USDA → USDC on Stacks DEX
- Bridge USDC from Ethereum
- List borrower position for sale

[Swap on DEX] [List for Sale] [Cancel]

Acceptance Criteria: - ☐ Loans grouped by stablecoin for clarity - ☐ Stablecoin prominently labeled - ☐ Repayment amount shown in correct stablecoin - ☐ Balance check shows sufficiency - ☐ Warning if insufficient balance in required stablecoin - ☐ Helpful suggestions (swap, bridge, sell position) - ☐ Repayment button shows stablecoin requirement - ☐ One-click repayment if sufficient balance - ☐ Collateral release confirmed visually

6.3 Lender Interface (Must Have - P0)

FR4.5: Browse Auctions with Stablecoin Filter Marketplace with Stablecoin Filtering:

Active Loan Auctions

Filter by Stablecoin:

[All (10)] [USDA (6)] [USDC (3)] [xUSD (1)]

Sort by: [Best APR]

Showing USDA Loans (6)

USDA Loan #42 • 14h 23m left

Borrow: \$50,000 USDA

Current: \$51,200 USDA (4.8% APR)

Max: \$53,500 USDA (7.0% APR)

Collateral: 1.5 sBTC (LTV: 67%)

Your profit: \$1,200 USDA

3 bids placed

[Place Bid in USDA]

USDA Loan #38 • 8h 15m left

Borrow: \$25,000 USDA
Current: \$26,100 USDA (8.8% APR)
Max: \$27,000 USDA (12.0% APR)
Collateral: 0.8 sBTC (LTV: 65%)

Your profit: \$1,100 USDA
2 bids placed

[Place Bid in USDA]

[Load More USDA Loans...]

Showing USDC Loans (3)

USDC Loan #45 • 6h 42m left

Borrow: \$100,000 USDC
Current: \$107,500 USDC (9.5% APR)
Max: \$110,000 USDC (12.0% APR)
Collateral: 2.5 sBTC (LTV: 80%)

Your profit: \$7,500 USDC
5 bids placed

[Place Bid in USDC]

[Load More USDC Loans...]

Stablecoin Filter Benefits: - Lenders with USDA focus on USDA loans - Institutional lenders filter to USDC only - See available opportunities in stablecoins you hold - No need to browse irrelevant auctions

Acceptance Criteria: - ☐ Filter tabs work instantly (client-side) - ☐ Badge shows count per stablecoin - ☐ Loans clearly labeled with stablecoin - ☐ All

amounts in correct stablecoin - [] “Place Bid” button shows required stablecoin
- [] Empty state if no loans for selected stablecoin - [] Sorting works within
filtered results - [] Mobile-responsive layout

FR4.6: Place Bids in Specific Stablecoin Bidding Interface with Balance Check:

Place Bid on Loan #42

This loan requires: USDA
Your USDA balance: \$125,000 Sufficient

Current lowest bid: \$51,200 USDA (4.8% APR)
Borrower's max: \$53,500 USDA (7.0% APR)

Your bid (total repayment in USDA):
[\$50,800] USDA
↓
Implied APR: 3.2%
Your profit: \$800 USDA
Status: Valid (beats current by \$400)

Lower bids have better chance to win!

[Submit Bid in USDA]

If Wrong/Insufficient Stablecoin:

Insufficient USDA Balance

This loan requires: USDA
Your USDA balance: \$0
You need: \$51,000 USDA to bid

You have in other stablecoins:

- USDC: \$50,000
- xUSD: \$10,000

Options:

- Swap USDC → USDA on Stacks DEX

- Browse USDC loans instead
- Get USDA from exchange/bridge

[Swap on DEX] [Browse USDC Loans]

Acceptance Criteria: - ☐ Stablecoin requirement prominently displayed - ☐
 Balance check performed in real-time - ☐ Clear error if insufficient balance - ☐
 Helpful suggestions (swap or find matching loans) - ☐ Implied APR updates as
 user types - ☐ Bid validation (must be < current lowest) - ☐ One-click submission
 if balance sufficient - ☐ Transaction confirmed with txid - ☐ Notification
 if outbid later

FR4.7: Lender Portfolio (Multi-Stablecoin) Portfolio Dashboard with Stablecoin Breakdown:

Lender Portfolio Overview

Total Deployed Capital

- USDA: \$75,000 (50%)
- USDC: \$50,000 (33%)
- xUSD: \$25,000 (17%)
- Total: \$150,000

Expected Returns

- USDA: \$79,500 (+\$4,500)
- USDC: \$53,200 (+\$3,200)
- xUSD: \$25,700 (+\$700)
- Total: \$158,400 (+\$8,400)

Portfolio Stats

- Active Loans: 5
- Average APR: 7.2%
- Total Profit Earned: \$2,100
- Next Maturity: 18 days (Loan #45)

USDA Positions (2 loans, \$75,000 deployed)

Loan #42 (USDA)

Lent: \$50,000 USDA
Repay: \$50,800 USDA
Profit: \$800 USDA (3.2% APR)
Due in: 32 days

[\[List for Sale\]](#) [\[Details\]](#)

Loan #38 (USDA)

Lent: \$25,000 USDA
Repay: \$26,100 USDA
Profit: \$1,100 USDA (8.8% APR)
Due in: 18 days

[\[List for Sale\]](#) [\[Details\]](#)

USDC Positions (2 loans, \$50,000 deployed)

Loan #45 (USDC)

Lent: \$30,000 USDC
Repay: \$31,200 USDC
Profit: \$1,200 USDC (8.0% APR)
Due in: 45 days

[\[List for Sale\]](#) [\[Details\]](#)

...

Acceptance Criteria: - ☐ Overview shows breakdown by stablecoin - ☐ All loans grouped by stablecoin - ☐ Expected returns calculated per stablecoin - ☐ Portfolio metrics accurate - ☐ Historical performance tracked - ☐ Export to CSV includes stablecoin data - ☐ Mobile-responsive design

6. User Interface Requirements

6.1 Design Principles

Clarity Over Complexity: - Clean, professional interface prioritizing critical information - Progressive disclosure - show advanced features when needed - Clear visual hierarchy guiding user attention - Mobile-responsive design for all screens

Trust Through Transparency: - All loan terms visible before commitment - Real-time auction progress with live bidding - Clear stablecoin selection and balance displays - Transaction status clearly communicated at every step

Speed and Efficiency: - Minimize clicks to complete core actions - Smart defaults based on common patterns - Quick filters for browsing loans by stablecoin - One-click actions where possible (with confirmation)

6.2 Core User Flows

Flow 1: Wallet Connection Wallet Connection Flow:

```
Landing Page
  ↓
[Connect Wallet Button]
  ↓
Wallet Selection Modal
    Leather Wallet (Recommended)
    Xverse Wallet
    Asigna Wallet
  ↓
Wallet Authorization
  ↓
Dashboard (Authenticated)
```

Wallet Status Display:

Connected: SP2ABC...XYZ

Balances:

- sBTC: 2.5 BTC (~\$125,000)
- USDA: \$15,000
- USDC: \$8,500
- xUSD: \$2,000

Total Value: ~\$150,500

[Disconnect] [Switch Account]

Requirements: - Support Leather, Xverse, Asigna wallets (Stacks ecosystem)
- Display all token balances (sBTC, USDA, USDC, xUSD) - Show total portfolio value in USD - Handle wallet disconnection gracefully - Show pending transactions with status - Mobile wallet support via WalletConnect

Flow 2: Create Loan Request (Borrower) Multi-Step Loan Creation with Stablecoin Selection:

Step 1: Choose Stablecoin

Create New Loan - Step 1: Choose Stablecoin

Which stablecoin do you want to borrow?

USDA (Recommended)
Native Stacks stablecoin
Available liquidity: \$850,000
Typical APR range: 4-8%
Most popular: 65% of loans

USDC
Institutional standard (USD-backed)
Available liquidity: \$320,000
Typical APR range: 5-9%
Usage: 28% of loans

xUSD
Alternative stablecoin option
Available liquidity: \$95,000
Typical APR range: 6-10%
Usage: 7% of loans

Tip: Choose the stablecoin you plan to repay with. USDA has the deepest liquidity.

