Scientific Research Publishing

Journal of Software Engineering and Applications, 2020, 13, 303-311
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

A Value Token Transfer Protocol (VTTP) for Decentralized Finance

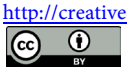
Arshdeep Bahga, Vijay K. Madisetti

Georgia Institute of Technology, Atlanta, GA, USA
Email: arshdeepbahga@gmail.com, vkm@gatech.edu

How to cite this paper: Bahga, A. and Madisetti, V.K. (2020) A Value Token Transfer Protocol (VTTP) for Decentralized Finance. *Journal of Software Engineering and Applications*, **13**, 303-311.
https://doi.org/10.4236/jsea.2020.1311020

Received: October 16, 2020
Accepted: November 23, 2020
Published: November 26, 2020

Copyright © 2020 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/



Open Access

Abstract

We present Value Token Transfer Protocol (VTTP), a decentralized finance protocol for exchange of value or tokens within and between participating blockchain networks, fiat bank accounts and fiat wallets. The protocol allows intra-chain or inter-chain transfers of cryptocurrencies or tokens. VTTP works in both client-server and peer-to-peer models. The protocol comprises receiving from a client a transfer request to transfer value in a form of a cryptocurrency or a token, determining if the transfer request is intra-chain or inter-chain, transmitting to the client a response to the transfer request, the response comprising a raw transaction, receiving from the client a response to the raw transaction wherein a private key of a user is used to sign the raw transaction, defining a signed transaction, verifying a signature of the signed transaction and broadcasting the signed transaction to the sending and receiving blockchain networks.

Keywords

Blockchain, Decentralized Finance, Open Finance

1. Introduction

Blockchain technology provides the ability to establish trust in a peer-to-peer network through a distributed consensus mechanism rather than relying on a powerful central authority [1]. Blockchain has brought about an economic paradigm shift by transforming financial products into trustless and transparent with the ability to run without intermediaries. This movement is often referred to as Decentralized finance (DeFi) or open finance. DeFi aims to create an alternate financial system by replacing centralized banks or trusted third-parties with smart contracts.

Existing Blockchain platforms lack interoperability and transfer of value be-

tween blockchains is often a challenging task for users. In this paper we present, Value Token Transfer Protocol (VTTP), a decentralized finance protocol for exchange of value or tokens within and between blockchain networks [2] [3]. VTTP allows intra and inter-chain transfers of cryptocurrencies and tokens. VTTP supports both client-server and a peer-to-peer communication architecture. In the client-server model, VTTP works as a request-response protocol based on a client-server architecture, where a VTTP Client sends requests to a VTTP Server, and the server responds to the requests. In the peer-to-peer model, VTTP works as a peer-to-peer protocol where VTTP Peers communicate directly with their peers and a VTTP Coordinator is used for coordinating the communication between peers.

VTTP is blockchain platform or network independent. VTTP can be used to send any type of tokens between different blockchain networks or within a blockchain network, as long as the VTTP client and server know how to interpret and transfer tokens. VTTP is stateless and each VTTP request contains all the information required to process a request. VTTP client and server do not maintain state between successive requests. Value Token Transfer Protocol (VTTP) provides the following features:

- Intra-chain value transfer of native cryptocurrency (e.g. ETH on Ethereum blockchain).
- Intra-chain value transfer of ERC20 tokens (e.g. sending OMG tokens and receiving SNT tokens).
- Inter-chain value transfer of cryptocurrencies (e.g. Send ETH from Ethereum blockchain and receive LTC on Litecoin blockchain).
- Intra and Inter-chain exchange of cryptocurrencies and ERC20 tokens (e.g. send BAT token from Ethereum blockchain and receive LTC on Litecoin blockchain).
- Exchange of fiat currency (in fiat bank accounts and fiat wallet apps) with tokens on blockchain networks.
- Fiat value transfer between fiat accounts or wallets of participating fiat banks or fiat wallets.
- Retrieve information on accounts, contracts, transactions for all participating blockchain networks, fiat bank accounts and fiat wallets.

