Wrapped bunkercoin on smart chains

Phase 1

Introduction

This document describes the implementation and mechanisms of the wrapped bunkercoin token (wBKC), the smart contract, BKC vault and stakeholders.
The system has the role to allow users of bunkercoin to transfer their token to a smart chain while maintaining the trust of value over their assets. The bunkercoin(BKC) tokens are therefore wrapped into a ERC-20 token minted and burned on the smart chain.
Conceptually the keyholder of the smartcontract mints wBKC tokens in the name of the users locking BKC and releases BKC in the name of the users burning wBKC.

Roles and definitions

Follows the definitions, main roles and responsibilities in the system:

User - a person or entity interacting with the BKC chain (holding BKC tokens)
Keyholder - an entity holding the private keys to the smart contracts and BKC Vault
wBKC contract - the ERC-20 smart contract deployed on the smart chain
BKC Vault - a BKC chain address trusted to lock and release funds

The keyholder

The keyholder is an abstract entity composed of multiple trusted developers or established community members. The keyholder acts on the quorum of n out of m of it's members.
The members of the keyholder are expected to communicate and collaborate to maintain the functionality of the system. The keyholder should strive to gain the trust of the community through transparency and good communication.

In order to create the keyholder entity:

1. The core developers will publish a short list of names to be voted/agreed by the community
2. The names on the list(keyholders) will exchange and public their public keys(in both smart chains and BKC chain)
3. The keyholders will make public their public keys, and signed messages establishing their role
4. The keyholders will create a multisig wallet address and multisig contract (n out of m sigs) representing the keyholder entity.

The keyholder members are expected to act in good faith and maintain trust and the requirements of the system by communicating with the community and controlling the keyholder entity.

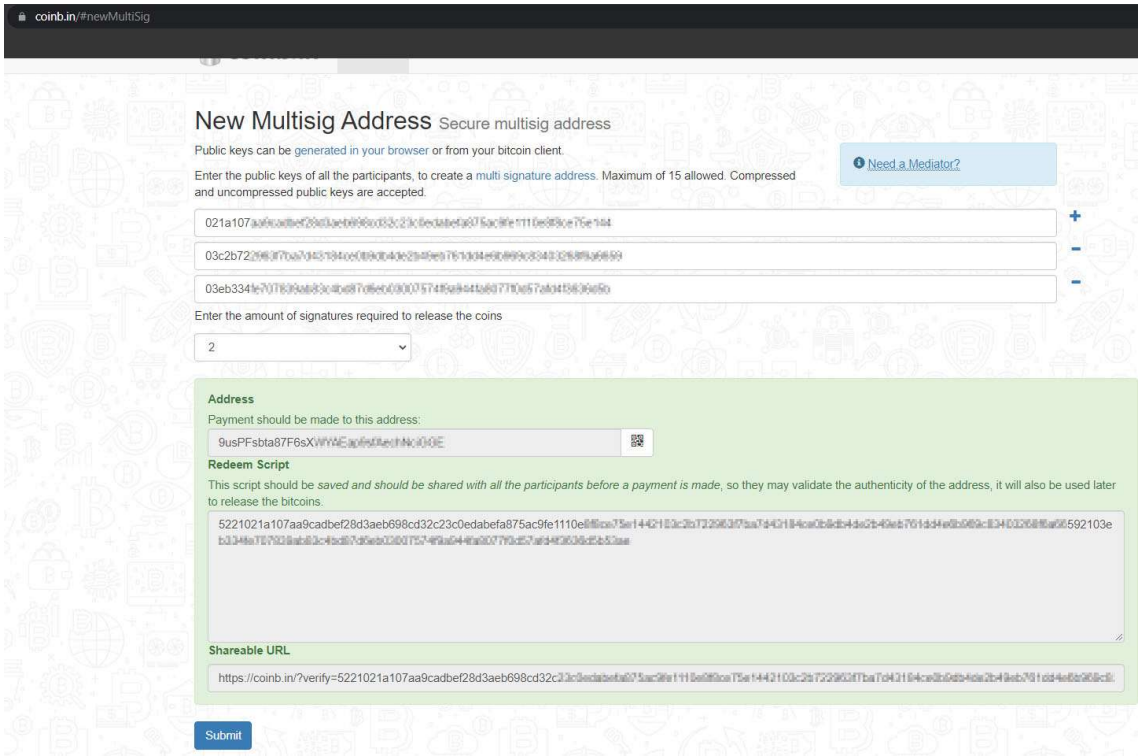
The BKC Vault

The BKC Vault is an abstract entity representing a multisignature address on the BKC chain.
The vault is created as a pay-to-script address requiring at least n out of m signatures of the keyholder members.

The balance of this address is considered to be proof of coverage for the minted wBKC tokens.

The BKC Vault should at all times have the same or more tokens that the existing wBKC tokens in circulation.

Example multisig 2/3 wallet



The wBKC contract

The wBKC contract is an ERC-20 smart contract deployed on a smart chain.
The address and code of the contract should be public and verifiable.

