BigTangle: The Revolution in Blockchain Technology

The Whitepaper

BigTangle

Brief overview

The core idea

The core idea of the BigTangle project is the creation of a global economic system in which all actors, from private individuals to companies to states can interact directly or indirectly with all actors at any time and in a simple manner, i.e. manage their economies and assets. Blockchain technology thus becomes the global economic and social standard through BigTangle.

The problems

As a payment system, the solution must be equal to or better than Paypal, Visa and Alipay in terms of scalability and cost-performance.
As a decentralized market and exchanges, the solution has to be equal to or better than NASDAQ, the NY Exchange or Binance in terms of scalability and confirmation speed.
As a decentralized supply chain management system, the solution must be applicable on aglobal scale.
As a decentralized E-Commerce solution, the solution must be equal to or better than Amazon and Alibaba by eliminating fees and centralization overhead.

The Solution

Only a solution with a parallelizable architecture and an implementation based on Big Data technology can achieve all of the aforementioned properties at the same time. Without sufficient scalability and cost-performance, a cryptocurrency network cannot achieve ubiquity and become standard.
BigTangle is a cryptocurrency network extending directed acyclic graph architectures with Markov Chain Monte Carlo (MCMC) as a consensus algorithm and distributed Proof-of-Work. Through the use of industry standard big data technology in conjunction with the parallelizable architecture, BigTangle is a successor to conventional blockchains in the sense that it generalizes existing blockchain and smart contract architectures and makes them usable on a global scale.
BigTangle focuses on economically important key use cases. Custom token issuances, market exchanges, mining and smart contracts are supported.
BigTangle is very similar to family trees with MCMC as natural selection process. The application is build on microservices and is very easy for use.
Because of this and the unique design, BigTangle has the potential to exist as the only platform of its kind comparable to the Internet.

The advantages

Ease of use, Completely Feeless, Real-Time Transaction Confirmation, Infinite Scalability, Smart Contracts, Permissionless, Trustless, Decentralized App, Distributed Proof of Work and Quantum Security.

BigTangle Whitepaper

Kai Cui, Jianjun Cui,
Maximilian Hensel, Maximilian Lowin
kai.cui@bigtangle.net

July 29, 2018. Version 1.5

Abstract

BigTangle is a cryptocurrency network extending directed acyclic graph architectures with Markov Chain Monte Carlo (MCMC) as consensus algorithm. Through the use of industry-grade big data technology in conjunction with its parallelizable architecture, BigTangle is a successor to Bitcoin that can fulfill economically important key use-cases. Proof-of-Work mining, smart contracts and custom token self-issuances are supported. Key Features: Proof-of-Work Mining, Completely Feeless, Real-Time Confirmation, Infinite Scalability, Permissionless, Trustless, Decentralized, Distributed Proof of Work and Quantum Security.

I. Introduction

Since the inception of Bitcoin in 2009 [1], new cryptocurrencies have been rising in popularity and could potentially rise to rival fiat currencies in the future. Transitioning to such a digital currency offers various advantages, of which the authors believe the infrastructure cost savings in the financial sector from revolutionizing highly complex and opaque traditional transaction systems of current banking and stock market technologies to be the most attractive.

To achieve this attractivity, two key properties are required: scalability and the absence of fees in general. Additionally, low transaction confirmation times, ease of use, security and anonymity are other baseline properties required for widespread adoption. Traditional Proof-of-Work-based blockchain approaches fail to meet these requirements [7], while Proof-of-Stake-based approaches [20] might face other problems such as voter politics, mining regulation etc.

In this paper we propose BigTangle, a scalable Proof-of-Work-based cryptocurrency as a protocol for the internet of value. The proposed solution's architecture is a directed acyclic graph (DAG) generalization of blockchains with MCMC as consensus algorithm [4] that is capable of scaling to infinite transactions per second while remaining feeless. The recently popularized DAG architectures [4][8][9] have the potential to scale beyond traditional blockchains and avoid problems of blockchains such as block forks [15] and scalability issues [7].