[Cancel]

[Continue →]

Step 2: Loan Parameters

Create New Loan - Step 2: Loan Details

Borrowing: USDA

Collateral Amount
[1.5] sBTC
\$75,000 at current price
Your balance: 2.5 sBTC

Loan Amount (USDA)
[\$50,000] USDA
LTV: 66.7% Safe (recommended <80%)

Maximum Repayment (USDA)
[\$53,500] USDA
Max APR: 7.0% Competitive
(Market avg: 6.5% for 60-day loans)

Loan Duration
30 days 60 days 90 days

Auction Duration
12 hours 24 hours 48 hours
24 hours recommended for best rates

[← Back]

[Review & Confirm →]

Step 3: Review & Confirm

Review Your Loan Request

Loan Summary

Stablecoin: USDA
You will lock: 1.5 sBTC (~\$75,000)
You will receive: \$50,000 USDA
You will repay: \$50,000 - \$53,500 USDA
(Depends on winning bid)
Loan duration: 60 days
Auction duration: 24 hours

Important Notes:

- Your 1.5 sBTC will be locked immediately
- If no bids received, collateral returns to you
- Winning lender will pay in USDA only
- You MUST repay in USDA to unlock your sBTC
- NFT positions will be minted (tradeable)

Network Fee: ~0.05 STX (~\$0.50)

I understand the terms and risks

[\[← Back\]](#) [\[Confirm & Create Auction\]](#)

Requirements: - Three-step wizard with clear progress indicator (1/3, 2/3, 3/3) - Step 1: Stablecoin selection with liquidity and usage stats - Step 2: Real-time LTV calculation and market comparison - APR calculation from max repayment amount - Input validation at each step - Clear warnings about risks and requirements - Transaction confirmation modal - Success state with link to auction - Error handling for insufficient balance - Mobile-optimized for all steps with touch-friendly controls

Flow 3: Monitor Active Auctions (Borrower View) Live Auction Dashboard:

LIVE AUCTION: Loan #127

Stablecoin: USDA

Your Collateral: 1.5 sBTC (~\$75,000)

Loan Amount: \$50,000 USDA
Your Max Repayment: \$53,500 USDA (7.0% APR)

Time Remaining: 8h 23m 14s
65% complete

Current Winning Bid:

\$51,200 USDA
Winning APR: 4.8%
You save: \$2,300 vs your max!

Bidder: SP2DEF...ABC
Placed: 2 hours ago

Total Bids Received: 4

Bidding History:

- #1: \$53,500 USDA (7.0% APR) - 7h ago
SP2ABC...XYZ
- #2: \$52,800 USDA (5.6% APR) - 5h ago
SP2BCD...YZA
- #3: \$51,800 USDA (3.6% APR) - 3h ago
SP2CDE...ZAB
- #4: \$51,200 USDA (2.4% APR) - 2h ago
SP2DEF...ABC (Current Winner)

[\[Cancel Auction\]](#) [\[View Details\]](#) [\[Share Link\]](#)

Requirements: - Real-time countdown timer with seconds - Visual progress bar showing auction completion - Current lowest bid displayed prominently with large font - Savings vs max repayment calculated and highlighted - Complete bidding history with timestamps - APR calculated for each bid - Stablecoin type clearly displayed throughout - Option to cancel auction (only if no bids and >1 hour remaining) - Mobile push notifications for new bids (opt-in) - Auto-refresh every 10 seconds - WebSocket updates for instant bid notifications - Share link

generator for promoting auction

Flow 4: Browse Auctions (Lender View) Auction Marketplace with Multi-Stablecoin Filtering:

Browse Active Auctions (18 live)

Filter by Stablecoin:

[All (18)] [USDA (12)] [USDC (5)] [xUSD (1)]

Sort: Highest APR Time Left Amount

Your Balances: USDA \$65K | USDC \$45K | xUSD \$8K

Loan #127 USDA

Borrow: \$50,000 USDA
Current Bid: \$51,200 USDA (4.8% APR)
Borrower Max: \$53,500 USDA (7.0% APR)

Collateral: 1.5 sBTC (~\$75,000)
LTV: 66.7% Safe
Duration: 60 days
Time Left: 8h 23m

4 bids • Your balance: \$65,000 USDA

[Place Bid in USDA] [View Details]

Loan #125 USDC

Borrow: \$100,000 USDC
Current Bid: \$107,200 USDC (8.6% APR)
Borrower Max: \$109,000 USDC (9.0% APR)

Collateral: 3.0 sBTC (~\$150,000)
LTV: 66.7% Safe
Duration: 90 days
Time Left: 2h 15m Ending Soon

7 bids • Your balance: \$45,000 USDC
(Insufficient - need \$100K)

[\[Get More USDC\]](#) [\[View Details\]](#)

Loan #124 USDA

Borrow: \$25,000 USDA
Current Bid: \$26,100 USDA (8.8% APR)
Borrower Max: \$27,000 USDA (10.0% APR)

Collateral: 0.8 sBTC (~\$40,000)
LTV: 62.5% Safe
Duration: 30 days
Time Left: 18h 42m

2 bids • Your balance: \$65,000 USDA

[\[Place Bid in USDA\]](#) [\[View Details\]](#)

[\[Load More \(15 remaining\)\]](#)

Requirements: - Filter tabs for each stablecoin with loan counts in real-time - User's balance for each stablecoin shown at top - Stablecoin badge/icon prominently displayed on each card - Sort options: Highest APR, Time Left (urgent first), Loan Amount - Current bid and max bid both visible - APR calculated and displayed for both - Collateral value and LTV with safety indicator - Time remaining with urgency highlighting (<3 hours = "Ending Soon") - Balance sufficiency check per loan - "Place Bid" button shows required stablecoin - Helpful CTAs if insufficient balance (swap, get more, browse others) - Empty state if no auctions in selected stablecoin filter - Pagination or infinite scroll for >20 auctions - Auto-refresh every 15 seconds for live updates - Mobile-responsive

grid layout

Flow 5: Place Bid (Lender Flow) Bidding Modal with Balance Validation:

Scenario A: Sufficient Balance

Place Bid on Loan #127

Required Stablecoin: USDA

Loan Details:

- Loan Amount: \$50,000 USDA
- Duration: 60 days
- Collateral: 1.5 sBTC (~\$75,000, LTV 66.7%)
- Borrower: SP2ABC...XYZ

Current Lowest Bid: \$51,200 USDA (4.8% APR)

Borrower's Max: \$53,500 USDA (7.0% APR)

Time Left: 8h 23m

Your Bid (Total Repayment in USDA):

[\$51,000] USDA

Effective APR: 4.0%

Your profit: \$1,000 USDA in 60 days

Daily return: \$16.67

Valid: Lower than current bid (\$51,200)

Valid: Above minimum (\$50,000)

Your USDA Balance: \$65,000

Required if you win: \$50,000 USDA

Remaining after: \$15,000 USDA

Note: USDA will be locked if you win

[Cancel] [Confirm Bid]

Scenario B: Insufficient Balance

Place Bid on Loan #127

Required Stablecoin: USDA

Insufficient USDA Balance

Your USDA Balance: \$12,000

Required to bid: \$50,000 USDA

Shortfall: \$38,000 USDA

Your Other Assets:

- USDC: \$45,000 (can swap to USDA)
- xUSD: \$8,000 (can swap to USDA)
- STX: 50,000 (~\$50,000, can swap to USDA)

Option 1: Swap to USDA

[Swap \$38K USDC → USDA] (~\$38 fee)

[Swap \$38K STX → USDA] (~\$76 fee)

Option 2: Browse Loans in Your Stablecoins

[Browse USDC Loans (5 active)]

[Browse xUSD Loans (1 active)]

Option 3: Get More USDA

[Buy USDA on DEX] [Deposit More]

[Close]

Requirements: - Stablecoin requirement prominently displayed at top - Balance check before allowing bid submission - Real-time APR calculation as user types bid amount - Profit calculation in stablecoin and daily rate - Validation rules clearly shown: - Bid must be lower than current lowest (or max if first bid) - Bid must be loan amount - Visual indicators for valid/invalid bids - Clear warnings if insufficient balance - Helpful suggestions with one-click actions: - Swap alternatives with estimated fees - Browse loans in stablecoins user already holds - Links to acquire more of required stablecoin - Confirmation

modal after successful bid placement - Transaction hash and Stacks explorer link - Option to set bid notifications (email/push) - Mobile-optimized number input with calculator-style keypad

7. Non-Functional Requirements

7.1 Performance

Metric	Target	Rationale
Page Load Time	< 2 seconds	Users expect fast DeFi UIs
Transaction Confirmation	< 15 seconds	Stacks block time ~10 min, but UI should show pending quickly
Auction Data Refresh	Every 15 seconds	Balance real-time feel with API efficiency
API Response Time	< 500ms (p95)	Maintain responsive user experience
WebSocket Latency	< 200ms	Near-instant bid notifications
Mobile Performance	60 FPS scrolling	Smooth mobile experience

