BITSHARES TESTNET STRESS-TEST

Fabian Schuh BitShares Europe, bitshares.eu*
Erlangen (Bavaria), Germany
`fabian@bitshares.eu`

Abstract—**BitShares 2.0 is an industrial-grade decentralized platform built for high-performance financial smart contracts. In order to show its capabilities in the field, we have conducted a stress test on the public testnet. The testnet has been deployed with the identical code base that is used for the BitShares network and has nodes around the globe. A multi-phase stress-test has been proposed and accepted that modifies the maximum transaction size, maximum block size and block confirmation times in the live network during the stress test. Validators have been kept up to date by means of stake-weighted voting [1].**

1   Introduction

The Graphene Platform has been developed by Cryptonomex specifically for BitShares, went through many changes and has done its best to stay on top of blockchain technology. One of it's public forks, BitShares, is publicly traded for over 2 years and has yet to show it's full potential. For this reasons, we have deployed a testnet using the very same technology that BitShares is built on, specifically for testing algorithms, implementations and also scalability.

Here, the term *scalability* refers to the amount of transactions that can be applied to the blockchain at scale. Several factors need to be taken into account to correctly interpret any results obtained through testing. Among these are the specification of the deployed servers (CPU/RAM) that produce the blocks (validators), the interconnectivity of the nodes in the Peer-2-Peer network, the round-trip times and latency between nodes, as well as the geographical distance between nodes.

Obviously, a globally distributed network represents the worst case scenario when it comes to latency between nodes limited mostly by the speed of light and the size of the planet. A network that is hosted locally can result in better overall performance but doesn't offer the same robustness and redundancy as a global network.

The number of validators, furthermore, does not affect the throughput as long as all active validators can keep up with the requirements of the network. All active validators are treated equally and are given a slot to produce their blocks in each round [1]. Increasing the number of validators (a.k.a. witnesses) comes with an increased robustness against server failures, but

also results in a longer period to reach transaction finality [1] which describes the absolute irreversibility of transactions after 2/3 of all validators approved a given block and its' transactions.

The goal of the public stress-test performed on the graphene-based testnet was to identify the limiting factors and bottlenecks at scale with multiple parties involved. We furthermore wanted to demonstrate scalability of current state of the art blockchain technologies.

2   Testnet Setup

We have deployed a separated blockchain for the public testnet that has been launcehd in January 2016. That blockchain was open to the public and every new account has been donated some of the core assets called `TEST`. By the time of the stress-test, the blockchain has had over 6,800,000 blocks, already and over 25,000,000 operations processed.

2.1   Software

The software for the testnet backend has been maintained by BitShares Europe and is available for review on github.com. It is an almost identical fork of the Graphene code base that BitShares is built on with only marginal changes to accommodate the separated blockchain.

The tools that have been developed for the stresstest and the analysis are mostly available in separated repositories aswell.

2.2   Validators

The validators' job is to collect unconfirmed and pending transactions as received through a Peer-2-Peer network, verify and validate them and publish your approval over those transactions in form of a signed block that carries those transactions.

Given that the Graphene testnet also uses Delegated Proof of Stake (DPOS) as it's consensus mechanism, the validators (a.k.a. block producers) can be voted in and out by means of the stake-based governance system [1]. This allows us to 1. modify the number of validators 2. replace failing validators by standby validators 3. pick validators that are closer geographically (if location is known) every maintenance interval. This interval is used to tally all votes made since the previous maintenance block and is set to 5 min on the test-network.

At the beginning of the stress-test, we will have these validators active:

blckchnd-x Intel Xeon E3, 32GB RAM, bare bone, Germany

jim.witness1 Intel XeonÂ® E5, 28-56GB RAM, Azure, South Korea

smailer-5 Intel Xeon E3, 32GB RAM, Germany

init0 Intel Core i7, 32GB RAM, bare bone, Germany

lafona2 Intel Avoton, 16GB RAM, France

delegate.ihashfury Intel Atom C2750, 32GB RAM, bare bone, France

f0x

taconator-witness

fr-blockpay

de-blockpay

arthur-devling

alpha-jpn

2.3   Reference Full Node and Seed Node

A bare bone reference node is provided by BitShares Europe that allows participants to interface with the Peer-2-Peer network without running their own full-nodes. The endpoint is available at `wss://node.testnet.bitshares.eu` and is powered by a Intel Core i7 with 64GB of RAM which carries two fully balanced full nodes to deal with the traffic.

A frontend-wallet is provided under `https://testnet.bitshares.eu`.

3   Limiting Factors

In this section we briefly discuss the limiting factors we have identified prior to the stress-test. For the sake of proper description, we first need to look into the distinction of *blocks*, *transactions*, and *operations*.