BigTangle's features are a superset of features supported by Bitcoin, including but not limited to escrow transactions, bonded contracts, third-party arbitration, multiparty signatures and its stack language Script in general. The Bitcoin blockchain is a special case in BigTangle's DAG architecture. Using the mining reward process detailed later, it is possible to change the BigTangle's parameters to return to a conventional blockchain.

In contrast to most recent high performance cryptocurrencies, BigTangle employs a Proof-of-Work-based mining process where most honest transactions are rewarded and help securing the network. This mining process incentivises users to run full nodes and secure the network, providing the advantages

of inflationary currency models and value through economic coupling to the real world. Full node operators and miners are therefore compensated with a time-normalized amount of new BigTangle tokens proportional to their mining contribution.

BigTangle is a successor to Bitcoin that focuses on a variety of economically important key use-cases: Beyond the decentralization of payment processing, the network can be used as a base service layer for the decentralization of markets in general, transfer and ownership management, authenticity proofs for assets of any kind or supply chains and ownership management as it has been described in as early as 1998 [25].

In the authors' opinion, a transaction system capable of supporting the global transaction volume of banks and stock markets requires sufficiently performant computer clusters to work as full nodes. BigTangle employs established industrial grade big data technologies such as Apache Kafka, Spark and its GraphX API.

By utilizing local approximations to previously non-scalable graph computations of the asynchronous Tangle in addition to big data computation technologies, the proposed solution suffices the aforementioned properties.

Minimal end-user client requirements are a side effect of using cluster nodes as service providers, allowing end-users to participate and issue transactions without having to store and handle huge amounts of data but instead providing hashing power.

II. Overview

The protocol maintains a public ledger of transactions that are contained within blocks. In contrast to blockchain-based solutions, blocks reference and thereby approve two previous blocks and indirectly their predecessors to form a directed acyclic graph. A more detailed explanation of the base architecture and other important existing concepts can be found in [4].

As per protocol, a set of blocks is valid if all contained blocks are valid per se and no conflicts exist between any of the contained blocks. When issuing new blocks, it is to be made sure that the set of blocks approved[1] by the new block is valid. Contributing blocks therefore helps securing and validating BigTangle by increasing the confirmation level of all approved blocks.

Participants are connected in a standard peer-to-peer network via a gossip protocol as fall-back solution. In addition to that, BigTangle will employ Apache Kafka data streaming to increase scalability and propagation speed. Network participants are split into two different archetypes: clients and network nodes. Generic end-users and small-time miners can participate as clients that issue transactions with the aid of a network node, using their own hashing power to create blocks and solve the low-difficulty Proof-of-Work themselves, while network nodes maintain a copy of the graph and provide validated tip pairs to build upon.

The network nodes can derive account balances and transaction states from the graph and provide the information to clients in exchange for e.g. hashing power. Furthermore, a network node operator might choose to also participate in the mining process himself by using his available computational power to solve Proof-of-Works for new blocks in addition to validating the blocks.

The server-side validation as described in [4] can be effectively computed by utilizing approximations. The network nodes create ~~their own local view~~ of the Tangle by maintaining helper constructs such as locally confirmed block sets called milestones, based on which

[1] Any indirectly or directly referenced blocks (ancestors) of a block are defined as approved by it.

validation is performed. The consequence is that additional conflicts are checked over the naive Tangle conflict checking, resulting in a stricter validity evaluation than without this approximation. Additional information can be found in chapter 3.

Popular solutions to scalable cryptocurrencies include highly complex sharding, voting-based and capital-based Proof-of-Stake or workarounds [7] with the potential for exorbitant fees. Instead, we propose a fully permissionless solution that returns to the well-known Proof of Work approach of the original Bitcoin solution.

Mining rewards serve as a network maintenance incentive instead of fees. Since it is impossible without sharding to allow every device to participate as network nodes while achieving infinite scalability, it is instead intended that network nodes are deployed in sufficiently big computer clusters utilizing state-of-the-art big data technology. Instead of end-users hosting full network nodes and requiring significant computational resources, their clients cooperate with network nodes by e.g. providing mining revenue and building blocks.