2. Related Work

Decentralized finance (DeFi) is a new decentralized financial instrument system that is built on programmable blockchain networks such as Ethereum. New financial instruments and digital assets can be created through programmable smart contracts on public blockchain networks. A decentralized architecture for decentralizing finance using decentralized blockchain oracles is presented in [4]. Decentralized Oracles such as Band Protocol [5], Tellor [6] and Chainlink [7] act as intermediaries between blockchain-based smart contracts and traditional non-blockchain applications.

3. Proposed Approach

We propose Value Token Transfer Protocol (VTTP), a decentralized finance protocol for exchange of value or tokens within and between blockchain networks.

Figure 1 shows the components of VTTP. VTTP works as a request-response protocol based on a client-server architecture, where a VTTP client sends requests to a VTTP Server, and the server responds to the requests. The VTTP clients may be available for different platforms and devices such as a desktop client, a mobile client or an embedded client. Users send VTTP requests to the VTTP server using VTTP clients. VTTP requests contain VTTP commands which are processed by the VTTP server. A VTTP server may have one or more VTTP Workers to process VTTP requests and execute the VTTP commands sent by VTTP clients. VTTP server has blockchain clients for each of the participating blockchain networks, fiat banks, and fiat wallets. VTTP is an application layer protocol and works alongside Hypertext Transfer Protocol (HTTP) and on top of a transport layer executing Transmission Control Protocol (TCP) and an Internet layer executing Internet Protocol (IP).

VTTP can also work as a peer-to-peer protocol where VTTP peers communicate directly with their peers and a VTTP coordinator is used for coordinating the communication between peers. VTTP peers generate and send transactions to the participating blockchain networks, fiat banks, and fiat wallets, to execute a value transfer. A separate blockchain network may be used for user identity and access management. An identity verification and certification procedure is performed for securely linking blockchain accounts to real users. The identity (and associated blockchain accounts) of each user may be separately verified through