7.2 Security

Requirement	Implementation	Priority
Smart Contract Audit	Professional audit before mainnet (e.g., CoinFabrik, Least Authority)	Critical
Multi-Stablecoin Security	Whitelist validation, balance checks, dynamic call safety	Critical
No Private Keys	Non-custodial - user wallets only	Critical
Input Validation	All user inputs sanitized (amounts, addresses)	Critical
Frontend Security	CSP headers, XSS protection, HTTPS only	High
Rate Limiting	API rate limits to prevent abuse	High
Bug Bounty	Public bug bounty program post-launch	Medium
Monitoring	Real-time transaction monitoring for anomalies	High

7.3 Scalability

Component	Target Capacity	Growth Strategy
Concurrent Users	1,000+ simultaneous	CDN + load balancing
Active Auctions	100+ concurrent	Efficient indexing and caching
Transaction Volume	500+ tx/day	Stacks blockchain native capacity
Database	10,000+ loans history	PostgreSQL with archival strategy
API Throughput	10,000 req/min	Horizontal scaling with Kubernetes
Stablecoin Contracts	3+ simultaneously	Modular contract architecture

7.4 Availability & Reliability

Metric	Target	Implementation
Uptime	99.9% (frontend)	Multi-region deployment, auto-scaling
Smart Contract Uptime	100% (Stacks network)	Decentralized blockchain - no single point of failure
RPC Redundancy	3+ Stacks nodes	Failover between multiple RPC providers
Disaster Recovery	< 1 hour recovery	Automated backups, documented procedures
Zero Downtime Deploys	Required	Blue-green deployment strategy

7.5 Usability

Requirement	Implementation
Mobile Responsive	Mobile-first design, touch-optimized
Wallet Compatibility	Leather, Xverse, Asigna wallets
Internationalization	English (Phase 1), expandable to 5+ languages
Accessibility	WCAG 2.1 Level AA compliance
Error Messages	Clear, actionable error messages with suggestions
Loading States	Skeleton screens, progress indicators
Onboarding	Interactive tutorial for first-time users

Requirement	Implementation
Help Documentation	FAQ, tooltips, video guides

7.6 Monitoring & Observability

Tool/Metric	Purpose
Grafana Dashboards	Real-time metrics (auctions, volume, stablecoin distribution)
Error Tracking	Sentry for frontend errors
Transaction Monitoring	Stacks explorer integration for all transactions
User Analytics	PostHog or Mixpanel for behavior analysis
Alerting	PagerDuty for critical issues
Logs	Centralized logging with ELK stack

7.7 Compliance & Legal

Requirement	Status
Terms of Service	Required before launch
Privacy Policy	GDPR-compliant
Disclaimer	Clear risk warnings displayed
No KYC Required	Permissionless protocol (Phase 1)
Geoblocking	None (decentralized protocol)
Open Source License	GPL-3.0 or MIT (to be determined)

8. Success Metrics

8.1 Phase 1 Key Performance Indicators (KPIs)

Launch Success (Month 1-2)

Metric	Target	Measurement
Testnet to Mainnet Transition	Clean migration	Zero critical bugs in first week

Metric	Target	Measurement
Security Audit	Pass with zero critical issues	Audit report published
First Loan Created	Within 48 hours of launch	Transaction timestamp
First Auction Completed	Within 1 week of launch	Loan #1 finalized
Unique Borrowers	3+ in first month	Unique wallet addresses
Unique Lenders	10+ in first month	Unique wallet addresses

Growth Metrics (Month 3-6)

Metric	Target	Measurement Method
Total Loan Volume	\$1M+ by Month 6	Sum of all loan amounts
Active Loans	15+ concurrent	Loans in “active” status
Average Loan Size	\$50K-\$100K	Mean loan amount
Repeat Borrowers	50%+	Borrowers with 2+ loans
Repeat Lenders	60%+	Lenders with 2+ loans
Protocol TVL	\$500K+ locked	sBTC collateral value

Stablecoin Adoption (NEW - Multi-Stablecoin Metrics)

Metric	Target	Rationale
USDA Market Share	55-70% of volume	Primary stablecoin, best liquidity
USDC Market Share	20-35% of volume	Institutional demand
xUSD Market Share	5-15% of volume	Alternative preference
Stablecoin Diversity	2+ used regularly	Healthy multi-coin ecosystem
Cross-Stablecoin Swaps	Track swaps initiated from UI	User behavior insight

Auction Performance

Metric	Target	Calculation
Average Bids per Auction	3-5 bids	Total bids / total auctions

Metric	Target	Calculation
Auction Success Rate	>90% receive bids	Auctions with 1 bid / total auctions
Average APR (Winning)	4-8%	Mean APR of finalized loans
Auction Duration Preference	70%+ choose 24 hours	Modal auction duration
Bid Competition	50%+ auctions have 3+ bids	Healthy competition indicator

User Engagement

Metric	Target	Tracking
Daily Active Users (DAU)	50+ by Month 6	Unique daily wallet connections
Weekly Active Users (WAU)	150+ by Month 6	Unique weekly wallet connections
Retention (30-day)	>40%	Users active in Month 2 who started in Month 1
Session Duration	5+ minutes average	Time spent on platform
Bounce Rate	<40%	Single-page visits

Financial Health

Metric	Target	Formula
Default Rate	<2%	Defaulted loans / total loans
Repayment Rate	>98%	Repaid loans / matured loans
Average LTV	60-70%	Mean collateral / loan ratio
Protocol Revenue	Track for future	Currently zero (no fees Phase 1)

8.2 Success Milestones

Month 1: Launch Success - Mainnet deployment with zero critical bugs - Security audit published (zero critical findings) - First 3 loans created and funded - All 3 stablecoins used at least once

Month 2: Early Traction - 10+ unique borrowers - 30+ unique lenders - \$250K+ total volume - First loan successfully repaid

Month 3: Product-Market Fit Signals - 50% of borrowers return for second loan - Average 4+ bids per auction - Mining conference attendance (Mining Disrupt Miami or similar) - Positive community feedback on social media

Month 4-6: Growth Phase - \$1M+ cumulative volume - 15+ concurrent active loans - Partnership with 1+ mining pool or large miner - Featured on Stacks ecosystem platforms

8.3 Testing & Quality Metrics (NEW)

Metric	Target	Purpose
Test Coverage	>95%	Comprehensive test coverage across all stablecoin scenarios
Unit Test Pass Rate	100%	All unit tests passing before deployment
Integration Test Pass Rate	100%	End-to-end flows validated
Stablecoin Test Scenarios	15+ test cases	USDA, USDC, xUSD fully tested
Load Test Results	1000+ concurrent users	Platform handles peak load
Security Scan Results	Zero critical vulnerabilities	Automated security scanning

8.4 Community & Marketing Metrics

Metric	Target (Month 6)	Channel
Twitter Followers	1,000+	@BitcoinLendingProtocol
Discord Members	500+	Community discord
Documentation Views	5,000+ monthly	Docs site analytics
Press Mentions	3+ articles	Bitcoin/DeFi media
Conference Presentations	2+ events	Mining Disrupt, Stacks events
Partnership Announcements	2+ integrations	Stacks ecosystem partners

8.5 Failure Criteria (Red Flags)

These metrics indicate need for pivot or intervention:

Metric	Threshold	Action
No loans after 2 weeks	0 loans	Revisit marketing, pricing
High cancellation rate	>50% auctions cancelled	Improve lender acquisition
Default rate spike	>5%	Tighten LTV requirements
Single stablecoin dominance	>90% in one coin	Investigate why others unused
Zero repeat users	<10% repeat	UX issues, poor experience
Critical bugs	Any that risk funds	Immediate pause and fix

9. Phase 1 Deliverables

9.1 Deliverable Overview

Phase 1 consists of **11 core deliverables** across smart contracts, frontend, security, testing, and business development. Total budget: **\$308,000** over **7 months**.

Code	Deliverable	Month	Duration	Cost	Status
D1.1	Security Audit (Enhanced)	1-3	2.0 mo	\$88,000	Planned
D1.2	Stacks Mainnet Deploy	1	0.7 mo	\$34,000	Planned
D1.3	sBTC Collateral Integration	1	0.6 mo	\$23,000	Planned
D1.4	Competitive Bidding Auction	2	0.6 mo	\$23,000	Planned
D1.5	NFT Positions Trading	2-3	0.6 mo	\$23,000	Planned
D1.9	Multi-Stablecoin Integration	2-3	1.5 mo	\$44,000	NEW
D1.5a	Lending/Borrowing UI (Enhanced)	3-5	2.0 mo	\$24,000	Expanded

Code	Deliverable	Month	Duration	Cost	Status
D1.5b	NFT Marketplace UI	3-5	1.2 mo	\$15,000	Planned
D1.10	Stablecoin Testing Suite	4-5	1.0 mo	\$8,000	NEW
D1.6	Miner Outreach & BD	3-7	5.0 mo	\$17,000	Planned
D1.7	\$1M Volume Milestone	7	1.0 mo	\$9,000	Planned
	TOTAL	0-7	7 months	\$308,000	

9.2 Detailed Deliverable Specifications

D1.1: Security Audit (Enhanced) - \$88,000 Scope Expansion: Original audit budget increased by \$10,000 to cover multi-stablecoin complexity.

