Trading Coins and Bilateral Settlement on Provenance Blockchain

Provenance Blockchain Foundation · Follow
Published in Provenance Blockchain · 5 min read · Apr 22, 2022

Blockchains are effectively designed to track the creation, transfer and ownership of digital currencies across accounts. By being a decentralized, distributed and immutable network of transactions, we are able to easily determine what accounts own what on a blockchain network.

A common transaction that blockchain technologies support is a transfer of a digital currency from a signing account to another receiving account. This type of transaction is unilateral: a one-way transfer, where the transferrer receives nothing in return from the recipient.

The Unilateral Problem

When a unilateral transfer occurs in exchange for money, goods or services, it is assumed a separate value exchange happens off-chain. If the transfer was in exchange for another digital currency, the sender is trusting that the recipient will also transfer a previously agreed upon asset and quantity back.

This raises a couple of obvious issues:

1. The recipient is not required to transfer another digital currency back and must act in good faith.
2. Parties who are exchanging value must already know of each other and have a means of communication.

Exchanges solve this problem by providing a user interface that allow buyers and sellers to participate in a marketplace and settle bilaterally with one another. Exchanges are commonly centralized, where buyers and sellers trust a middle man to handle the settlement of assets being bought and sold.

However, centralized exchanges still rely on trust in a third party. Decentralized exchanges that remove the middle man can be built directly on blockchain using smart contracts and open-source software.

Decentralized Solution

Provenance Blockchain makes it easy for a developer to build a decentralized exchange. We'll break down how to run a rudimentary exchange using the bilateral exchange smart contract to get you started.

Let's first define some terminology that you should be familiar with.

- Order book: A listing of buy and sell orders, including the identifying party, number of shares and price of order.

- Bid: An order to buy an asset on an order book in exchange for another asset
- Ask: An order to sell an asset on an order book in exchange for another asset.

By using Provenance Blockchain, the smart contract can act as the order book. The bilateral exchange smart contract allows accounts on the Provenance Blockchain to directly place bid and ask orders to it. The smart contract instance becomes the decentralized bilateral settlement engine, allowing for real-time settlement without counter-party risk.

Into the Details

Let’s break down the steps in plain english. You can interact with the Provenance Blockchain using the CLI or the gRPC endpoints. The following example assumes you have installed provenanced and are running a local node.

Create the Accounts

You will need a `buyer` and `seller` key pair that represent the respective parties transacting on the Provenance Blockchain.

Both accounts must receive `HASH` token in order to pay for the gas fees of placing bids and asks.