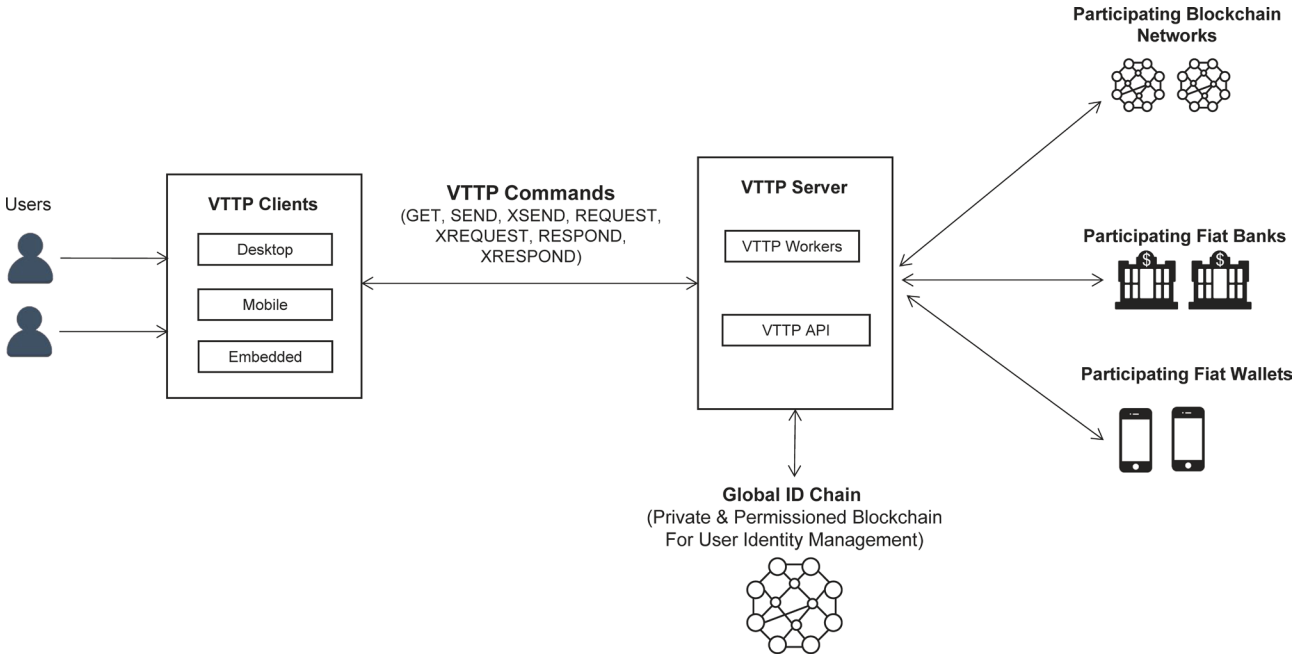


Figure 1. VTTP components.

an identity verification process [8].

3.1. VTTP Server Architecture

Figure 2 shows the VTTP server architecture. A VTTP server may have one or more VTTP Workers to process VTTP requests and execute the VTTP commands sent by VTTP clients. VTTP server has blockchain clients for each of the participating blockchain networks, fiat banks, and fiat wallets. A separate blockchain network may be used for user identity and access management. The VTTP server contains additional services, such as User Identity & Access Management Service, Authentication & Authorization Service, and Analytics & Reporting Service. The VTTP server contains inter- and intra-blockchain messaging services and connectors for databases, cloud services & blockchain networks. A transactions filter is used in the server to filter transactions. The server uses various Smart Contracts to bolster security. These smart contracts are executed for each VTTP request and perform additional verification (such as verifying sender and receiver's address). The smart contracts enforce checks such as time limits or quantity restrictions. Some smart contracts perform functions similar to virus filters, for filtering out suspicious transactions. New smart contracts can be distributed to VTTP servers in a manner similar to virus updates.

3.2. Intra-Chain Value Transfer

Figure 3 shows the VTTP intra-chain value transfer process. The VTTP intra-chain value transfer process enables transfer of cryptocurrency or tokens from one account to another account on the same blockchain network. For example, consider an intra-chain value transfer request where a User A wants to