Audit Coverage: - Core lending protocol logic - Competitive bidding auction mechanism - **Multi-stablecoin whitelist management (NEW)** - **Dynamic stablecoin contract calls (NEW)** - **Balance validation across stablecoins (NEW)** - NFT minting and trading - Collateral lockup and release - Edge cases and attack vectors

Deliverables: - Comprehensive audit report - List of findings (critical, high, medium, low) - Remediation recommendations - Follow-up review after fixes implemented - Public publication of audit report

Acceptance Criteria: - [] Zero critical vulnerabilities - [] All high-severity issues resolved - [] Audit report publicly published - [] Smart contracts deployed to mainnet only after clean audit

Timeline: Months 1-3 (2 months)

Budget: \$88,000 (\$78K original + \$10K multi-stablecoin)

D1.2: Stacks Mainnet Deploy - \$34,000 Description: Deploy all smart contracts to Stacks mainnet with proper initialization.

Components: - Main loan protocol contract - NFT contracts (borrower + lender positions) - Stablecoin whitelist initialization - Contract ownership and admin setup - Integration with Stacks ecosystem

Deliverables: - Deployed contracts on Stacks mainnet - Contract addresses documented - Admin keys properly secured - Deployment verification scripts - Mainnet monitoring setup

Acceptance Criteria: - ☐ All contracts deployed successfully - ☐ Contract verification on Stacks explorer - ☐ Ownership transferred correctly - ☐ Integration tests passing on mainnet - ☐ Monitoring and alerts configured

Timeline: Month 1 (0.7 months)

Budget: \$34,000

D1.3: sBTC Collateral Integration - \$23,000 Description: Integrate sBTC as the collateral asset with proper lockup/release mechanisms.

Components: - sBTC contract integration - Collateral deposit functionality - Collateral withdrawal on repayment - Collateral claim on default - LTV calculation and validation

Deliverables: - Working sBTC deposit flow - Collateral release mechanism - Default handling logic - Integration tests - Documentation

Acceptance Criteria: - ☐ Borrowers can lock sBTC as collateral - ☐ Collateral automatically released on repayment - ☐ Lenders can claim collateral on default - ☐ LTV calculations accurate - ☐ Edge cases handled (reorgs, etc.)

Timeline: Month 1 (0.6 months)

Budget: \$23,000

D1.4: Competitive Bidding Auction - \$23,000 Description: Implement competitive bidding auction mechanism for interest rate discovery.

Components: - Auction creation logic - Bid placement and validation - Lowest-bid-wins logic - Auction finalization - Time-based auction expiry

Deliverables: - Working auction smart contract - Bid validation rules - Auction state management - Finalization mechanism - Comprehensive tests

Acceptance Criteria: - ☐ Borrowers can create auctions with parameters - ☐ Lenders can place competitive bids - ☐ Only valid bids accepted (lower than current) - ☐ Auction finalizes correctly at expiry - ☐ Winner determined and loan activated

Timeline: Month 2 (0.6 months)

Budget: \$23,000

D1.5: NFT Positions Trading - \$23,000 Description: Implement SIP-009 NFTs for tradeable loan positions.

Components: - Borrower position NFTs - Lender position NFTs - NFT transfer logic - Position ownership validation - Marketplace-ready metadata

Deliverables: - SIP-009 compliant NFT contracts - NFT minting on loan finalization - NFT burning on loan completion - Transfer functionality - Metadata with loan details

Acceptance Criteria: - ☐ NFTs minted for both parties on loan activation - ☐ NFTs can be transferred/sold - ☐ Position ownership validated for repayment/claim - ☐ NFTs burned on loan completion - ☐ Metadata displays loan info correctly

Timeline: Months 2-3 (0.6 months)

Budget: \$23,000

D1.9: Multi-Stablecoin Integration (NEW) - \$44,000 Description: Full implementation of multi-stablecoin support (USDA, USDC, xUSD) throughout the protocol.

Components: - Stablecoin whitelist smart contract - Dynamic stablecoin contract calls - Per-loan stablecoin storage - Balance validation before bids/repayments - Frontend stablecoin selection UI - Stablecoin filtering and grouping

Deliverables: - Whitelist management contract - Updated loan contract with stablecoin field - USDA integration (primary) - USDC integration (secondary) - xUSD integration (optional) - Frontend stablecoin selector - Stablecoin filter components - Balance check UI components

Acceptance Criteria: - ☐ Users can choose stablecoin when creating loan - ☐ Whitelist prevents unapproved stablecoins - ☐ Dynamic transfers work for all 3 stablecoins - ☐ Balance checks prevent insufficient bids - ☐ Frontend clearly displays stablecoin type - ☐ Filters work correctly (All/USDA/USDC/xUSD) - ☐ Loans group by stablecoin in UI

Timeline: Months 2-3 (1.5 months)

Budget: \$44,000 (NEW deliverable)

D1.5a: Lending/Borrowing UI (Enhanced) - \$24,000 Description: React-based frontend for core lending and borrowing flows, expanded to support multi-stablecoin.

Components: - Wallet connection (Leather, Xverse, Asigna) - Create loan wizard (3 steps with stablecoin selection) - Browse auctions with stablecoin filters - Place bid modal with balance checks - Active loan management - Repayment interface - Balance displays for all stablecoins

Deliverables: - Complete borrower flow - Complete lender flow - Mobile-responsive design - Stablecoin selection and filtering - Real-time auction updates

- Transaction status tracking

Acceptance Criteria: - [] Users can connect wallet - [] Borrowers can create loans in any stablecoin - [] Lenders can browse and filter by stablecoin - [] Lenders can place bids with balance validation - [] Real-time auction countdown works - [] Repayment flow validates correct stablecoin - [] Mobile-friendly on all screen sizes

Timeline: Months 3-5 (2.0 months, expanded from 1.5)

Budget: \$24,000 (expanded from \$18K)

D1.5b: NFT Marketplace UI - \$15,000 **Description:** Frontend for trading NFT loan positions (borrower and lender).

Components: - List NFT for sale interface - Browse marketplace listings - Buy NFT flow - Pricing and offer system - Position transfer handling

Deliverables: - NFT listing interface - Marketplace browse page - Purchase flow - Price discovery mechanism - Transfer confirmation

Acceptance Criteria: - [] Users can list their NFTs with asking price - [] Marketplace displays all listings - [] Users can buy listed NFTs - [] Transfer occurs correctly - [] Loan ownership updates after transfer

Timeline: Months 3-5 (1.2 months)

Budget: \$15,000

D1.10: Stablecoin Testing Suite (NEW) - \$8,000 **Description:** Comprehensive testing across all stablecoin scenarios to ensure multi-stablecoin functionality.

Components: - Unit tests for each stablecoin (USDA, USDC, xUSD) - Integration tests for stablecoin switching - Edge case testing (wrong stablecoin, insufficient balance) - Cross-stablecoin scenario tests - Load testing with multiple stablecoins

Deliverables: - 15+ stablecoin-specific test cases - Automated test suite - Test coverage report (target >95%) - Edge case documentation - Load test results

Acceptance Criteria: - [] All USDA flows tested - [] All USDC flows tested - [] All xUSD flows tested - [] Wrong stablecoin rejection tested - [] Balance insufficiency tested - [] Mixed stablecoin portfolio tested - [] >95% code coverage achieved

Timeline: Months 4-5 (1.0 month)

Budget: \$8,000 (NEW deliverable)

D1.6: Miner Outreach & Business Development - \$17,000 **Description:** Target acquisition of Bitcoin miner borrowers and establish partnerships.

Components: - Mining conference attendance (Mining Disrupt, BTC Prague)
- Direct outreach to mining operations - Educational content for miners - Partnership discussions - Community building

Deliverables: - 3+ miner conversations per week - Attendance at 2+ mining conferences - Educational blog posts/videos - Partnership MOU with 1+ miner
- First 10+ borrowers onboarded

Acceptance Criteria: - ☐ 10+ miners aware of protocol - ☐ 3+ miners actively using protocol - ☐ Conference presentations delivered - ☐ Educational content published - ☐ Community Discord active

Timeline: Months 3-7 (5 months, parallel)

Budget: \$17,000

D1.7: \$1M Volume Milestone - \$9,000 **Description:** Achieve \$1M+ cumulative loan volume by end of Phase 1.

