The Graphene Technology - Overview

Graphene Foundation
Deventer, Netherlands
contact@graphene.community

This is a preliminary release.

***Abstract*—The Graphene technology is an industrial-grade decentralized framework to realize high-performance, scalable and secure business solutions utilizing the Blockchain.**

1 Introduction

The Graphene technology was first used to realize the BitShares Blockchain, which was launched 2015 with its roots already back in 2013. The BitShares Blockchain utilized the Graphene technology to implement high-performance smart contracts with focus on the financial services sector. It has been used for several other projects, e.g. Steem, Muse and Peerplays, and recently for EOSIO in the core concepts.

What is Blockchain Blockchain, also known as distributed ledger technology, allows a network of users to keep a record of transactions. In layman's terms, a blockchain is like an "Excel sheet" where each column and row (blocks) have records (words, numbers or whatever you put into an excel sheet) recorded. However unlike normal Excel sheets and databases, the blockchain is distributed, meaning that it runs across multiple nodes (computers) and for a new block to be added, all nodes have to "agree" or come to a consensus. Blockchain technology is the technology of the future and provides a trust-less platform without the need for a middle man; security through cryptography and time stamps; and is decentralized which prevents a single point of failure.

This document serves to introduce the Graphene technology as a framework for realizing a Blockchain, its architecture as well as its governance system using a core native token.

2 Architecture

The Graphene technology is a framework that is available under MIT license and that can be used to realize a Blockchain that constitutes the following components which are described individually.

2.1 Transactions

When users want to interact with any Blockchain, they construct so called *transactions* and transmit them to the network (see section 2.3). These present messages contain instructions about what particular *operation(s)* a user wants to use. A common operation is the simple *transfer* operation that comes with transfer-specific instructions that provides the necessary information for this action, such as the sender, receiver, the amount to transfer as well as an optional encrypted memo. To allow multiple operations to take place subsequently, multiple operations can be bundled into a single transaction.

To identify against the system, transactions are cryptographically signed by the users. These signatures *authenticate* a user and provide *authorization* for the operations containted in the transaction. Transactions can be required to include a fee or other rate-limiting measure to prevent spamming the network.

2.2 Blockchain

The Blockchain serves as a journal (e.g. a ledger) of user-signed instructions that become a binding agreement as soon as they are included into a block. After inclusion into a block, the agreements are stored indefinitely and immutably by means of a hash-linked-list (the Blockchain). From this ordered sequence of transactions, a *current state* (think: account balances) can be determined by processing all transactions consecutively starting at the very first block. As we will see later, the software will ensure that instructions that are stored in the Blockchain have been successfully authenticated and validated. For validating and processing operations a common set of rules define the consequences of particular actions, which are part of the of the Blockchain protocol (see section 2.5).

2.3 Networking

A Blockchain merely defines a means of storage and can be used in a non-distributed, single-participant fashion as well as in a distributed internet-based mesh network often referred to as Peer-2-Peer (P2P) network. In the latter case, multiple parties are connected with each other in a way that incoming transactions are forwarded to every other connected participant. A transaction ultimately reaches a so called *block producer*. A block producer verifies incoming transactions against a hard-coded protocol and bundles them into a single block that is added to the existing Blockchain. At this point, a transaction is considered confirmed and executed. The effects of an executed operation on the current state are defined in the Blockchain protocol (see section 2.5).

2.4 Consensus

Consensus is the process by which a community comes to a universally recognized, unambiguous agreement on a piece of information. In the context of Blockchains, consensus means

agreement about the validity rules for transactions (i.e. the Blockchain protocol - see section 2.5), and the order in which they have been observed by the Blockchain. This ultimately results in an agreement about the *current state* that is build deterministically from those validity rules and the sequence of transactions.

The most commonly known consensus scheme is Proof-of-Work (PoW) as introduced by the Bitcoin Blockchain. Most dominant disadvantage is the heavy power consumption and the scalability in terms of transactions per second and confirmation times. The Graphene technology makes use of an algorithm called Delegated Proof of Stake (DPoS) that was developed specifically to replace the wasteful 'mining' process, increase throughput and reduce reaction times of the Blockchain. It is a tremendous improvement when it comes to consumption of electricity.