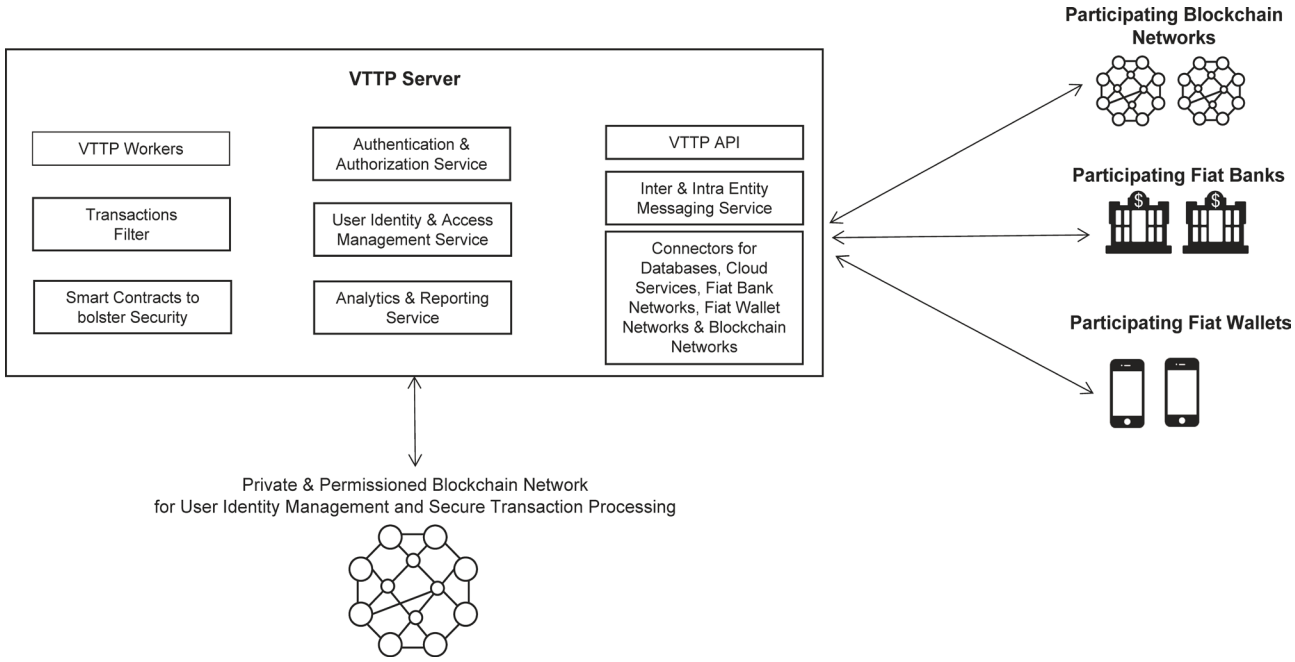


Figure 2. VTTP server architecture.

transfer certain units of a cryptocurrency or tokens from an account on a blockchain network to the account of another User B on the same blockchain network. At step 1, User A initiates value transfer request to send cryptocurrency or tokens to User B (e.g. to send 1 ETH from User A to User B). At step 2, the VTTP client sends a VTTP SEND request to the VTTP server. At step 3, the VTTP server generates a raw transaction and returns the same in SEND response. At step 4, User A signs the raw transaction with the private key and VTTP client sends the VTTP SIGN transaction. At step 5, VTTP server verifies the signature and broadcasts the transaction to the blockchain network. At step 6, User A receives a value transfer notification. At step 7, User B receives a value transfer notification via VTTP Client.

3.3. Inter-Chain Value Transfer

Figure 4 shows the VTTP inter-chain value transfer process. The VTTP inter-chain value transfer process enables transfer of cryptocurrency or tokens from an account on a blockchain network to another account on a different blockchain network.

At step 1, User A initiates a cross chain value transfer request to User B (e.g. to send 1 ETH from User A to User B who receives the value in equivalent number of LTC). At step 2, VTTP client sends a VTTP SEND request to the VTTP server. At step 3, VTTP server generates a raw transaction and returns the same in SEND response. In this raw transaction the "from" field is User A's account, and "to" field is a "Vault Account" on blockchain network-1. At step 4, User A signs the raw transaction with the private key and VTTP client sends the VTTP SIGN transaction. At step 5, VTTP server verifies the signature and

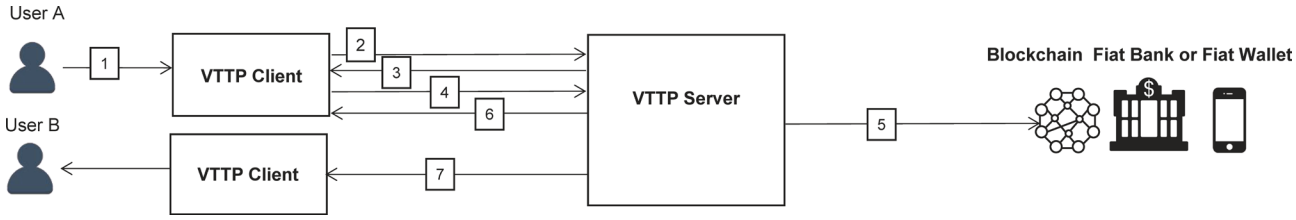


Figure 3. VTTP intra-chain value transfer process.