Components: - Volume tracking dashboard - Liquidity incentives (if needed)
- Marketing campaigns - Lender acquisition - Performance analytics

Deliverables: - Volume dashboard - Marketing materials - Lender outreach results - Milestone achievement documentation

Acceptance Criteria: - ☐ \$1M+ cumulative loan volume - ☐ Volume distributed across stablecoins - ☐ 15+ active loans - ☐ Sustainable growth trajectory - ☐ Positive user feedback

Timeline: Month 7 (1 month)

Budget: \$9,000

10. Technical Constraints

10.1 Blockchain Constraints

Stacks Blockchain: - Block time: ~10 minutes (slower than Ethereum) - Transaction throughput: ~100-200 TPS - Smart contract language: Clarity (not Solidity) - Gas costs: Paid in STX (fluctuates with STX price) - Finality: Anchored to Bitcoin (high security, slower confirmation)

sBTC Constraints: - Peg mechanism: Must trust sBTC peg operators (Phase 1) - Availability: sBTC must be live on Stacks mainnet - Liquidity: sBTC liquidity determines max loan sizes - Conversion: Users must convert BTC → sBTC before use

Multi-Stablecoin Constraints: - USDA: Availability and liquidity on Stacks (currently live) - USDC: Requires bridge to Stacks (bridge trust assumptions) - xUSD: Availability TBD (may launch with 2 stablecoins if not available) - Whitelist: Can only add stablecoins that are SIP-010 compliant

10.2 Smart Contract Constraints

Clarity Language Limitations: - No loops (prevents infinite gas attacks, but limits flexibility) - No recursion - No floating point math (all integer-based) - Limited string manipulation - No inter-contract calls to non-whitelisted contracts

Implications for Protocol: - Must batch operations carefully - Fixed-point math for interest calculations - Pre-compute or limit array operations - Carefully design contract interactions

10.3 Frontend Constraints

Wallet Support: - Must integrate with Stacks wallets (Leather, Xverse, Asigna) - Different wallet APIs require separate integration code - Mobile wallet support via WalletConnect

Real-time Updates: - Stacks blocks every ~10 minutes limits real-time feel - WebSocket connections needed for push updates - API polling as fallback (every 15-30 seconds)

Browser Compatibility: - Must support modern browsers (Chrome, Firefox, Safari, Edge) - Mobile browsers (iOS Safari, Android Chrome) - No IE support required

10.4 Integration Constraints

Third-Party Dependencies: - Stacks.js library for blockchain interaction - sBTC contract (must be live and stable) - Stablecoin contracts (USDA, USDC, xUSD) - Wallet providers (Leather, Xverse, Asigna) - RPC node providers (for API calls)

API Dependencies: - Stacks blockchain API (Hiro API) - Price feed for USD/BTC conversion (display only, not protocol-critical) - IPFS or similar for NFT metadata storage

10.5 Security Constraints

Non-Custodial Requirement: - Protocol cannot hold private keys - All funds controlled by smart contracts or user wallets - No trusted intermediaries for core functions

Audit Requirements: - Must complete professional security audit before mainnet - Cannot launch with critical or high-severity vulnerabilities - Must

address all audit findings

Testing Requirements: - Comprehensive test coverage (>95%) - Testnet deployment and testing before mainnet - Multi-stablecoin scenarios fully tested

11. Out of Scope

11.1 Features Explicitly Excluded from Phase 1

The following features are **intentionally excluded** from Phase 1 to maintain focus and ship quickly:

Native Bitcoin Custody

- **Not in Phase 1:** Direct Bitcoin collateral without sBTC wrapper
- **Rationale:** Requires complex threshold signature infrastructure (validator network)
- **Timeline:** Phase 2 (Months 8-16)
- **Why Wait:** sBTC provides sufficient functionality for initial launch and validation

Multi-Chain Deployment

- **Not in Phase 1:** Ethereum, Solana, Base, or other chains
- **Rationale:** Need to validate product-market fit on Stacks first
- **Timeline:** Phase 3 (Months 18-28)
- **Why Wait:** Multi-chain adds significant complexity and dilutes focus

Automated Liquidations

- **Not in Phase 1:** Automatic collateral liquidation based on price feeds
- **Rationale:** Requires oracle integration (contradicts oracle-free design)
- **Alternative:** Manual default handling after loan maturity
- **Why:** Oracle-free is core innovation; liquidations add complexity without immediate need

Flash Loans

- **Not in Phase 1:** Single-block loans without collateral
- **Rationale:** Increases attack surface and audit scope significantly
- **Timeline:** Possibly Phase 2 or 3 if demand exists
- **Why Wait:** Not core to target user base (miners need longer-term loans)

Governance Token

- **Not in Phase 1:** Protocol governance token or DAO structure
- **Rationale:** Premature for MVP; adds regulatory complexity

- **Timeline:** Phase 3 or beyond (if needed)
- **Why Wait:** Focus on core product first, governance later

Variable Interest Rates

- **Not in Phase 1:** Interest rates that change during loan period
- **Rationale:** Adds complexity; fixed rates simpler for MVP
- **Alternative:** Competitive bidding sets rate at auction start
- **Why:** Users prefer predictability in early version

Partial Loan Repayments

- **Not in Phase 1:** Ability to repay loan in installments
- **Rationale:** Increases smart contract complexity
- **Alternative:** Full repayment only at maturity
- **Why Wait:** Most miners prefer lump-sum repayment anyway

Credit Scoring / Reputation System

- **Not in Phase 1:** On-chain credit scores or borrower ratings
- **Rationale:** Insufficient data in early stages
- **Timeline:** Phase 2 or 3 after sufficient loan history
- **Why Wait:** Need loan data first to build meaningful scores

Stablecoin Swaps Within Protocol

- **Not in Phase 1:** Built-in DEX for swapping between USDA/USDC/xUSD
- **Rationale:** Existing Stacks DEXes (Velar, ALEX) serve this purpose
- **Alternative:** Direct users to external DEXes
- **Why:** Don't reinvent the wheel; focus on core lending innovation

Loan Extensions / Refinancing

- **Not in Phase 1:** Ability to extend loan duration or refinance
- **Rationale:** Adds complexity to auction and repayment logic
- **Timeline:** Phase 2 if user demand exists
- **Why Wait:** Validate core product first

Mobile Native App

- **Not in Phase 1:** iOS/Android native applications
- **Alternative:** Mobile-responsive web app (PWA)
- **Rationale:** Web-first is faster to build and maintain
- **Timeline:** Phase 3 if usage warrants investment

Institutional KYC/AML

- **Not in Phase 1:** KYC/AML compliance for institutional users
- **Rationale:** Permissionless protocol is core value proposition
- **Timeline:** Separate enterprise offering (if needed) in Phase 3+
- **Why:** Regulatory complexity better addressed once core product validated

11.2 Limitations Accepted for Phase 1

These are known limitations we accept to ship faster:

Stablecoin Limitations

- **Limitation:** Only USDA, USDC, xUSD supported (not all stablecoins)
- **Impact:** Some users may want USDT, DAI, or others
- **Mitigation:** Start with 3 most liquid options, expand based on demand
- **Acceptable:** 3 stablecoins covers 90%+ of likely user preferences

Collateral Type

- **Limitation:** Only sBTC accepted as collateral (not BTC, STX, or other assets)
- **Impact:** Users must convert BTC → sBTC first
- **Mitigation:** Clear instructions for sBTC conversion
- **Acceptable:** sBTC is the standard for Bitcoin on Stacks

Loan Sizes

- **Limitation:** Practical maximum loan size limited by sBTC liquidity
- **Impact:** Large miners (\$5M+) may not find sufficient liquidity
- **Mitigation:** Start with \$50K-\$500K range, grow over time
- **Acceptable:** Most miners need <\$500K working capital

Gas Costs

- **Limitation:** Stacks transaction fees paid in STX (user must hold STX)
- **Impact:** Users need small amount of STX for gas
- **Mitigation:** Clear warning in UI; faucet for small amounts
- **Acceptable:** Standard for all Stacks dApps

Block Time / Finality

- **Limitation:** ~10 minute block times (slower than Ethereum)
- **Impact:** Transactions take longer to confirm
- **Mitigation:** Clear pending states in UI; optimistic updates
- **Acceptable:** Security benefit of Bitcoin anchoring outweighs speed