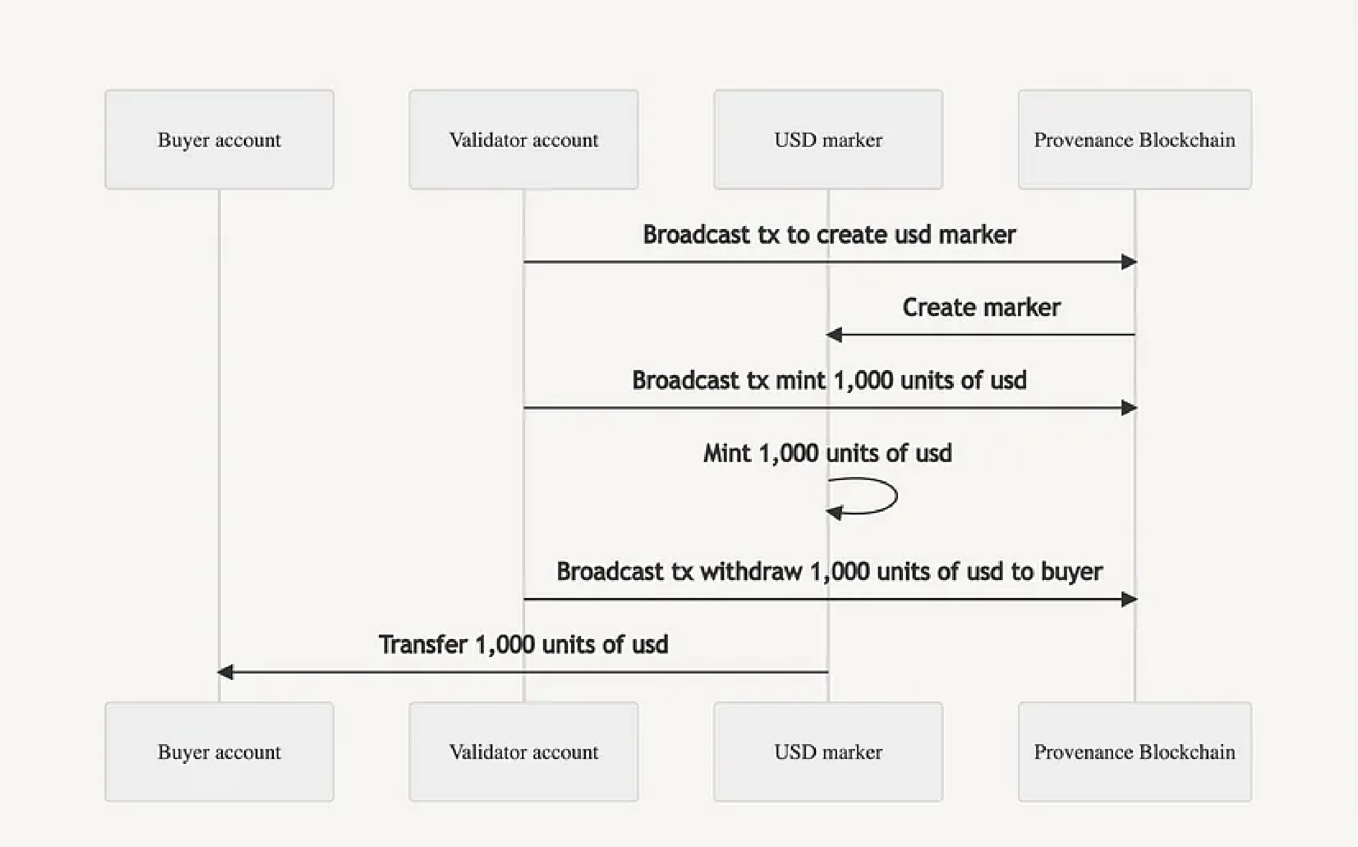
Create the Markers

To exchange two assets, you will need two different digital currencies. You will need a `validator` account that administrates these two new digital currencies. The validator account also must receive `HASH` token in order to pay for gas fees.

You can use the Marker Module to create a `gme` and `usd` denominated marker. For simplicity, let's mint 1,000 units of each coin.

Withdraw the `gme` coin minted from the marker to the `seller` address.

Withdraw the `usd` coin minted from the marker to the `buyer` address.