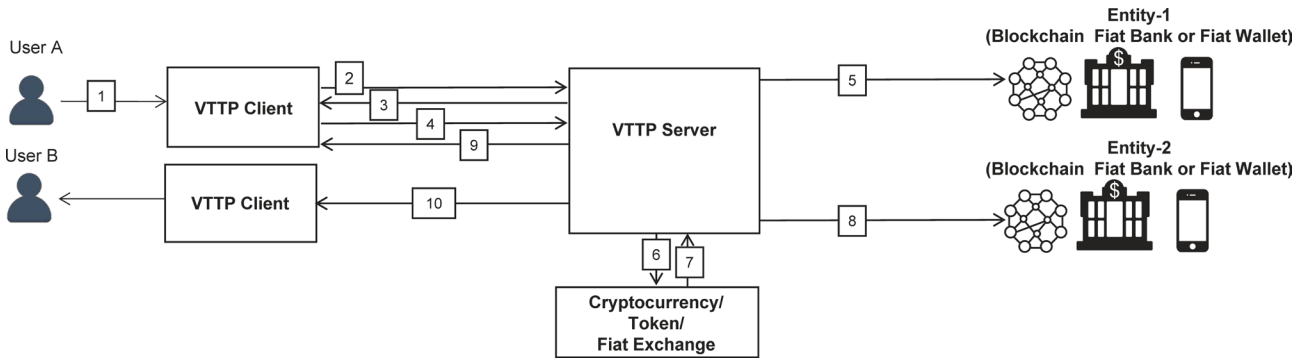


Figure 4. VTTP inter-chain value transfer process.

broadcasts the transaction to the blockchain network-1. At step 6, when the value transfer from User A account to Vault account on blockchain network-1 is confirmed, the cryptocurrency and tokens are sent to a Cryptocurrency/Token/Fiat Exchange account. At step 7, cyptocurrency or tokens are exchanged. At step 8, the exchanged cyptocurrency, tokens or fiat currency are sent to User B account on blockchain network-2. At step 9, User A receives a value transfer notification. At step 10, User B receives a value transfer notification via VTTP Client.

4. Implementation Case Study

In this section we describe some implementation details of VTTP such as commands, response code, transaction signing process, multisig transactions, token-based authentication and two-factor authentication.

4.1. VTTP Commands

VTTP supports the following commands:

- **GET**: Retrieve information about an account, contract, transaction, exchange rate for a token.
- **SEND**: Send value from one account to another account in same network.
- **XSEND**: Send value from one account to another account in another network.
- **REQUEST**: Request value from an account in the same network.
- **XREQUEST**: Request value from an account in another network.
- **RESPOND**: Accept or deny a request received from an account in the same network.
- **XRESPOND**: Accept or deny a request received from an account in the another network.
- **SIGN**: Sign and approve a transaction.

4.2. VTTP Response Codes

VTTP supports the following response codes:

- **1xx—Request Received:** For information purpose. E.g. A value transfer request is received and is being processed.
- **2xx—Request Completed:** The requested action has been successfully completed.
- **3xx—Request Pending:** The VTTP command has been accepted, but the requested action is being held in abeyance, pending receipt of further information.
- **4xx—Client Error:** The VTTP command was not accepted due to a client error and the requested action did not take place.
- **5xx—Server Error:** The VTTP command was not accepted due to a server error and the requested action did not take place.

4.3. VTTP Transaction Signing

Figure 5 shows the transaction signing process in VTTP. VTTP transactions

that transfer value are signed and approved by the user on the client side. For example, to send value from one account to another account within the same blockchain network, the VTTP client sends a VTTP SEND command. The VTTP server generates the blockchain network specific raw transaction and returns the raw transaction in the response. The user then signs the raw transaction with the private key and sends the signed transaction with the VTTP SIGN command. The VTTP server verifies the signature, broadcasts the signed transaction to the blockchain network, and sends a SIGN response. With this model of signing transactions on the client side, the user can retain the private keys on the user's local machine and need not share them with the VTTP server.

4.4. VTTP Multisig Transactions

Figure 6 shows the multi-signature ("multisig") transaction signing process in

Figure 5. Illustration the transaction signing process in VTTP.