DPoS allows to generate a new block at a fixed rate (block production/confirmation time) with minimal computational requirements. This means that the Blockchain can process more transactions in significantly less time and at almost no cost when compared to PoW-based Blockchains[1]. Block production is performed by a set of so called *witnesses* (block producers) that take turns. After every turn, the order of block producers is randomized in a deterministic manner such that all parties agree on the new order.

2.5 Protocol

The most essential part of Blockchain technologies is referred to in this document as Blockchain protocol. It defines the behavior of the entire system including consequences and side-effects when processing transactions. Users utilize particular features by crafting a transaction that contains a particular letter-of-interest (also referred to as *operation*).

Since the Blockchain, as a means of a storage, only stores incremental changes (e.g. transfers), the final balance of each account together with other information needs to be tracked separately in the *current state*.

It is important to note that the protocol is deterministic in the sense that the very same state is generated when applying the same sequence of operations (as provided by the Blockchain). This makes Blockchain technologies tamper proof and auditable.

Each operation of them hooks into the Blockchain protocol at least three times:

- **Validation**: During validation, the raw instructions (also referred to as *payload*) are checked for consistency. Taking the example of a transfer, it needs to be ensured that the amount to transfer is positive.
- **Evaluation**: In the evaluation step, the operation-specific instruction is validated against the current state of the Blockchain. Taking the example of a transfer, it needs to be ensured that the amount to be transferred is available in the account of the sender.
- **Application**: This step takes action in the sense that it modifies the current state. Taking the example of a transfer, the account balance of the sender is reduced and the account balance of the receiver is increased according to the amount of tokens transferred.

[1] https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

Example: Transfer operation Consider a simple *transfer* operation that sends funds from one account to another. Here, the protocol defines the validation rules such as negative amounts are being prevented. The evaluation ensures that the sender cannot transfer more than what is in his account balance. When applying a transfer from Alice to Bob, Alice is credited the transferred amount while Bob receives the amount. Here, *transfer* refers to the operation *type*, while the sender, receiver, and amount refers to the operation-specific instructions. Obviously, different operation types come with different instructions.

2.6 Extensibility

The Graphene technology is extensively modularized and implements its operations independently of each other. This allows for adding new features once the corresponding code, which the implements validation, evaluation and application methods, reaches maturity. In a sense, operations for a Blockchain implemented with the Graphene technology framework are *smart-contracts* and allows for extending the range of functions of the system. This can be done in a *static* or *dynamic* fashion, which will be illustrated with two examples.

Static smart contracts Example BitShares Blockchain: In contrast to other smart-contracting platforms, the BitShares Blockchain requires new features to be vetted by the core developers and approved by the core token holders before they can be installed by means of a network-wide protocol upgrade. As a consequence, the platform is considered much more solid as new features require to go through multiple stages of quality assurance. These protocol upgrades are well coordinated and already happened 28 times (Q3/2018) in the past.

Dynamic smart contracts Example EOSIO Software: While many key components of EOSIO are heavily reworked, the concepts of the technology remain the same. The EOSIO Software allows that smart contracts are put on the Blockchain dynamically and are then interpreted on the fly. This allows to be flexible in the provided smart contracts, but it completely removes the review and quality assurance process and the user is required to trust every single smart contract.

2.7 Performance and Scalability

Blockchains utilizing the Graphene framework have publicly demonstrated sustaining over 3,000 (three thousand) *transactions* per second and over 22,000 (twentytwothausand) *operations* per second on a distributed test network, as shown by the stress test of the BitShares Blockchain. This technology can easily scale to over 100,000 (hundred thousand) or more transactions per second with relatively straightforward improvements to server capacity and communication protocols.

To achieve this industry-leading performance, the Graphene

technology has borrowed lessons learned from the LMAX Exchange[2], which is able to process 6 million transactions per second. Among these lessons are the following key points:

- Keep everything in memory.
- Keep the core business logic in a single thread.
- Keep cryptographic operations (hashes and signatures) out of the core business logic.
- Divide validation into state-dependent and state-independent checks.
- Use an object oriented data model.

