Velos: High-speed Trustless Transactions

By Stephen Andrews

Abstract. Blockchain technology rivals traditional financial institutions with a cryptographically secured peer-to-peer network. This creates a decentralized environment where transactions can take place without a “trusted” middleman in between. These trustless transactions occur between two parties; transactions are signed and recorded on-chain, and the receiving party can only completely trust the transaction once it has been included in a block, and that block has received multiple confirmations. However, decentralization comes at a cost - slow transaction speeds and long confirmation times. This paper describes a method to operate a trustless, smart contract based solution utilizing techniques similar to atomic swaps and multi-sig contracts. This method would allow for high-speed transactions with instant confirmation times.

Introduction

Tezos is a smart contract blockchain protocol built with functional programming in mind; because of this, Tezos smart contracts can be formally verified to prove mathematical correctness. Tezos implements a delegated proof of stake consensus mechanism, allowing the stakeholders to validate new blocks. The Tezos platform is also governed on-chain, further empowering stakeholders to decide on how the platform will evolve and grow. These features make Tezos a very robust, future-proof and secure blockchain protocol.

Tezos has a stated theoretical throughput of approximately 30 transactions per second (TPS), with a confirmation time of a few minutes; these numbers are far below traditional payment processors, making Tezos a poor replacement candidate in its current state.

Instead of altering the Tezos protocol to solve this issue, this paper proposes an alternate solution - Velos. Velos allows for a similar trustless exchange to occur off-chain. This works by creating an on-chain contract between a source of funds (the sender) and a guarantor of funds (the gateway). Once this contract has been established, the sender may distribute their stored balance to a destination (receiver) in the form of a transaction promise, which can occur off-chain and be confirmed and trusted instantly.

Transactions

A sender will generate a signed transaction to distribute tez (the native Tezos token), which is then validated and co-signed by the gateway and verified by the receiver. Once verified, the receiver can trust the transaction even when it hasn’t occurred on-chain – this process is instant, allowing for high transaction speed and low confirmation times. The receiver will claim the value of the transaction in the future once the transaction has been settled on-chain.

Velos works because of the inclusion of the gateway; the gateway is responsible for maintaining the balance of a sender off-chain using a centralized side-chain (referred to as the transaction-chain, or txchain). Additionally, the gateway holds a balance of tokens within the contract, which is referred to as the gateway’s reserves. When the gateway signs a transaction, they are providing a “guarantee”

to distribute the transaction amount from the gateway's reserves irrespective of if the sender's balance is sufficient or not.

Transaction-chain

The transaction-chain (or txchain) is a centralized side-chain run by the gateway; it reflects all transactions that the gateway has signed. All transactions are "chained" together in a similar way to blocks in a blockchain. The gateway will use this txchain to maintain an accurate balance for a given sender, as some unsettled transactions may exist (i.e. transactions that haven't occurred on-chain).

When a gateway settles transactions to the smart contract, they must be done in order; this is to ensure the sequence of transactions are maintained. Although the txchain is centralized and not distributed, the Velos smart contract enforces strict penalties for bad behaviour, and rewards honest behaviour.

The benefit of utilizing this centralized txchain is transaction speed– the theoretical TPS of Velos is in the thousands, and can be developed to rival that of traditional payment processors.

Gateway

Gateways can be any third party willing to operate a Velos smart contract and txchain instance. As the gateway controls a major centralized network, Velos deploys a number of counter-measures to reduce the financial viability of bad behaviour. The gateway has a major disincentive of signing invalid transactions – i.e. signing a transaction for a sender who doesn't have the balance available. If the gateway co-signs an invalid transaction, the difference will be deducted from the gateway's reserves. This difference is referred to as "gateway loss".

The smart contract is also designed to "burn" an amount of tez equal to the gateway loss. This is also deducted from the the reserves whenever an invalid transaction is signed. Here's an example of a valid and invalid transaction, both being signed by the gateway, which illustrates the financial costs involved when a gateway signs an invalid transaction.

Valid transaction		**Invalid transaction**	
Transaction amount	50ꜩ	Transaction amount	50ꜩ
Sender's available balance	50ꜩ	Sender's available balance	20ꜩ
Gateway loss	*0ꜩ*	*Gateway loss*	*30ꜩ*
Gateway fine	*0ꜩ*	*Gateway fine*	*30ꜩ*
Receiver output	**50ꜩ**	**Receiver output**	**50ꜩ**
Gateway net-loss	**0ꜩ**	**Gateway net-loss**	**60ꜩ**

The gateway must also maintain a minimum reserve-to-balance ratio (RBR), which is enforced by the smart contract. This is the ratio of the reserve balance to the total balance held by all senders. When this RBR is not met, reserve withdrawals and sender deposits will fail. This places further restrictions on how a gateway can operate, and helps to ensure that a gateway contract retains enough tez in reserves.

To provide an incentive for gateways to act honestly, a fee can be captured from the transaction and made available to the gateway. Furthermore, the balance of the smart contract can be delegated and used to validate blocks on the Tezos platform, earning additional tez in the form of validation rewards.