The contract will display an ERC-20 interface for interacting with the users.
The only keyholder can control the minting and burning of wBKC by calling the mint and burn methods of the smart contract.

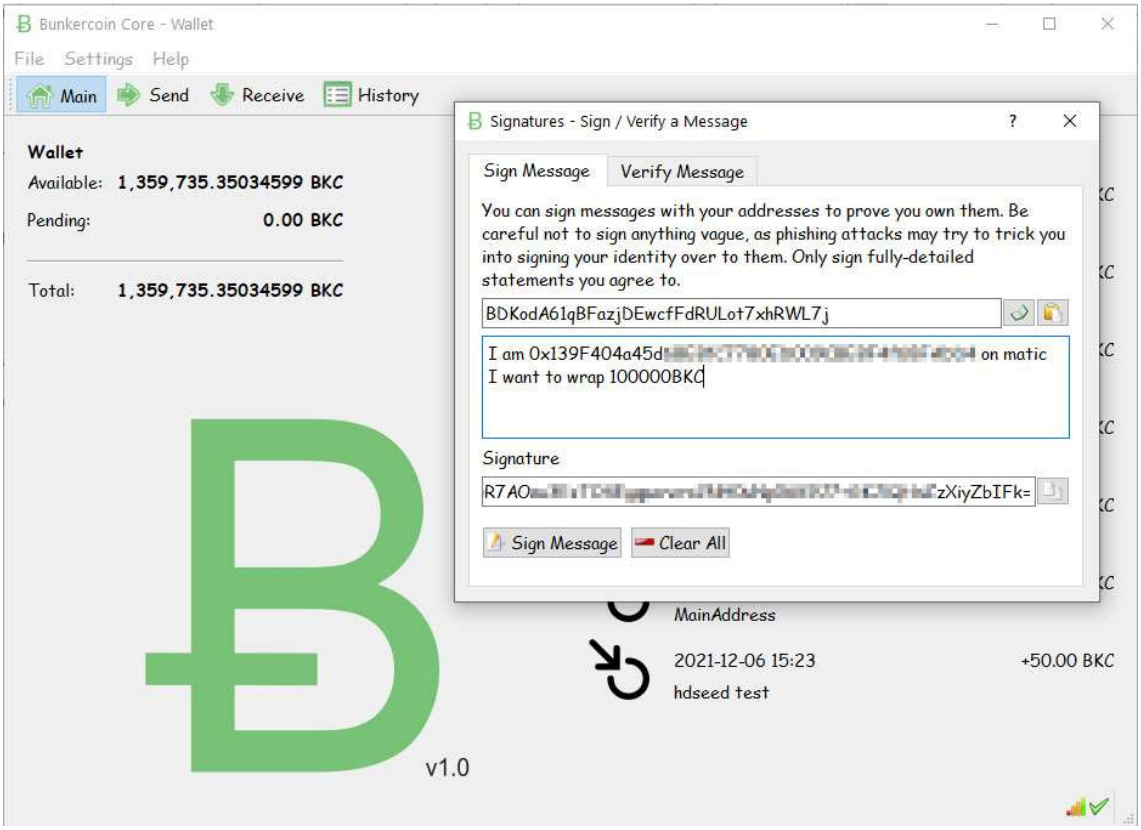
Deployment of phase 1

For the initial deployment the roles and contracts should be deployed and validated by the community before the beginning of the minting process.

Deposit period

Users wanting to wrap their BKC asset to wBKC will:

1. Create a signed message from their BKC wallet containing:
   Their smart chain address, the amount they want to wrap, a short message establishing their identity



2. Send a transaction from their wallet address to the BKC Vault address for the exact amount they want to wrap.
3. Submit the signed message and the txid to the keyholder members.

Keyholders must acknowledge the message, verify the signature of the message and verify the validity and confirmations of the tx.

At the end of the deposit period, the keyholders don't accept any more deposits.

Minting period

The keyholders will mint wBKC tokens in the exact amount deposited BKC in the BKC Vault. The wBKC tokens will be minted to the address of the users who locked BKC in the vault.

The integrity of the addresses that should be awarded wBKC can be verified by comparing the signed messages and the Transactions to the BKC vault.
At the end of the minting period keyholders will not mint any more coins.