By following these simple rules, the Graphene technology is theoretically able to process >10,000 (ten thousand) transactions per second without any significant effort devoted to optimization. To put things into perspective[3], at peak times, the Ethereum and Bitcoin Blockchain jointly process roughly 0.7% of the peak capacity of the BitShares Blockchain (Q3/2018, maximum capacity according to distributed stress testing).

3 Identity

The Graphene technology makes use of human-readable account names that have to be registered together with public-keys in the Blockchain prior to its usage. Thus, the Blockchain acts as a name-to-public-key resolver similar to the traditional Domain Name Service (DNS). These named accounts enable users to easily remember and communicate their account information instead of using error-prone alphanumeric *addresses*. Depending on individual needs, applications making use of Graphene technology can create environments which have full KYC (Know Your Customer) support through so called *whitelisting* which enables a maximum of control or transparency when so desired.

3.1 Permissions

The Graphene technology designs permissions around accounts, rather than around cryptography, making it easier to use. Every account can be controlled by combination of weighted accounts and/or keys. This creates a hierarchical structure that reflects how permissions are organized in real life, and makes multi-user control over funds easier for users. Hence, the Graphene technology does technically not have multi-signature accounts, but has multi-account permissions. That said, each public/private key pair is assigned a weight, and a threshold is defined for the *authority* (see definition below). In order for a transaction to be valid, sufficient entities must sign so that the sum of their weights meets or exceeds the threshold.

3.2 Authorities

The Graphene technology employs a first of its kind hierarchical private key system to facilitate regular keys and backup keys. Regular (*active*) keys are for day-to-day usage, while a separate backup (*owner*) key can be used to recover access to an account in case of loss of the regular keys. Ideally, the owner key is meant to be stored offline, and only used when the account's keys need to be changed or to recover a lost key. Most software that supports the Graphene technology also facilitates the use of a Master Password that encrypts the client's keys locally.

[2] https://martinfowler.com/articles/lmax.html
[3] http://blocktivity.info/

4 The core utility token

The Graphene technology utilizes a core native token – arbitrarily called GPH in this section – which serves as a utility token and offers governance properties to its holders. Governance describes the progress of governing the Blockchains many variable aspects in a way it it can adapt to future changes more easily.

4.1 Governance

The Graphene technology allows that decisions are made by the holders of GPH core native token, weighted by the amount of GPH owned. In order to improve voting participation and simplify the life of GPH holders, voters can either vote directly or delegate voting power to so called *proxies*. This is similar to a representative democracy, where selected persons decide the course of action. Those leaders have to account for their actions and can be unelected by the core token holders. Unwanted actions includes censoring, favoring, or simply the failure to produce blocks in a timely manner. However, the difference to a democracy is that voters in the community have their vote weighted by the amount of GPH that they own in their account. Votes may or may not decay over time, depending on the actual implementation.

At any time, voters have to decide on the following aspects of a Blockchain powered by the Graphene technology. The list may not be complete for an actual implementation as other aspects can be added to be voted on.

Members for Block Production (Witnesses) Block production is arranged through DPoS, which requires block producers to run for witness and campaign for sufficient votes from GPH holders before they can produce blocks on the Blockchain and consequently get rewarded per produced block. Given the governance system and quick re-tallying of votes, a misbehaving block producer can be dismissed within hours. Next to the actual selection of block producers, the voters also have a say over how many block producers should exist.

Project Funding (Workers) Last but not least, the voters have control over who receives funding from the Working Budget of the Blockchain. A worker applies for project funding and needs to campaign for sufficient votes before being rewarded. Similar to block producers and committee members, the rigorous voting system allows almost immediate removal by BTS holders and proxies.

Example: Introducing Blockchain Governance (Committee) The BitShares Blockchain introduces an additional entity that needs to be voted on, namely the committee. The Committee comprises a board that has control over a few Blockchain parameters such as block size, block time, witness reward, and over 30 others. Additionally, the BitShares platform introduces transaction fees that need to be paid by the users.