Auction Duration Constraints

- **Limitation:** Minimum auction duration 12 hours (due to block times)
- **Impact:** Can't do ultra-fast auctions like 1-hour
- **Mitigation:** Offer 12h / 24h / 48h options
- **Acceptable:** 24 hours is optimal for most use cases anyway

“Automatic Auction Finalization”

- **Limitation:** Auction finalization is not automatic—someone must explicitly call `finalize-auction()`
 - **Rationale:** Stacks contracts cannot auto-execute. No cron jobs, scheduled tasks, or validators watching for triggers.
 - **Impact:** If neither borrower nor lender calls finalize after auction ends, assets remain locked indefinitely
 - **Mitigation:** Both parties are strongly incentivized to finalize (lender wants to earn interest; borrower wants funds). UX prompts encourage finalization. Worst case: both lose the opportunity, but collateral is safe.
 - **Future Enhancement:** Phase 2 may add recovery mechanisms (expiry deadlines, permissionless finalization with refunds, etc.) if this becomes a real-world problem
 - **Acceptable for Phase 1:** Self-interested behavior ensures most auctions finalize. This is a feature (no automatic costs) rather than a bug.
-

11.3 Future Considerations

Features we're tracking for future phases but not committing to:

- **Undercollateralized Loans:** For high-reputation borrowers (requires credit scoring)
 - **Interest-Only Loans:** Pay interest periodically, principal at end
 - **Collateral Diversification:** Accept multiple collateral types in one loan
 - **Cross-Collateral Loans:** Use multiple collateral assets
 - **Synthetic Assets:** Loan denominated in BTC, paid in stablecoin
 - **Insurance Pools:** Lender insurance against defaults
 - **Yield Aggregators:** Auto-reinvest loan returns
 - **Social Features:** Borrower profiles, reviews, direct messaging
 - **Advanced Analytics:** Historical APR charts, yield comparisons
 - **API for Integrations:** Programmatic access for partners
 - **White-Label Solutions:** Customizable frontend for partners
-

12. Risk Assessment

12.1 Technical Risks

Risk 1: Smart Contract Vulnerabilities **Description:** Critical bug in smart contracts could lead to loss of user funds.

Likelihood: Low (with professional audit)

Impact: Critical (protocol failure, loss of funds)

Risk Score: HIGH

Mitigation Strategies: - Professional security audit before mainnet (Coin-Fabrik, Least Authority, or similar) - Public bug bounty program post-launch (\$50K+ rewards) - Gradual rollout with small loan caps initially (\$50K max first month) - Circuit breaker mechanism for emergency pause - Multi-signature controls for critical functions - Comprehensive test coverage (>95%) - Testnet deployment and testing (2+ months)

Residual Risk: Low after mitigations

Risk 2: Multi-Stablecoin Integration Bugs **Description:** Errors in dynamic stablecoin contract calls or balance validation could allow wrong stablecoin usage or insufficient funds.

Likelihood: Medium (new complex feature)

Impact: High (user funds at risk, UX broken)

Risk Score: HIGH

Mitigation Strategies: - Enhanced audit scope specifically covering multi-stablecoin logic (+\$10K budget) - Whitelist validation prevents unapproved tokens - Balance checks before every bid and repayment - Comprehensive test suite (D1.10) with 15+ stablecoin scenarios - Staged rollout: Launch with USDA only, add USDC/xUSD week 2 - Clear UI warnings when wrong stablecoin or insufficient balance - Integration tests for all stablecoin combinations

Residual Risk: Low after mitigations

Risk 3: sBTC Peg Failure **Description:** sBTC loses peg to Bitcoin, collateral value becomes unstable.

Likelihood: Low (but not zero)

Impact: High (collateral value uncertainty)

Risk Score: MEDIUM

Mitigation Strategies: - This is a systemic risk we must accept for Phase 1 - Clear disclaimers to users about sBTC trust assumptions - Monitor sBTC peg health via dashboard - Conservative LTV ratios (recommend <70%) provide

buffer - Phase 2 eliminates this risk with native Bitcoin custody - Diversification: Multiple stablecoins reduces correlated risk

Residual Risk: Medium (accepted systemic risk)

Risk 4: Stacks Network Issues **Description:** Stacks blockchain experiences downtime, congestion, or technical problems.

Likelihood: Low (Stacks is mature)

Impact: Medium (transactions delayed, UX degraded)

Risk Score: LOW

Mitigation Strategies: - Multiple RPC endpoints with automatic failover - Frontend gracefully handles network errors - Transaction retry logic with exponential backoff - Clear status indicators for pending transactions - Monitor Stacks network health proactively

Residual Risk: Low

Risk 5: Oracle-Free Design Limitation **Description:** Without price oracles, we can't automatically liquidate undercollateralized loans.

Likelihood: Certain (design choice)

Impact: Low (acceptable for target users)

Risk Score: LOW

Mitigation Strategies: - This is intentional - oracle-free is a feature, not a bug - Conservative LTV requirements (recommend <70%) - Fixed-term loans with maturity dates (no indefinite loans) - Manual default handling after maturity - NFT positions allow risk transfer via secondary market - Future: Could add optional oracle-based liquidations without removing oracle-free option

Residual Risk: Acceptable (design tradeoff)

12.2 Business Risks

Risk 6: Insufficient Liquidity (Lender Side) **Description:** Not enough lenders provide stablecoin liquidity, auctions receive no bids.

Likelihood: Medium (market uncertainty)

Impact: High (product fails to launch successfully)

Risk Score: HIGH

Mitigation Strategies: - Pre-launch lender outreach (DeFi communities, Stacks ecosystem) - Attractive yields (4-8% APR competitive with DeFi) -

Clear risk/reward proposition in marketing - Partner with DeFi protocols for liquidity - Multiple stablecoins increases available liquidity pool - NFT positions allow exit liquidity via secondary market - Consider liquidity mining incentives if needed (Phase 1.5)

Contingency: If <50% auctions receive bids in Month 1, activate lender incentives

Residual Risk: Medium

Risk 7: Low Borrower Demand **Description:** Bitcoin holders don't see value in borrowing, low loan creation.

Likelihood: Low (validated demand from miners)

Impact: High (no product-market fit)

Risk Score: MEDIUM

Mitigation Strategies: - Target mining operations with clear need for liquidity - Conference attendance (Mining Disrupt, BTC Prague) - Direct outreach to 50+ mining operations - Educational content explaining benefits - Competitive rates vs traditional lenders - Multiple stablecoins accommodate different preferences - Permissionless access (no KYC friction)

Contingency: If <5 loans created in Month 1, pivot marketing or adjust terms

Residual Risk: Low (strong target user validation)

Risk 8: Stablecoin Preference Imbalance **Description:** All users prefer one stablecoin (e.g., only USDA), others unused.

Likelihood: Medium (user preferences unpredictable)

Impact: Low (not a failure, just underutilized feature)

Risk Score: LOW

Mitigation Strategies: - Launch with USDA as primary (highest liquidity) - Monitor stablecoin distribution in analytics - If one coin dominates >90%, consider simplifying to single stablecoin - Alternatively, incentivize usage of underutilized stablecoins - User education on benefits of each stablecoin option - Not a critical issue - having options doesn't hurt

Residual Risk: Low (acceptable outcome)

Risk 9: Competitive Pressure **Description:** Competitor launches similar oracle-free lending protocol.

Likelihood: Low (first-mover advantage)

Impact: Medium (market share dilution)

Risk Score: LOW

Mitigation Strategies: - First-mover advantage on Stacks - Open-source builds community and trust - Focus on Bitcoin miners (specific niche) - Multi-stablecoin feature differentiates - Strong community building (Discord, Twitter) - Path to Phase 2/3 creates moat (native Bitcoin, multi-chain) - Network effects: more users = better liquidity = more users

Residual Risk: Low

12.3 Regulatory & Legal Risks

Risk 10: Regulatory Uncertainty **Description:** Unclear regulatory status of DeFi lending, especially in certain jurisdictions.

Likelihood: Medium (DeFi regulation evolving)

Impact: High (could force shutdown or compliance)

Risk Score: MEDIUM

Mitigation Strategies: - Permissionless protocol (no central entity controls funds) - No KYC/AML in Phase 1 (purely decentralized) - Clear disclaimers and terms of service - Non-profit foundation structure (planned) - Legal consultation before launch - Monitor regulatory developments proactively - Geographic diversity (no single jurisdiction point of failure)

Contingency: Can comply with regulations in specific jurisdictions if needed

Residual Risk: Medium (accepted for decentralized protocols)

Risk 11: Stablecoin Regulatory Issues **Description:** Regulatory action against stablecoin issuers (USDC, others) could impact availability.