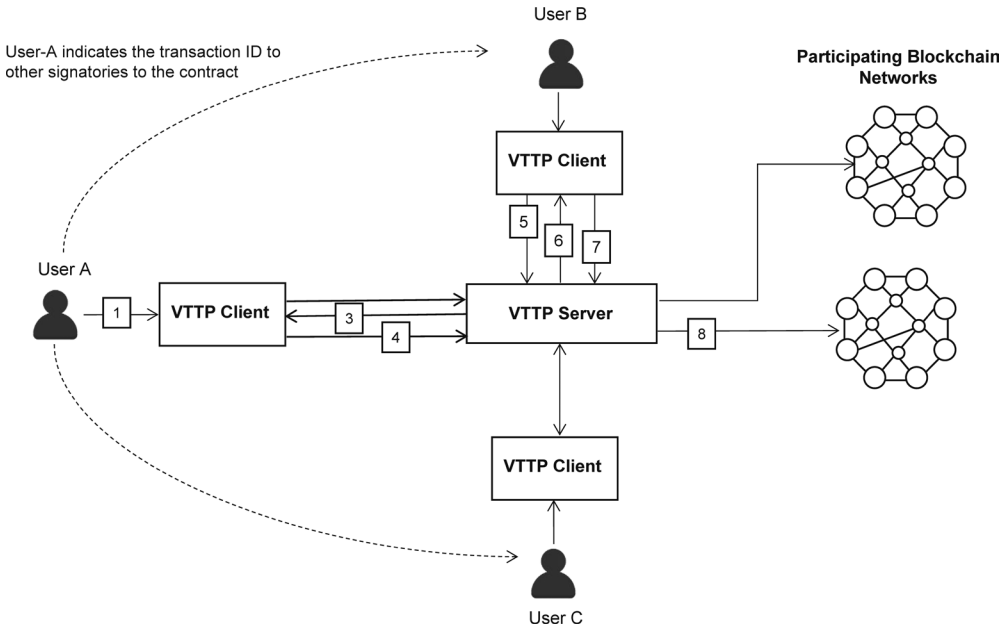


Figure 6. Illustration the multi-signature transaction signing process in VTTP.

VTTP. An example of using VTTP for a multisig contract that requires 2 out of 3 signatures to process a transaction is described. At step 1, User A initiates value transfer request to send cryptocurrency or tokens. At step 2, VTTP client sends a VTTP SEND request to the VTTP server. At step 3, VTTP server generates a raw transaction and returns the same in SEND response. At step 4, User A signs the raw transaction with the private key and VTTP client sends the VTTP SIGN transaction. User A may indicate the transaction ID to other signatories to the contract or other signatories may get a notification from the VTTP server. At step 5, User-B retrieves the transaction using the transaction ID. At step 6, VTTP server returns the raw transaction to be signed by User B. At step 7, User B signs the raw transaction with the private key and VTTP client sends the VTTP SIGN transaction. At step 8, VTTP server verifies the signatures of User A and User B and broadcasts the transaction to a blockchain network.

4.5. Token-Based Authentication

Figure 7 shows the token-based authentication process in VTTP. A VTTP client can authenticate with a VTTP server using an authentication token which is generated by the client and verified by the VTTP server. VTTP may use existing authentication token standards such as JSON Web Token (JWT) [9] for securely transmitting information between a client and server as a JSON object. At the client side, the username and password fields are combined and encrypted to generate an encrypted authentication string. The VTTP client sends a VTTP AUTH request to the VTTP server containing the encrypted authentication string. The VTTP server decrypts the encrypted authentication string and verifies the user's credentials, and then generates a JSON Web token. A JSON Web Token contains header, payload and signature fields. The VTTP server returns a VTTP AUTH response containing the JSON Web Token. The VTTP client uses this token for all subsequent VTTP requests.