Similar to other blockchain technologies (i.e. Bitcoin), a single block may contain multiple transactions. Each transaction is signed by one or multiple entities and thus requires the validators to perform elliptic curve signature verification as well as public key recovery for authorization.

In contrast to other blockchains, Graphene-based blockchain *explicitly* allow to bundle multiple *operations* into a single transaction. Similar to Bitcoin allowing to bundle multiple outputs, but with the options to execute different smart contracts offered by the blockchain subsequently. The easiest application is similar to Bitcoin's multi-send feature where a single user sends bitcoins to many addresses. In the case of Graphene/BitShares, the user would also sign a single transaction with a single signature but the transaction would carry many `transfer` operations. Additionally, a user may put a combination of `trade`/`transfer`/`borrow` operations (or any other) into a single transaction to ensure that they are executed subsequently.

As can be seen, the main difference between bundling many transactions into a block and bundling many operations into a transactions is that in the latter case, the operations are guaranteed to be executed subsequently and that only a single authorization (e.g. signature) needs to be validated and verified.

This distinction is important as our test results will clearly distinguish between the throughput of *operations* and the throughput of *transactions*.

From a scalability point of view, the limiting factors are the time and resources that are required to validate a signature for a given transaction and the time and resources that are required to append a transactions to the blockchain and execute its corresponding smart contract/operation.

Since the Graphene technology is built such that the signature validation can be done independent of the blockchain's current database state, the signature verification and key recovery can be trivially parallelized by means of a cluster or the use of a graphics processing unit (GPU). However, as the required software for this parallel verification was not available at the time of the stress-test, we expect the throughput to be significantly higher once we can validated on a GPU.

For this reason, and because we want to see the limiting factors when applying validated transactions to the blockchain, parts of our test scenario are focused around producing transactions that carry hundreds of *transfer* operations with just a single signature to be verified.

4   Phases of the Stress-Test

Since we use Graphene as our underlying technology, most blockchain parameters can be changed in real-time with no need for protocol upgrades or hard forks.

In contrast to the public BitShares network, the majority of the stake in the public testnet is owned by BitShares Europe and allows us to change the parameters without the need to collude with other stakeholders.

This allows us to setup a multiphase stress-test that will go through a set of different blockchain parameters to gradually grow the processed amount of transactions on the blockchain.

4.1   Modified Blockchain Parameters

For our stress-test, we have decided to focus on three blockchain parameters only:

Max. block size This limit allows us to modify the size of the blocks that are considered valid by the network. For our test, the size will be between $1\,\mathrm{MB}$ and $10\,\mathrm{MB}$. The limiting factor is the supported data rate and connectivity of the validating nodes since blocks need to be produce and broadcast within a certain time interval. A broadcast block needs to be received by the subsequent validator in time, otherwise the subsequent block cannot be linked to the expected previous block properly.

Max. transaction size Each *block* can carry multiple *transaction* and, in contrast to many other blockchain technologies, transactions on Graphene-based blockchains can carry multiple *operations*. In our test, we assume that most of the operations are simple *transfers* of size $22\,\mathrm{bytes}$. Together with the transaction header, a simple single-transfer (unsigned) transaction is $36\,\mathrm{bytes}$ large. During the stress-test, we allow between 50 and 1000 transfer operations to be bundled into a single transaction.

Block confirmation time The block confirmation time is the expected time between blocks. At the beginning we will start with a $3\,\mathrm{s}$ block interval and reduce it down to $1\,\mathrm{s}$ at which point

we expect the network to loose it's robustness as it is distributed globally and round-trip times together with the need to transmit non-empty blocks might take longer.

4.2   Tested Parameter Sets

The stress-test contained seven phrases. As can be seen, the last two phases change the block confirmation time and drastically reduce the maximum block size to ensure that blocks can at least be transferred in a timely manner. Whether blocks are propagated to the witnesses in time is out of our hands since we are running on a public and globally distributed Peer-2-Peer network.

phase	max. tx size	max. block size	block interval
1	1114 bytes	1 MB	3 s
2	1114 bytes	5 MB	3 s
3	1114 bytes	10 MB	3 s
4	11,014 bytes	10 MB	3 s
5	22,014 bytes	10 MB	3 s
6	22,014 bytes	2 MB	2 s
7	22,014 bytes	1 MB	1 s

5   Results

5.1   Processed Transactions/Operations

5.2   Transaction/Operation Throughput

5.3   Memory and Processing Requirements

6   Conclusions

7   Acknoledgements

References

[1] "BitShares 2.0: General Documentation," *BitShares Whitepapers*, 2015.