Likelihood: Low for USDC/USDA, Unknown for xUSD

Impact: Medium (loss of one stablecoin option)

Risk Score: LOW

Mitigation Strategies: - Multi-stablecoin strategy provides redundancy - If one stablecoin faces issues, others remain available - Can add/remove stablecoins from whitelist as needed - USDA is decentralized (like DAI), less regulatory risk - USDC is US-regulated, provides legitimacy - Diversification across stablecoin types (centralized vs decentralized)

Residual Risk: Low

12.4 Market Risks

Risk 12: Bitcoin Price Volatility **Description:** Rapid BTC price changes affect collateral value, could lead to defaults.

Likelihood: High (Bitcoin is volatile)

Impact: Medium (manageable with LTV buffers)

Risk Score: MEDIUM

Mitigation Strategies: - Conservative LTV recommendations (<70%) - Borrowers incentivized to maintain safe ratios - Short loan durations (30-90 days) limit exposure - Clear warnings about volatility risk - Borrowers can add collateral if needed (manual process) - No automatic liquidations (oracle-free design)

Residual Risk: Medium (accepted market risk)

Risk 13: Stablecoin Depeg Events **Description:** USDA, USDC, or xUSD loses its \$1 peg during active loans.

Likelihood: Low for USDC/USDA, Unknown for xUSD

Impact: High (value uncertainty, user losses)

Risk Score: MEDIUM

Mitigation Strategies: - Multi-stablecoin reduces correlated risk - USDA and USDC have different peg mechanisms (diversification) - Clear disclaimers about stablecoin risks - Monitor stablecoin health metrics - Can remove unstable stablecoin from whitelist - Users bear stablecoin risk (not protocol's fault)

Residual Risk: Medium (systemic DeFi risk)

12.5 Operational Risks

Risk 14: Team Capacity **Description:** Small team (2-3 core) may struggle with scope, delays possible.

Likelihood: Medium (ambitious roadmap)

Impact: Medium (launch delays, feature cuts)

Risk Score: MEDIUM

Mitigation Strategies: - Realistic 7-month timeline (not rushed) - Clear prioritization (Phase 1 scope well-defined) - Contractors/specialists for specific tasks (frontend, security) - Aggressive use of existing libraries (Stacks.js, React) - Out-of-scope list prevents feature creep - Buffer time built into schedule

Residual Risk: Medium

Risk 15: Dependency Risks Description: Critical dependencies (Stacks.js, wallet providers, sBTC) could have breaking changes.

Likelihood: Low (mature ecosystem)

Impact: Medium (temporary disruption)

Risk Score: LOW

Mitigation Strategies: - Pin dependency versions (no automatic updates) - Monitor ecosystem changes proactively - Multiple wallet integrations (not single point of failure) - Test thoroughly before dependency upgrades - Maintain good relationships with Stacks ecosystem teams

Residual Risk: Low

12.6 Risk Matrix Summary

Risk	Likelihood	Impact	Risk Score	Mitigation Quality
Smart Contract Bugs	Low	Critical	HIGH	Strong
Multi-Stablecoin Bugs	Medium	High	HIGH	Strong
sBTC Peg Failure	Low	High	MEDIUM	Accepted
Stacks Network Issues	Low	Medium	LOW	Strong
Oracle-Free Limitation	Certain	Low	LOW	By Design
Insufficient Liquidity	Medium	High	HIGH	Good
Low Borrower Demand	Low	High	MEDIUM	Good
Stablecoin Imbalance	Medium	Low	LOW	Good
Competitive Pressure	Low	Medium	LOW	Good
Regulatory Uncertainty	Medium	High	MEDIUM	Monitor
Stablecoin Regulation	Low	Medium	LOW	Good
BTC Price Volatility	High	Medium	MEDIUM	Accepted
Stablecoin Depeg	Low	High	MEDIUM	Systemic
Team Capacity	Medium	Medium	MEDIUM	Good
Dependency Risks	Low	Medium	LOW	Good

Overall Risk Assessment: MEDIUM

Risk Tolerance: Acceptable for Phase 1 MVP with strong mitigation strategies

13. Timeline and Budget

13.1 Revised Phase 1 Timeline (7 Months)

Original Plan: 6 months, \$254,000

Revised Plan: 7 months, \$308,000

Reason for Extension: Multi-stablecoin integration and enhanced testing require additional development time

Key Changes: - +1 month for multi-stablecoin development (D1.9) - +\$44K for multi-stablecoin integration - +\$10K for enhanced security audit scope - +\$8K for comprehensive stablecoin testing (D1.10)

13.2 Phase 1 Gantt Chart (7 Months)

MONTH 1: Foundation & Security

Week 1-3: D1.2 Mainnet Deploy
Week 2-3: D1.3 sBTC Collateral
Week 2-3: D1.4 Competitive Bidding
Week 2-3: D1.5 NFT Positions
Week 3-4: D1.1 Security Audit START

MONTH 2: Multi-Stablecoin Development

Week 1-4: D1.9 Multi-Stablecoin (NEW)
- Whitelist contract
- USDA integration
- USDC integration
- xUSD integration
Week 1-4: D1.1 Security Audit

MONTH 3: Enhanced Development & Audit

Week 1-2: D1.9 Multi-Stablecoin Complete
Week 1-4: D1.5a Lending/Borrowing UI
- Stablecoin selector UI
- Balance checks
- Filtering
Week 1-4: D1.5b NFT Marketplace UI
Week 1-2: D1.1 Security Audit Complete
Week 3-4: Address Audit Findings
Week 3-4: D1.6 Miner Outreach BEGIN

MONTH 4: Testing & Integration

Week 1-4: D1.5a UI Completion
Week 1-4: D1.5b Marketplace Completion
Week 1-4: D1.10 Stablecoin Testing (NEW)
- USDA test suite
- USDC test suite

- xUSD test suite
- Integration tests

Week 1-4: D1.6 Miner Outreach

MONTH 5: Launch Preparation

Week 1-2: D1.10 Testing Complete
 Week 1-2: Final QA & Bug Fixes
 Week 2-3: Testnet Deployment
 Week 3-4: Mainnet Deployment
 Week 3-4: Marketing Preparation
 Week 1-4: D1.6 Miner Outreach

MONTH 6: Launch & Early Adoption

Week 1: MAINNET LAUNCH
 Week 1-4: D1.6 First Loans (All Coins)
 Week 1-4: Monitor Stablecoin Adoption
 Week 1-4: Community Support
 Week 1-4: Marketing & PR

MONTH 7: Growth & Milestone Achievement

Week 1-4: D1.7 Volume Growth
 Week 1-4: D1.6 Miner Outreach
 Week 1-4: Stablecoin Analytics
 Week 1-4: Optimizations & Fixes
 Week 4: \$1M VOLUME TARGET
 Week 4: Phase 2 Planning

13.3 Detailed Budget Breakdown (\$308,000)

Category 1: Development (\$200,000 - 65%)

Item	Cost	Duration	Description
Lead Developer	\$84,000	7 months	Clarity smart contracts, architecture
Frontend Developer	\$56,000	4 months	React UI, stablecoin UX
Backend/DevOps	\$58,000	2 months	Infrastructure, deployment, monitoring
Multi-Stablecoin Dev	\$24,000	1.5 months	USDA/USDC/xUSD integration (NEW)

Item	Cost	Duration	Description
Testing & QA	\$8,000	1 month	Comprehensive testing (NEW)
SUBTOTAL	\$200,000		

Changes from Original: +\$44K for multi-stablecoin work and testing

Category 2: Security & Audit (\$88,000 - 29%)

Item	Cost	Duration	Description
Primary Security Audit	\$68,000	6 weeks	Professional audit firm (CoinFabrik, etc.)
Multi-Stablecoin Audit	\$10,000	1 week	Enhanced scope for stablecoin logic (NEW)
Follow-up Re-audit	\$10,000	1 week	Re-audit after fixes implemented
SUBTOTAL	\$88,000		

Changes from Original: +\$10K for multi-stablecoin audit scope

Category 3: Marketing & Business Development (\$20,000 - 6%)

Item	Cost	Duration	Description
Miner Outreach (D1.6)	\$12,000	5 months	Direct outreach, educational content
Conference Attendance	\$5,000	2 events	Mining Disrupt, BTC Prague, etc.
Marketing Materials	\$3,000	One-time	Website, docs, videos, graphics
SUBTOTAL	\$20,000		

Changes from Original: Slight adjustment for longer timeline

Total Phase 1 Budget: \$308,000

Category	Amount	% of Total	Change
Development	\$200,000	65%	+\$44K
Security & Audit	\$88,000	29%	+\$10K
Marketing & BD	\$20,000	6%	Adjusted
TOTAL	\$308,000	100%	+\$54K