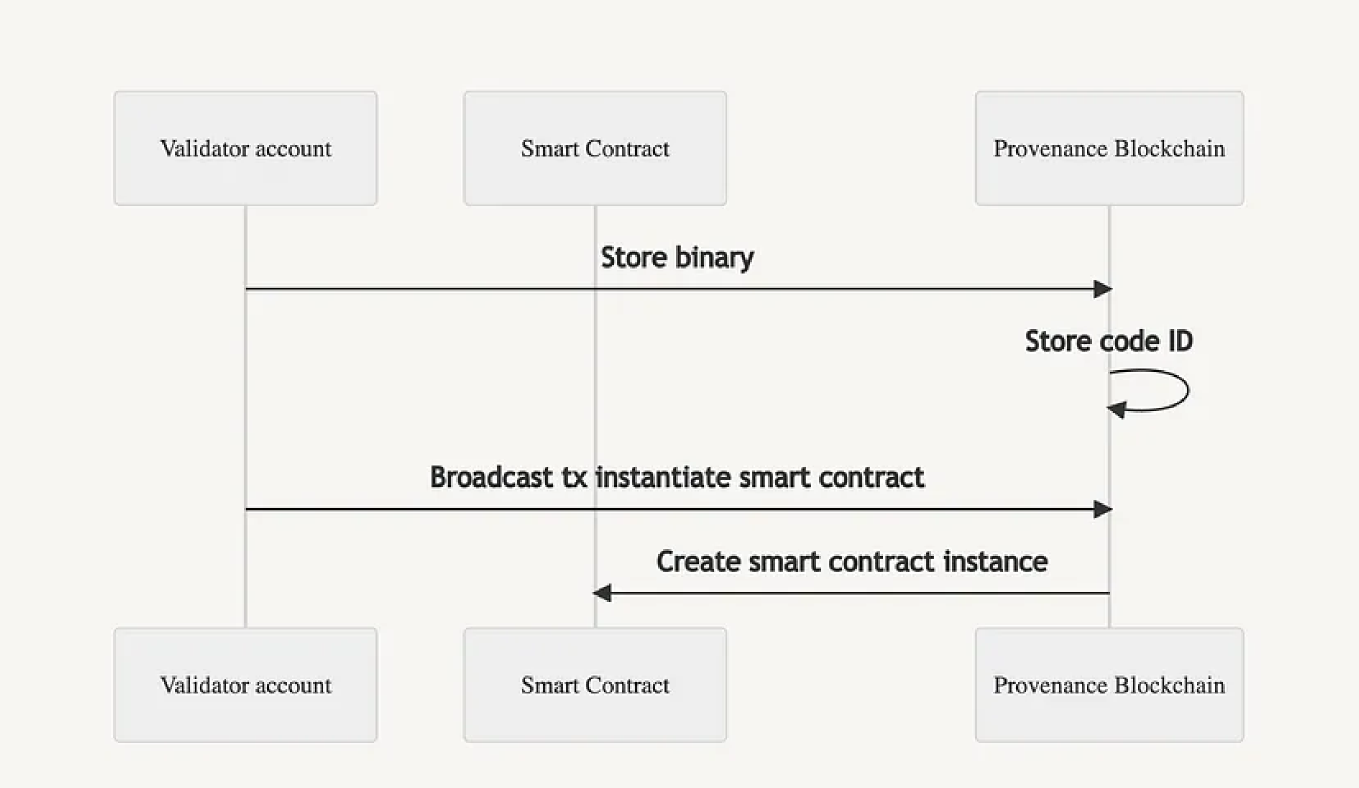


Note: This diagram shows the USD coin to buyer account flow. The GME coin to seller account would be equivalent.

Install the Smart Contract

You will need to store the bilateral settlement smart contract on your Provenance Blockchain node. Once the `wasm` binary is added, it should have a unique index identifier called the `Code ID`.

You will also use the `validator` account to administer the smart contract instance. You will use its key pair to instantiate this smart contract, which creates a special kind of account and corresponding address where the orders can be placed.