Nevertheless, the network stays permissionless and avoids centralized constructs. As long as nodes fulfill the minimum requirements for keeping up with the transaction volume, any node can effectively participate in network validation and mining.

Independent of the mining process, it is also intended for full nodes to exist regardless of mining rewards. For example, super market chains can deploy their own full nodes to process large transaction volumes themselves.

By utilizing Proof-of-Work, we can avoid drawbacks of Proof-of-Stake-based models such as political apathy, regulations and lower financial stability due to missing hardware investments.

To summarize, general properties provided by BigTangle are high hashing power and time-normalized inflation due to mining, infinite scalability, sufficiently fast transaction confirmation times, full decentralization, trustlessness and permissionlessness, feeless transactions and in-principle quantum security. To make use of these properties, BigTangle will natively support custom token issuances, smart contracts and decentralized token exchanges, in turn enabling economically important use cases.

III. Technical Details

In the following, we briefly discuss technical key details. For recapitulation on established concepts, please refer to existing literature such as [4].

i. Implementation

To achieve high scalability, the node implementation is built upon industry standard big data technologies, including but not limited to Apache Hadoop [28], Apache Kafka [29] and Apache Spark [27]. As mentioned before, Kafka is used to achieve efficient propagation, while Spark and its GraphX API are used to achieve efficient and scalable graph processing in the form of Pregel algorithms [30].

ii. Cryptographic Components

BigTangle relies on elliptic curve cryptography for multi-use signatures. The curve used is Bitcoin's Secp256k1. Similarly, the public keys are also Base-58 encoded, allowing Bitcoin users to reuse their addresses in BigTangle. The currently proposed Proof-of-Work hashing function is the Equihash algorithm [5]. The base architecture is quantum resistant as shown in [4].

iii. Transactions and Accounts

The accounting is based on Bitcoin's Unspent Transaction Output (UTXO) model. Users can

issue valid transactions as long as they can provide a valid input script for the used UTXOs. The UTXOs use Bitcoins Turing-incomplete stack language allowing for the same set of functionality as found in Bitcoin.

iv. DAG Architecture

As found in [4], we provide a short reasoning on why the Tangle base architecture as mentioned before is qualitatively stable and leads to short confirmation times even for extremely high block volumes.

The following assumptions are made: There exists a valid Poisson point process model for the incoming blocks with constant rate λ, an average block issuance time h, a stationary number of tips L_0, an idealized network latency of h such that any blocks issued at time t become visible as new tips at time $t+h$ and a tip selection in form of a uniform probability distribution over all current tips.

Since approximately λh invisible tips exist due to latency, an equal amount of tips must no longer be tips anymore due to stationarity. This means that the probability of choosing new tips is $r/(r+\lambda h)$ with the current amount of visible tips r. This leads to the mean of $2r/(r+\lambda h)$ tips chosen by a new block. Again, due to stationarity the mean must be equal to 1 such that the new tips replace the old tips without changing the average number of tips. This leads to $r = \lambda h$ or $L_0 = 2\lambda h$. Assuming L_0 to be large henceforth, this leads to an expected time until first approval of $L_0/(2\lambda) = h$.

Going further, there exists an average time until almost all new blocks approve a block that can be calculated as follows. At that point of time, the block can be considered locally confirmed due to the fact that most new blocks will approve the block.

Let $K(t)$ be the expected amount of approving tips at time t. Since the probability of a tip not being a tip after time h is the tip substitution rate $L_0/(2\lambda h) = 1/2$, at time t one half of $K(t-h)$ tips remain unapproved, while the other half is approved at least once. Let $\mathcal{A}$ be the set of tips from time $t-h$ that remain unapproved at time t and $\mathcal{B}$ the set of tips from time $t-h$ that were already approved at time t. Analogously to previous results, the probability p_1 that a new block approves at least 1 block from $\mathcal{B}$ and none from $\mathcal{A}$ such that K increases equals to

$$p_1 = \frac{K(t-h)^2}{2L_0} + \frac{K(t-h)}{L_0}\left(1 - \frac{K(t-h)}{2L_0}\right) \quad (1)$$

and the probability p_2 that a new block approves $\mathcal{B}$ twice such that K decreases is

$$p_2 = \frac{K(t-h)^2}{2L_0} \quad (2)$$

The differential equation for $K(t)$ follows: [11]

$$\begin{aligned} \dot{K}(t) &= \lambda \cdot (p_1 - p_2) \\ &= \lambda \cdot \frac{K(t-h)}{L_0}\left(2 - \frac{K(t-h)}{L_0}\right) \end{aligned} \quad (3)$$