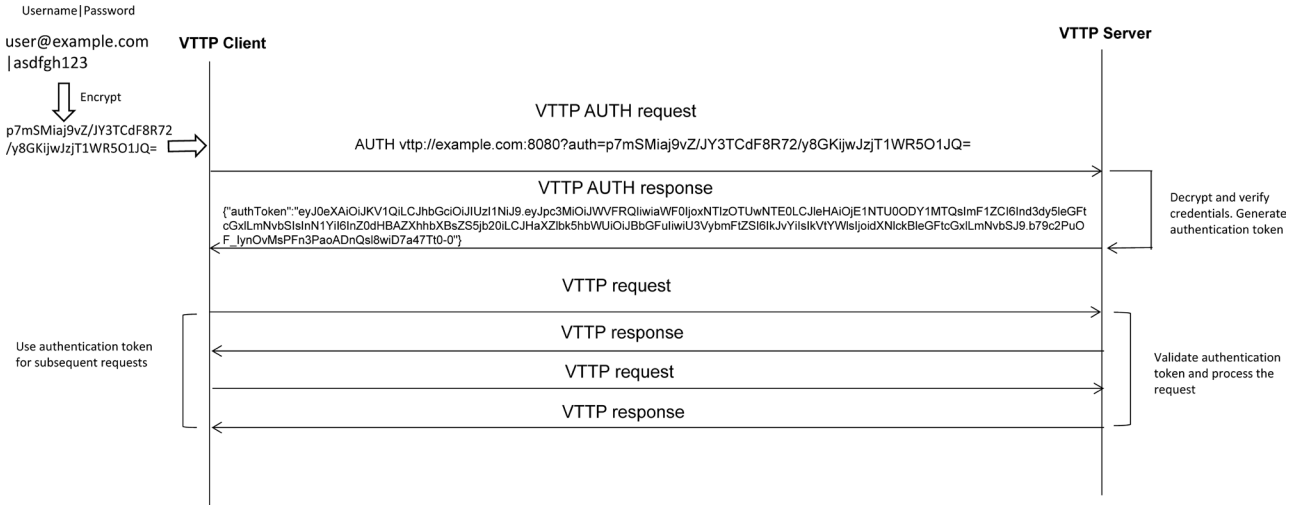


Figure 7. VTTP Token-based Authentication.

4.6. Two-Factor Authentication

VTTP supports two-factor authentication. To authenticate a VTTP client with a VTTP server when two-factor authentication is enabled for a user's account, the client first sends a VTTP AUTH request containing an encrypted authentication string. The VTTP server decrypts the authentication string and verifies the user's credentials. If two-factor is enabled for user's account, the VTTP server returns a field "is2FAEnabled" as "True" in the response. The VTTP client then sends another AUTH request, containing the encrypted authentication string and a two-factor authentication token. The VTTP server decrypts and verifies user's credentials and two-factor authentication token and generates JSON Web Token which is used as an authentication token for all subsequent requests sent by the VTTP client. The VTTP server returns a VTTP AUTH response containing the JSON Web Token. The VTTP client uses this token for all subsequent VTTP requests.

5. Conclusion and Future Work

We presented a decentralized protocol for exchange of value or tokens within and between blockchain networks that supports both client-server and a peer-to-peer communication architecture. The architecture of a VTTP server and the implementation details of the protocol were presented. Future work will focus on benchmarking the performance of VTTP server for intra- and inter-blockchain value transfers and implementing VTTP on Internet of Things (IoT) devices.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Bahga, A. and Madisetti, V. (2017) Blockchain Applications: A Hands-On Approach.

[2] Madisetti, V. and Bahga, A. (2020) Method and System for Exchange of Value or Tokens between Blockchain Networks. *WIPO PCT No. WO* 2020/190720.

[3] Madisetti, V. and Bahga, A. (2019) Use Case Extension to the Value Token Transfer Protocol. *US Provisional Patent Application No.* 62818798.

[4] Kumar, M. and Nikhil, R.S. (2020) Decentralising Finance Using Decentralised Blockchain Oracles. *International Conference for Emerging Technology* (*INCET*), Belgaum, 5-7 June 2020. https://doi.org/10.1109/INCET49848.2020.9154123

[5] Band Protocol—Secure, Scalable Blockchain—Agnostic Decentralized Oracle. https://bandprotocol.com/

[6] Tellor—The Decentralized Oracle for DeFi. https://tellor.io/

[7] Chainlink. https://chain.link/

[8] Madisetti, V. and Bahga, A. (2018) Method and System for Blockchain-Based Combined Identity, Ownership, Integrity and Custody Management. *US Patent No.* 10102526.

[9] (2015) Internet Engineering Task Force (IETF), JSON Web Token (JWT), RFC 7519.