Place Orders

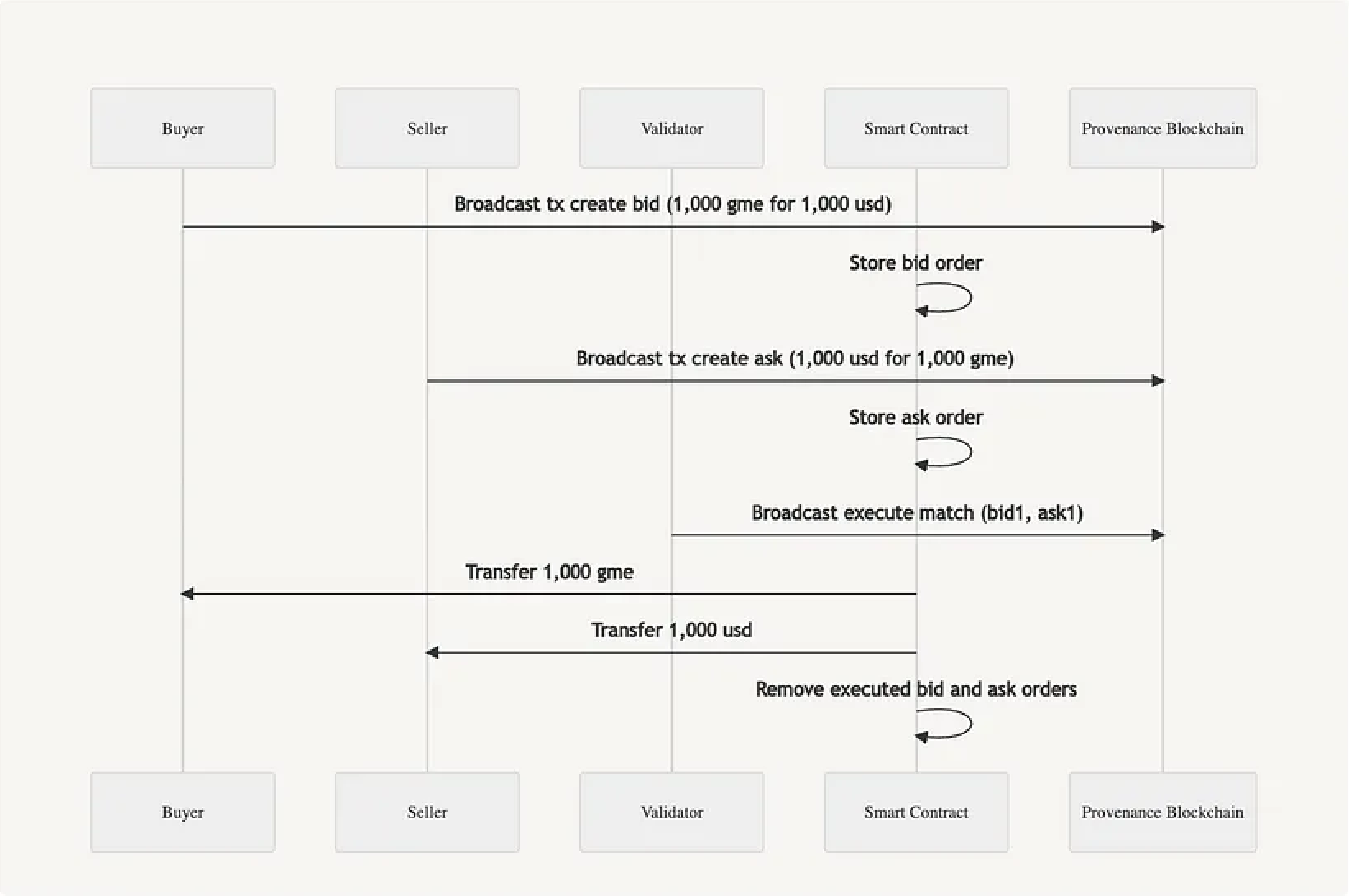
The `buyer` account can sign a `create_bid` transaction directly to the smart contract address. As part of the bid order, buyer will send 1,000 units of `usd` coin and specify that they want 1,000 units of `gme` coin in exchange. This is recorded in the smart contract state.

The `seller` can sign a `create_ask` transaction directly to the smart contract address. As part of the ask order, seller will send 1,000 units of `gme` coin and specify that they want 1,000 units of `usd` coin in exchange. This is also recorded in the smart contract state.

Execute Settlement

Since the above bid and ask orders align, a trade can be executed. The `validator` account would watch for potential matches and sign an `execute_match` transaction directly to the smart contract address when it sees an a trade that is executable.

Since the smart contract is already holding the 1,000 units of `gme` and `usd`, it can send the 1,000 units of `gme` to the `buyer` account and 1,000 units of `usd` to the `seller` account as part of a single transaction. The bid and ask orders are marked removed from the smart contract state and the order is considered complete.



Since the smart contract and validator trade monitoring and execution can be open source software utilizing Provenance Blockchain, trust is no longer assigned to a centralized authority. The source code can be independently audited and confirmed by any user of this exchange to behave accordingly.

Run the Example

Hopefully, this tutorial helped demystify bilateral settlement and how a simple decentralized exchange could be easily run on Provenance Blockchain.

Your Turn

For your next developer project, why not try building out your own decentralized exchange on Provenance Blockchain using this tutorial as a starting point?

This foundational knowledge can be used to create more complex settlement arrangements. Some potential examples:

- Auto-executing decentralized limit order book matching the highest bid price against lowest ask price when an order is placed.
- Trilateral settlement of cashless option exercises to common stock on trade execution.