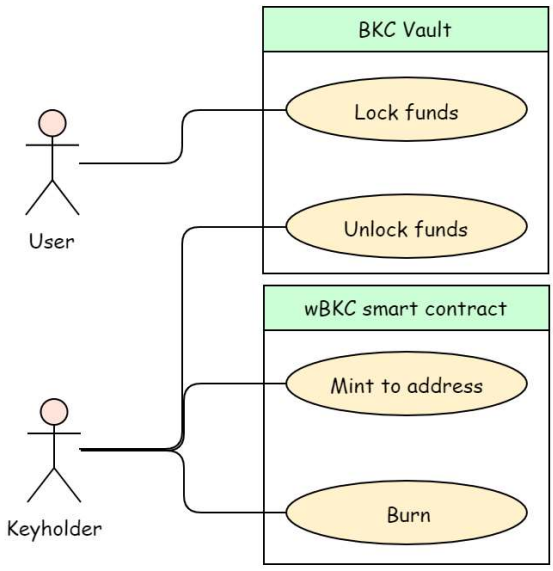
Trading period

The users holding wBKC can trade their tokens back to BKC by trading peer-2-peer with users willing to purchase wBKC.
wBKC can be traded as any ERC-20 token: on CEX or DEX.

We identify a particular class of users(merchants) that are facilitating the exchange of wBCK to BKC and vice versa. These users are important in the wrapping of tokens after minting is done.
We identify that the price of wBKC will be higher than BKC as wBKC is also containing the fees of transfer and minting.

System overview

Diagrams of users and interactions

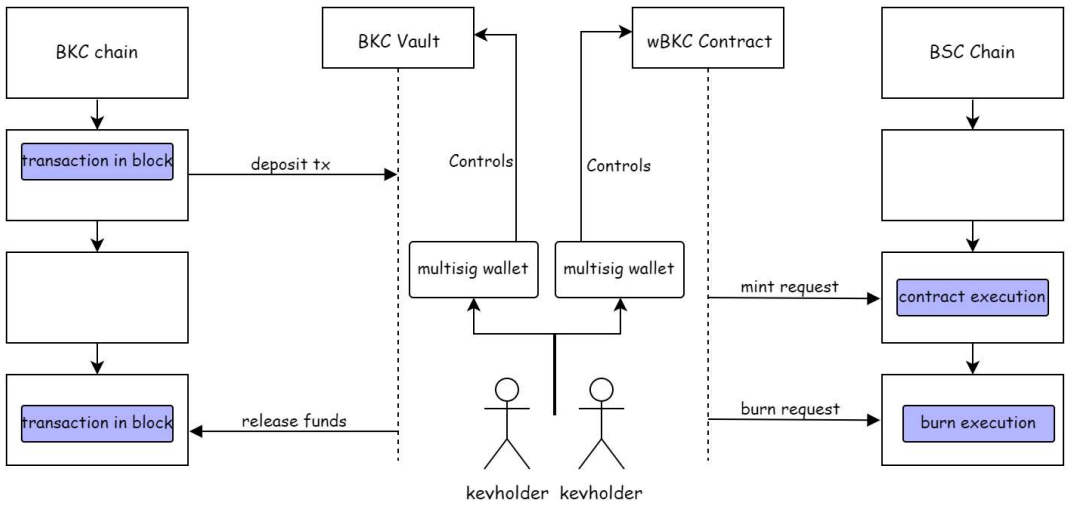


The user can lock funds for wrapping to wBKC

The Keyholder can mint funds to the user

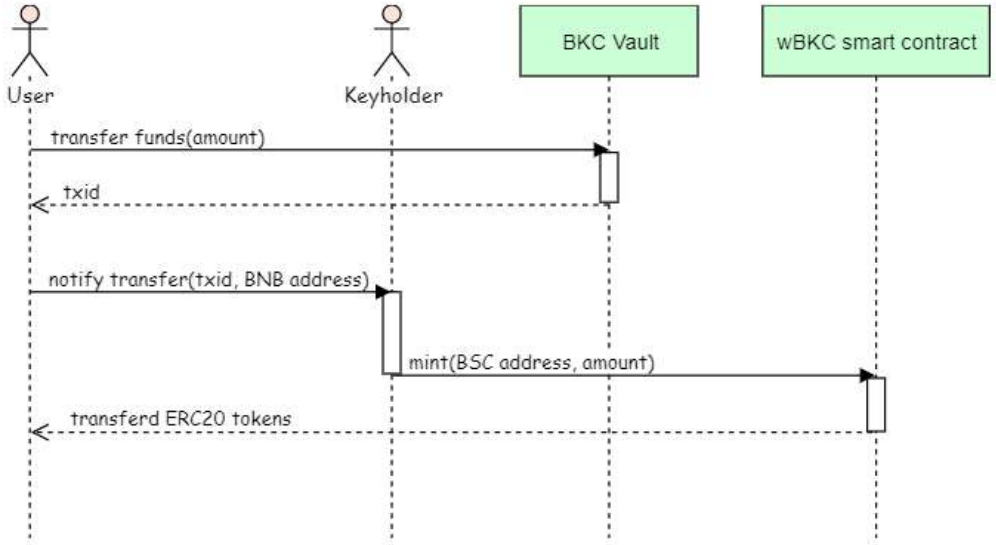
Can burn funds in its possession and

Can unlock funds to user



Interactions between chains

The keyholder has the responsibility to maintain the BKC Vault balance equal or higher than the wBKC amount in circulation by burning funds in its possession before a release.



Contract interactions sequence diagram