For $K(t)$ up to some $\epsilon L_0 \ll L_0$ the quadratic term can be dropped and with $\lambda h/L_0 = 1/2$ equation (3) is simplified to

$$\dot{K}(t) = \frac{K(t-h)}{2h} \quad (4)$$

With $K(0) = 1$ and $K(t) = e^{\frac{c}{h}t}$ it follows that

$$K(t) = e^{W(\frac{1}{2})\frac{t}{h}} \approx e^{0.352\frac{t}{h}} \quad (5)$$

with $W(\cdot)$ denoting the Lambert W function. The time t_0 until ϵL_0 is reached then evaluates to

$$t_0 \approx \frac{h}{W(\frac{1}{2})} \ln \frac{L_0}{\epsilon} \leq 2.84 \cdot h \ln L_0 \quad (6)$$

The time between $K(t)$ reaching ϵL_0 and approximately L_0 is neglected, resulting in an average time until confirmation of a block is given by (6). Remembering $L_0 = \lambda h$, this result shows that the confirmation time of this architecture scales logarithmically with the

block rate such that even very high block rates have a negligible effect on confirmation time.

Although only shown under simplifying assumptions such as uniform tip selection probability and idealized network latency, it can be argued that the above qualitatively holds for MCMC approval strategies and real networks. Simulations have shown that the confirmation time for MCMC approval strategies follows the results shown above [13].

v. Blocks

A block consists of its header and transactions. In addition to fields existing in Bitcoin, the header contains an additional reference to a previous block, a miner address, a type field for the types as seen below and additional data depending on their type. We list all base block types and their use:

Transfer Blocks contain transactions intended to transfer value from one owner to another.

Cross Domain Transfer Blocks contain transactions intended to transfer value from one domain to another. For more information on their intended use, see chapter BigTangle Intranet.

Mining Reward Blocks contain mining reward transactions that are computed in a deterministic fashion. They can require a more difficult Proof-of-Work than standard blocks. More on this in the mining process detailed later.

Token Issuance Blocks are used to issue custom tokens. Token issuances are identified by address plus sequence number and they are legitimized by the corresponding private key signatures. They can be configured to allow or disallow multiple further issuances.

Storage Blocks could be used to store minuscule amounts of user data. User data is identified by address and usage is legitimized by the corresponding private key signatures and the user data can be encrypted. User data is treated as a value object and can be transferred and traded. The BigTangle Mainnet either limits the size of the storage or prohibits such storage functions completely. We thereby create an application layer storage network based on pay for use.

Smart Contract Blocks are used to create a distributed virtual machine for decentralized autonomous corporations, smart contracts and any other distributed applications similar to other alternative blockchains [22][23].

The distributed applications can be implemented in most modern languages and are not limited to using specialized languages. The relevant code and state data is saved in the block as VM containers using technology such as Docker Composer [19] or Kubernetes Containers [16].

The execution changes the state data and creates new blocks in a sequence. As an example, the Mining Reward Process in BigTangle could be implemented as a smart contract and all nodes would execute the same computation for validated mining rewards based on the current data in BigTangle. As another example, a market exchange application could be implemented in such a form that it uses only a specific node for execution without further required validation (but with transparency).

Governance Blocks are used in the governance process. BigTangle participants can cast votes on matters by issuing governance blocks signed with their private keys.

vi. Participants

Participants can take on different roles in the network depending on their available resources and intentions. In the following, possible types

of participation are ordered in descending requirements of bandwidth, space and computational power:

Full Nodes keep a copy of the full BigTangle. They can fully participate in the network and provide any requested blocks.