Transaction lifecycle

Before the transaction (on-chain)

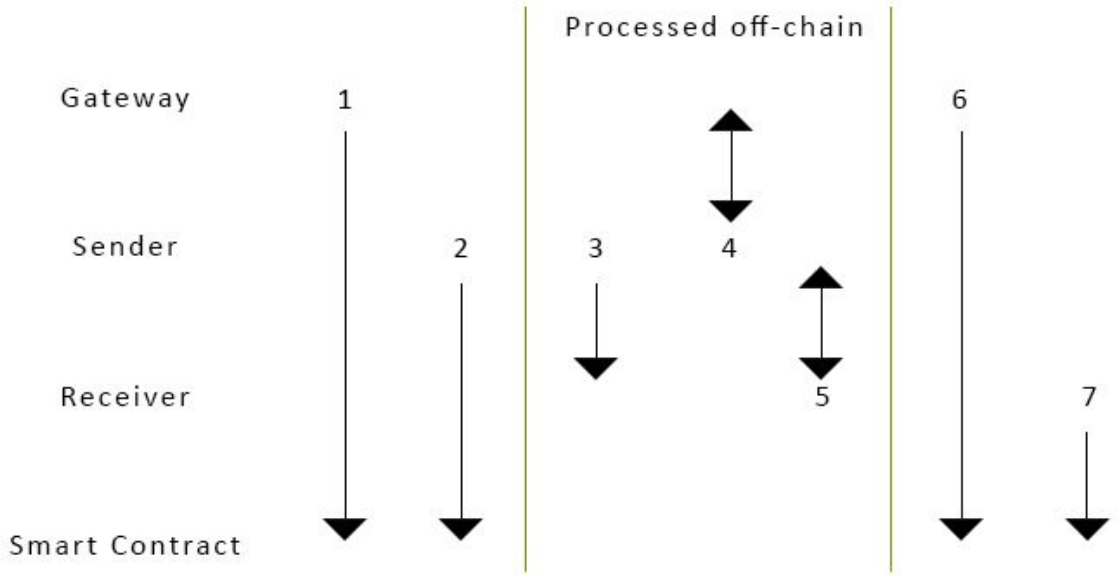
1) The gateway **initiates** the contract, and stores tez in the form of reserves
2) The sender **funds** their balance within the smart contract by sending tez

During the transaction (off-chain)

3) The sender **constructs** a signed request in collaboration with the receiver, and submits it to the gateway
4) The gateway **validates** the request, and returns a signed receipt. The receipt is combined with a secret key to form the promise, which is forwarded to the receiver
5) The receiver **verifies** the promise – the receiver can now accept the transaction. At this stage, the transaction is considered "unsettled"

After the transaction (on-chain)

6) The gateway **settles** the transaction, updating the balance of the sender on-chain
7) The receiver **claims** the value of the promise, receiving the transaction balance in tez



Transaction anatomy

A transaction is constructed and signed, imbedded with a secret known initially only to the sender – we call this the txRequest:

```
txRequest = senderAddress + receiverAddress + amount + fee + timestamp + hash(secret) +
                                        senderSignature
```

The txRequest is sent to the gateway to validate and co-sign. If the gateway deems the transaction as valid, a signed response is sent to back to the sender – we call this the txReceipt. The txReceipt is therefore signed by both the sender and the gateway:

```
txReceipt = txRequest + lastTxHash + gatewaySignature
```

The sender can now present the txReceipt and the secret to the receiver – this combination is the txPromise:

```
txPromise = txReceipt + secret
```

The receiver can verify the txPromise by checking the transaction data, verifying the signatures and ensuring the secret and hash match. This can occur off-chain, with the total process being instant. At this stage, the receiver can trust the transaction immediately. The receiver will then claim the balance of the transaction on-chain – this is performed by revealing the secret.

Smart contract

Smart contracts enforce immutable rules that must be adhered to; Velos utilises a uniquely constructed smart contract which works in tandem with the gateway and txchain. The smart contract balances the use of a centralized txchain by enforcing expensive penalties for bad behaviour, and rewarding good behaviour. Furthermore, the smart contract removes centralized control of the funds stored, ensuring that no single entity can negatively impact another party.

The Velos smart contract will be responsible for the following:

1) Maintaining sender balances;

   The smart-contract will keep a balance of all senders and their available balances. As transactions are settled, these balances will change. Senders will be able to deposit funds into the smart contract, increasing their available balance.

   A special process has also been identified for sender withdrawals, allowing a withdrawal to succeed after a predefined window has passed (to allow for the settlement of unsettled transactions).

2) Accepting transactions to be settled by the gateway;

   The gateway will periodically settle transactions to the smart-contact; this will correctly update the balances of the senders and allow the transactions to be claimed (or refunded). A receiver can reveal the secret linked to a transaction to the gateway, allowing the gateway to simultaneously settle and complete transactions. The gateway can settle multiple transactions at once, cutting down on gas costs.

3) Accepting transactions to be claimed by receivers;

   Receivers can choose to manually claim a transaction by sending it to the smart contract (as opposed to revealing the secret and waiting for the gateway to settle the transaction).

4) Accepting transactions to be refunded by senders;

   To protect senders from potential attacks, the contract will allow a sender to request a refund on an unclaimed transaction once a predefined time period has passed.

5) Maintaining gateway reserves;

   The gateway's reserves are also stored and managed via the smart contract. The gateway may withdraw against the reserves, but must satisfy the RBR. The gateway can also make deposits into the smart contract. The gateway can not accept sender deposits or gateway withdrawals if the RBR falls below a predefined value (e.g. 20%).

Conclusion

Velos illustrates a method which allows the operation of a centralized side-chain to work in tandem with an on-chain smart contract. The result is a high-speed trustless transaction system where funds are sent between two parties via a third-party guarantor. The guarantors are held accountable by high penalty costs to disincentivize bad behaviour, and rewarded to incentivize good behaviour.

Velos can be developed to rival traditional payment processors like Visa, taking advantage of on-chain smart contracts to foster decentralization, and off-chain transaction chains for speed and instant confirmation times.