13.4 Funding Strategy

Target Funding Sources Primary Target: \$308,000 for Phase 1

Funder	Target Ask	Likelihood	Timeline	Focus
Stacks Foundation	\$150,000	High (70%)	2-3 months	Stacks ecosystem growth
OpenSats	\$100,000	Medium (60%)	3-4 months	Open-source Bitcoin infrastructure
Spiral (Block)	\$50,000	Medium (50%)	3-4 months	Bitcoin utility and adoption
Other Sources	\$8,000	Low	Variable	Community grants, angels

Application Strategy: - **Month 0:** Submit Stacks Foundation application - **Month 1:** Submit OpenSats application
- **Month 1:** Submit Spiral application - **Month 2:** Follow up with all funders
- **Month 3:** Expect first funding decisions

Contingency if Funding Falls Short: - Can proceed with USDA-only (single stablecoin) for ~\$265K - Can extend timeline to reduce monthly burn - Can seek additional community funding or angel investment - Core innovation (competitive bidding) doesn't depend on multi-stablecoin

13.5 Milestone-Based Fund Release

Recommended Structure for Funders:

Tranche 1 (40% = \$123,200): Upon grant approval - Deliverables: D1.1 (Audit), D1.2-D1.5 (Core contracts) - Timeline: Months 1-2

Tranche 2 (40% = \$123,200): Mid-phase checkpoint - Deliverables: D1.9 (Multi-stablecoin), D1.10 (Testing), UI complete - Milestone: Security audit passed, testnet deployment successful - Timeline: Month 5

Tranche 3 (20% = \$61,600): Post-launch success - Deliverables: D1.7 (\$1M volume achieved) - Milestone: Mainnet launched, first 10 loans completed - Timeline: Month 7

Benefits: - De-risks funding for grant providers - Ensures accountability and progress - Aligns incentives (team funded as they deliver)

13.6 Phase 1 Success Criteria

Must-Have for Phase 1 Completion: - Security audit passed (zero critical findings) - Mainnet deployment successful - All 3 stablecoins (USDA, USDC, xUSD) functional - 10+ loans created and funded - 5+ loans successfully repaid - Zero critical bugs or fund losses - >95% test coverage achieved - \$1M+ cumulative loan volume

Nice-to-Have (Stretch Goals): - 20+ active borrowers - 50+ active lenders - Partnership with major mining operation - Featured on major DeFi/Bitcoin media - \$2M+ cumulative volume - All 3 stablecoins represent >10% usage each

13.7 Phase 1 → Phase 2 Transition

Timeline: Phase 2 begins Month 8 (immediately after Phase 1)

Prerequisites for Starting Phase 2: - Phase 1 fully operational (no critical issues) - Sufficient user traction (\$1M+ volume) - Funding secured for Phase 2 (\$463K) - Team ready to expand (recruit validator operators)

Phase 2 Budget: \$463,000 (separate application)

Phase 2 Duration: 9 months (Months 8-16)

Phase 2 Focus: Native Bitcoin custody with threshold signatures

Buffer Period: Months 17-18 (2 months)

Purpose: Stabilize Phase 2 before starting Phase 3

13.8 Cost Justification

Why \$308,000 vs Original \$254,000?

+\$54,000 increase justified by:

1. **Multi-Stablecoin Feature (+\$44,000):**
 - Competitive advantage (user choice, flexibility)
 - Reduces single point of failure risk
 - Increases addressable market
 - Provides valuable user preference data
 - Positions for institutional adoption (USDC)
2. **Enhanced Security Audit (+\$10,000):**
 - Multi-stablecoin complexity requires additional audit time
 - Dynamic contract calls need thorough review
 - Balance validation logic must be bulletproof
 - Risk of user fund loss makes this essential
 - \$10K is small price for security confidence
3. **Comprehensive Testing (+\$8,000 included in dev):**
 - 15+ stablecoin-specific test cases
 - Integration testing across all combinations
 - 95% coverage target
 - Prevents costly bugs post-launch
4. **Extended Timeline (+1 month):**
 - Realistic schedule reduces crunch and errors
 - Proper time for testing and QA
 - Better developer productivity
 - Higher quality final product

ROI on Additional Investment: - Multi-stablecoin could increase user base by 2-3x - Reduced risk = higher user confidence = more volume - Better product = stronger foundation for Phase 2/3 - \$54K investment could drive additional \$500K+ in volume

13.9 Budget Monitoring & Reporting

Monthly Reporting to Funders: - Budget burn rate vs plan - Deliverables completed - Milestones achieved - Risks and mitigation updates - Next month's plan

Key Metrics to Track: - Development velocity (story points per sprint) - Budget remaining vs timeline remaining - Feature completion percentage - Test coverage percentage - User acquisition (post-launch)

Contingency Plans: - 10% budget reserve for unexpected issues - Ability to reduce scope if funding delayed - Clear prioritization if budget cuts needed

Appendix A: Glossary

APR: Annual Percentage Rate - the yearly interest rate on a loan

Competitive Bidding Auction: An auction where lenders place bids on total repayment amounts, with the lowest bid winning

Implied APR: The annualized interest rate calculated from a bid amount, loan amount, and loan duration

DeFi: Decentralized Finance - financial applications built on blockchain without intermediaries

LTV (Loan-to-Value): Ratio of loan amount to collateral value, expressed as percentage

NFT: Non-Fungible Token - unique digital asset representing ownership

Oracle: External data feed providing off-chain information (e.g., prices) to smart contracts

Repayment Amount: Total amount (principal + interest) that borrower must pay to lender

sBTC: A 1:1 Bitcoin-backed asset on the Stacks blockchain

SIP-009: Stacks Improvement Proposal defining the NFT standard on Stacks

Stacks: A Bitcoin layer for smart contracts using Proof of Transfer consensus

USDT: Tether, a stablecoin pegged 1:1 to the US Dollar

Winning Bid: The lowest bid placed during an auction, which wins when the auction ends

Appendix B: References

Stacks Documentation: - <https://docs.stacks.co> - <https://book.clarity-lang.org>

sBTC Documentation: - <https://sbtc.tech> - <https://github.com/stacks-network/sbtc>

Competitive Analysis: - Aave: <https://aave.com> - Compound: <https://compound.finance> - MakerDAO: <https://makerdao.com>

Security Best Practices: - Trail of Bits: <https://github.com/crytic/building-secure-contracts> - Clarity Security Guide: <https://docs.stacks.co/clarity/security>

Appendix C: Contact & Feedback

Project Lead: Jamie

Organization: Bitcoin Lending Protocol Foundation (planned)

Website: (<https://bitcoin-lending-protocol-2egh.vercel.app/>)

GitHub: (<https://github.com/JamieFrame/Bitcoin-Lending-Protocol/tree/main/btc-lending-protocol>) **Discord:** [To be created]

Twitter: [To be launched]

Feedback: This PRD is a living document. Please provide feedback on: - Missing requirements - Unclear specifications - Unrealistic timelines - Budget concerns - Technical feasibility

Appendix D: Stablecoin Comparison

USDA (Arkadiko) - Primary

Type: Native Stacks stablecoin, STX-collateralized

Peg Mechanism: Over-collateralization (like MakerDAO's DAI)

Pros: - Highest liquidity on Stacks DEXes - Native to ecosystem (no bridging) - Decentralized (no custodian) - Battle-tested on Stacks - Best for DeFi-native users

Cons: - Collateralized by STX (not USD reserves) - Less familiar to traditional finance

Recommendation: Primary choice for most users

USDC (Bridged) - Secondary

Type: USD Coin bridged to Stacks

Peg Mechanism: 1:1 USD reserves held by Circle

Pros: - Institutional standard - Regulatory clarity - Familiar to TradFi - 1:1 USD backing - High trust factor

Cons: - Requires bridging (extra step) - Bridge trust assumptions - Lower liquidity on Stacks initially

Recommendation: Best for institutions and conservative investors

xUSD (Various) - Optional

Type: Alternative stablecoin options

Peg Mechanism: Varies by implementation

Pros: - Diversification - May offer unique features - Competition drives innovation

Cons: - Variable liquidity - Less established - Requires case-by-case evaluation

Recommendation: For users with existing xUSD holdings

End of Product Requirements Document - Phase 1

Document Version: 1.2 (Multi-Stablecoin Support)

Last Updated: January 12, 2026

This PRD defines Phase 1 with comprehensive multi-stablecoin support (USDA, USDC, xUSD), giving users flexibility while maintaining the oracle-free competitive bidding innovation.