Pruning Nodes maintain a pruned version of BigTangle. Only the most recent blocks in terms of confirmation are kept. The node can fully participate in the mining process.

Clients do not keep a copy of BigTangle. They rely on the nodes to provide them with necessary information to create transactions and blocks. Clients can solve Proof-of-Work for their issued blocks and thereby provide incentives for network nodes to assist them.

vii. Protocol Details

Node Maintenance
In the following, we briefly describe assorted technical details for preparing the Tangle base architecture to achieve scalable operation.

As mentioned before, the BigTangle node implementation locally maintains the milestone, a set of blocks it considers as locally confirmed and thereby in principle finalized. In addition, it maintains additional auxiliary information and block statistics such as rating, cumulative weight, depth, height etc. mostly as indicated in [4]. The milestone update process in simplified form consists of the following steps and is performed as often as possible:

1. Update relevant[2] block statistics.
2. Remove no longer locally confirmed blocks and their dependents[3] from milestone. (Should not happen often.)
3. Find new locally confirmed blocks, use conflict resolution procedure and add a non-conflicting set of those blocks to milestone.

We define as locally confirmed any block that has reached the upper confirmation threshold of $t_{upper} = 70\%$ in terms of rating and is sufficiently deep. We also add a hysteresis to removing blocks to prevent unnecessary reorganizations due to the probabilistic nature of MCMC.

Of particular note is the conflict resolution procedure. It will only find application here if malicious nodes successfully approve conflicting block combinations such that conflicting blocks are considered locally confirmed. In short, we process conflicts in descending order of maximum rating occurring in the conflicts, eliminating all losing candidates by removing them and all their dependents from the milestone or candidate set respectively.

Lastly, we may prune no longer relevant blocks and their statistics to prevent BigTangle from growing indefinitely in terms of storage space.

Validation and Approval Selection
When generating a new block, two previous blocks are required to approve such that no conflict exists in the union of referenced blocks (such that they are valid). To find such conflict-free block pairs, we apply an iterative MCMC algorithm similar to the approach shown in [12] to find single tips. By moving a pair of walkers forward while disallowing any conflicts and giving priority to the walker moving to higher rating, we resolve conflicts similar to the conflict resolution procedure detailed before and reach block pairs consistent with the milestone.

It is important to note that since we use the milestone as a shortcut to evaluating validity of new combinations of unconfirmed blocks, the validation overhead stays approximately

[2]Blocks are relevant if they are used in the MCMC random walks of either rating computation or tip selection.
[3]Dependents of a block are all blocks that either approve the block or use an output, token issuances etc. from a transaction of the block.

constant over time under the assumption of constant transaction influx. This coupled with a suitable pruning strategy allows us to avoid increasingly long back-tracing to the genesis block and enables scalability.

A simple example is shown in figure 1. Consider the validation of the black block. Instead of taking the set of all directly or indirectly approved blocks and validating this set, we only take the difference to the milestone (in this example all cyan and black blocks) and then validate this small set against the current milestone. This results in a scalable validity computation.

Note that the milestone block marked with an 'x' is not in the set of directly or indirectly approved blocks but is now also being validated against, meaning that this validation scheme approximates the naive Tangle validity definition by adding additional validation constraints: Instead of only checking for conflicts among all approved blocks, we now check for conflicts among the union of all approved blocks and milestone blocks. These additional constraints do not affect the validation in a negative way, since any milestone blocks are considered locally confirmed and blocks conflicting with the milestone should originally almost never be approved by any new blocks anyways.

In the case of other blocks conflicting with current milestone blocks and achieving higher rating than the milestone blocks, the old milestone blocks are eventually unconfirmed and the new blocks enter the milestone instead.