This technology is live and tested. Figure Technologies is currently using the power of Provenance Blockchain to back its Alternative Trading System (ATS), creating a marketplace for trading private company securities. Provenance Blockchain reduces the cost of running secondary transactions by leveraging its native support for creating non-native digital assets and smart contract engine for bilateral settlement.

LEE DUAN

Lee is an engineer working at Figure Technologies, Inc. on Figure Pay, Figure Equity Solutions, Alternative Trading Systems and USDF.

Blockchain Trading Provenance Blockchain Defi

Written by Provenance Blockchain Foundation

Follow

252 Followers · Editor for Provenance Blockchain

The public open-source blockchain used by over 60 financial institutions. Billions of dollars of financial transactions have been executed on Provenance.

More from Provenance Blockchain Foundation and Provenance Blockchain

Provenance Blockchain F... in Interchain Ecosyst...

Real-World Financial Assets Find Provenance

Traditional Finance (TradFi) has entered the new era, already actively leveraging the...

4 min read · Sep 15, 2023

25

Provenance Blockchain Fou... in Provenance Bloc...

What is DART?

How Figure turned a mortgage into an NFT using Provenance Blockchain

3 min read · Apr 26, 2022

17

Provenance Blockchain Fou... in Provenance Bloc...

Hands-on Testnet: Accounts, Wallets, and Coin Transfer

Play with the Provenance Blockchain Testnet

9 min read · Apr 27, 2022

24

Provenance Blockchain F... in Interchain Ecosyst...

Modernizing Financial Services with Blockchain Technology

With over $8 billion in real-world financial assets currently locked on-chain, Provenanc...

4 min read · Sep 28, 2023

3

See all from Provenance Blockchain Foundation

See all from Provenance Blockchain

Recommended from Medium

Arthur Hayes

Points Guard

(Any views expressed in the below are the personal views of the author and should not…

13 min read · 3 days ago

466 6

Neutra Finance

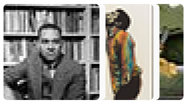
Uniswap V3 Delta Neutral Strategy—Part 2

Welcome back, Neutrons!

12 min read · Jan 17, 2024

67 1

Lists



My Kind Of Medium (All-Time Faves)

62 stories · 213 saves

Modern Marketing

61 stories · 420 saves

JUP	0.5607 $0.5607	-2.59%
ALT	0.31196 $0.31196	-5.31%
MANTA	2.74415 $2.74	-7.42%

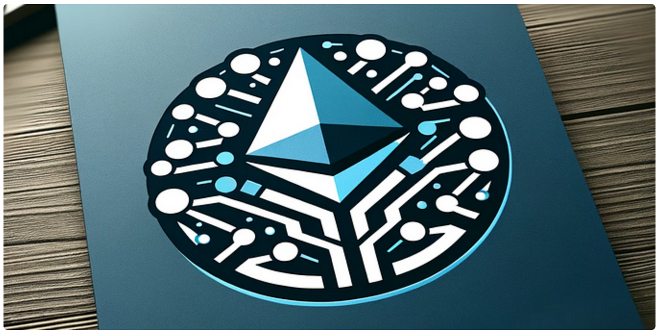
Crypto Big Stories in Coinmonks

This Trading Strategy Could Make You Rich: How to Make Money wit...

Every week, new tokens are listed on various crypto trading platforms, offering...

6 min read · Feb 5, 2024

553 7



Nikita Masych

Verkle Tries: Cryptography unleashed.

Ever wondered about internals of something powerful? Needless to say the subject of this...

6 min read · Jan 13, 2024

59

0xAnn in Crypto 24/7

Making Money Scalping Crypto

“Why do you work 9–5 when crypto trading is basically free money?”

✦ · 7 min read · Jan 9, 2024

729 17

CryptoWave0x

A Deep Dive into Monaco Protocol for Decentralized Peer-to-Peer...

Normally, the current online betting landscape, dominated by large corporations...

9 min read · Feb 1, 2024

9 1

See more recommendations