Those fees replenish the working budget and are the economical model of the BitShares Blockchain. The committee governs the fee schedule which defines the minimum fee for each operation. Voters can cast a vote for how many members the committee should constitute as well as vote for a particular set of members.

4.2 Initial Allocation

In the *genesis block* of a Blockchain the initial supply of the native core token is distributed to individual keys. These tokens can be claimed by proving ownership of the corresponding private key.

The core token usually comes with a limited supply that is different from circulating (liquid) supply. A maximum supply is to be put in place on the Blockchain. This can never be changed. Usually, not all core tokens are distributed initially, the remaining are set aside for future project funding and rewarding block producers, and are only accessible with approval by the GPH holders through the worker system. This so called working budget is also often referred to as *reserves*.

4.3 Supply

In this section, we would like to discuss the actual supply of the core GPH token in more detail. Firstly, we define the *max supply* as the supply that can be in circulation at most, similar to the fact that there will only ever be *up to* 21 million BTC on the Bitcoin Blockchain. Furthermore, the *circulating supply* represents that amount that currently is in circulation and held by participants on the Blockchain. Obviously, the circulating supply will always be less than or equal to the max supply. Furthermore, for the voting process, only the *circulating supply* applies.

4.4 Working Budget

The difference between max supply and circulating supply is called the *Working Budget* and has often been referred to to as the *reserves* in the past. A daily budget is defined that is used for development, with a defined maximum daily payout. From this daily budget payments are made for block production as well as for project funding. Of course, the GPH holders have the choice and need to approve payouts from the working budget.

Block Production (Witnesses) Block production comes at a cost for running and maintaining equipment. This is acknowledged by rewarding block producers in core GPH tokens per produced block. Mechanisms to adjust the amount per block can be put in place. Those GPH are taken from the working budget.

Project Funding (Workers) A certain amount of the daily available tokens can be allocated to make development possible by means of workers. Anyone can set up a worker on a Blockchain powered by the Graphene technology and ask for a daily allowance in GPH. If the GPH holders approve a particular worker, the GPH are transferred from the daily budget. A soft-limit defines the maximum amount of the daily budget that is given to all approved workers. Consequently, those workers that have received the most votes from GPH holders will receive their funds first. This means that workers, even if approved, may not be funded if the aforementioned threshold is hit. Furthermore, workers constantly stand under the scrutiny of the GPH holders who can disapprove (i.e. retract their vote, 'fire') workers that do not deliver.

5 Summary

Graphene is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, including leaders in finance, banking, IoT, supply chain, manufacturing and technology. Graphene uses P2P technology to operate businesses autonomously with no central authority. Transactions with instructions to the business logic are carried out collectively by the entire network. Graphene is open-source; its design is public and everyone can take parts and/or contribute. Through many of its unique properties, Graphene allows exciting uses of Blockchain Technology that could not exist previously including such as BitShares, Steem, PeerPlays, Muse and others.

Some highlights to conclude this overview:

Protection against fraud Any business knows the problem of transaction uniqueness and its audit trail that are revisited by auditors. Transactions on a Graphene-based blockchain are irreversible and secure, meaning that the cost of fraud is no longer pushed onto the shoulders of the business.

Fast and distributed transaction processing that scales A Graphene-based blockchain can execute many thousands of transactions every second in a distributed network, yet reach consensus about your business logic. In contrast to other blockchain systems, Graphene is capable of confirming your transactions in single digit seconds.

Multi-signature and accounts Graphene blockchains make use of an account-based transaction processing. This means, participants obtain a named account and can use it like an email address. Thanks to multi-signature, accounts can be secured in a way that requires multiple people to approve a transaction before it becomes valid.

Accounting transparency Many organizations are required to produce accounting documents about their activity. Using a Graphene-based blockchain allows you to offer the highest level of transparency since you can provide information to verify balances and transactions through the Blockchain. For example, non-profit organizations can allow the public to see how much they received in donations.

// add year and conclustion