Mining Process

To incentivise node operation and network maintenance, we introduce a mining process quite similar to the Bitcoin mining process. Since the BigTangle is an asynchronous network and every node sees a different version of the BigTangle, we cannot simply reward what is seen locally since we require an

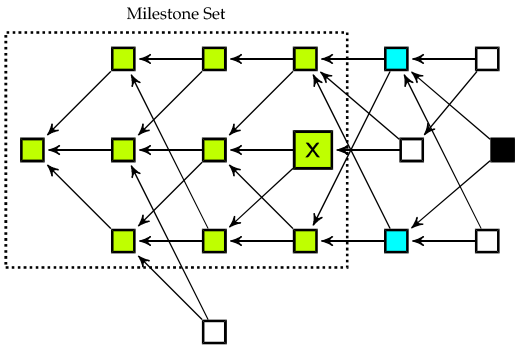


Figure 1: *Example for Validation (black block: block to validate, lime blocks: milestone blocks, white blocks: irrelevant unconfirmed blocks, cyan blocks: to validate vs. milestone, x: additionally confirmed over naive scheme)*

approximately fixed inflation rate. Instead, we introduce a fix point such that every node can calculate the same rewards in a deterministic manner.

Blocks are divided into height intervals and mining reward blocks are eventually issued after passing the reward height intervals to reward blocks created in the interval. All blocks referenced by the mining reward blocks in the respective interval are considered for compensation and the mining reward block must therefore be in conflict with other such blocks of the same reward height interval.

Using only the blocks approved by the mining reward block, we can compute consistent rewards in a deterministic fashion since we know the referenced subgraph to be unbroken in order for the mining reward block to be considered for confirmation. The calculation of rewards is then done locally. As an example, refer to figure 2 where the red dotted box contains potential reward candidates.

A key problem is deciding on a method to approve mining reward blocks that are consistent and fair according to the nodes

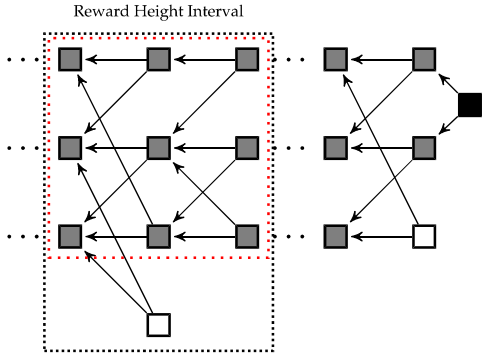


Figure 2: *Example for Mining Process (black block: considered reward block, gray blocks: used in reward calculation, white blocks: not used in calculation, red outline: reward candidates)*

local BigTangle state. The solution is to use the following constraints for approving such mining reward blocks:

All of the approved blocks in the specified height interval must be in the milestone and most of the milestone blocks in the specified height interval must be referenced at the time of reward block reception. To prevent deadlocks due to local inconsistencies, we allow this constraint to be overridden by e.g. sufficient time spent in the milestone, as in that case the majority of the network has accepted the block as valid.

Additionally, we must include countermeasures against non-validating miners' attacks, since otherwise it would be wise to simply build empty transactions upon empty transactions and relink them later.

We punish the blocks with the lowest cumulative weight of their specific height level as seen from the reward block's point view, since attackers will pursue a suboptimal tip selection algorithm in terms of cumulative weight if they avoid validating new blocks. In summary, we calculate cumulative weights for the candidates based on the mining reward block's point of view and then drop out those candidates of lowest cumulative weight in their height.

Finally, the next per-transaction reward is calculated analogously to Bitcoin's difficulty adjustment: By enforcing a monotonous increase of block timestamps and limiting the validity of timestamps from the future, the per-transaction reward is adjusted according to the current transaction rate to enforce an approximately constant coin emission rate.

Token Issuance Process

The token issuance process enables a variety of important use cases for the internet of value and supports features as proposed in [24]. We legitimize a new token issuance block by signing their transactions with the token's corresponding multiple private keys. A token is identified by its ID in form of a public key and sequence number.

The issuances can be configured to e.g. disallow further issuances and enforce other custom token rules. Any issuances following another issuance must adhere to the previous issuance's defined rules, e.g. multi-signature checks: the created tokens must be signed by the given number of keys to spent the tokens. The tokens can then be used analogous to BigTangle's system currency.

IV. Attack Mitigation

In the following, we examine a few new attack vectors due to the milestone process. For generic Tangle attack vectors such as double spends, please refer to [4]. We assume that at least two-thirds of the blocks are made by honest miners and validate correctly. For up to one-third of malicious hashing power, although hashing power does not directly correlate with hijacked rating tips, less than one-third of the rating is hijacked by the attackers for most of the relevant blocks since only one-third of the cumulative weight can be hijacked. Further mitigation can be provided by using low-pass filters during rating calculation.

- If percentage p of rating tips maliciously approve double spends, we must ensure that no reorganization occurs, meaning that the lower confirmation threshold must be below $(1-p)$.

- If percentage p of rating tips maliciously approve a conflict, we must ensure that no network split occurs, meaning that the lower confirmation threshold must be above $(\frac{1-p}{2}+p)$ to prevent the network from having conflicting blocks between their milestones due to a network split where up to 50% of honest miners plus malicious miners would not come to the same consensus as the other honest miners.

The maximum percentage for which such a lower confirmation threshold exists is $p_{max} = 1/3$. The corresponding lower confirmation threshold that follows from the equations is therefore $t_{lower} = 1 - p_{max} = 2/3$.

Parallelizing Proof-of-Work to accumulate highest cumulative weight and in turn gain more rewards is mitigated by the probabilistic nature of MCMC as well as network latency and milestone update rate in general being slower than Proof-of-Work computations.

Not validating any transactions runs the risk of building invalid blocks, while building your own subgraph by approving your own blocks only will lead to high orphaning risk due to introducing more than the optimal amount of transitions on your approved blocks.

Trying to relink a pre-built subgraph of higher height to circumvent gaining less cumulative weight is mitigated since rewarded blocks must all have been in the milestone for a while to be accepted by the majority of hashing power. Since there is network latency, it is argued that such a pre-built construct would not allow one to reward oneself only.

V. Mainnet Governance

To assure that the interests of BigTangle participants are safeguarded after its initial release, BigTangle will implement a governance model to achieve clear consensus on its future development.

Currently, it is planned to use a scheme as follows: the stake of stakeholders and hashing power of miners are counted in separate votes and simple majorities on both votes are required to activate BigTangle software updates.

VI. BigTangle Intranet

The BigTangle software can be deployed in private or other trusted environments, allowing one to run private, owned BigTangle networks with different rule sets.

These BigTangle networks are arranged in a hierarchy, i.e. they possess a parent Tangle such as the Mainnet between which a transfer of values is facilitated. For this purpose, each new Tangle has its own interface accounts (addresses) possessed by the private intranet operator from which it is possible to transfer funds into the parent Tangle and vice versa.

A user interested in transferring funds from the parent Tangle into one of its registered child Tangles can transfer tokens to one of the child Tangle's interface accounts, at which point they are either accepted into the child Tangle or returned by the trusted intranet owner.

Inside of such intranets, consensus protocol, transparency, permissiveness and other rules are set by the trusted intranet owner. Transfers of value can be performed internally as it is pleased. For example, in a work agency intranet it would be possible for clients to pay values to work forces in private and in arbitration of the owning work agency.

In general, enterprises and governments can deploy the software internally and e.g. do KYC (Know Your Customer) as well as privacy protection while remaining compatible with BigTangle's Mainnet.

This allows BigTangle to offer a holistic and flexible approach to value management, enabling privacy, transparency and accountability wherever needed by banks, stock exchanges or enterprises.

VII. Use Cases

Projected practical use cases allow the token to derive value and mainly include the substitution of various currently costly and trust-based technical processes. In the following, some important use cases as part of BigTangle's holistic interpretation of the internet of value are briefly explored.

i. Payment

A simple and important use case is payment processing. By providing scalable infrastructure, BigTangle enables the global transaction volume to be processed in one network. Most importantly, this offers infrastructural cost advantages by eliminating complex and costly processes of traditional payment processing for banks, companies and general populace.

Note that the network hashing power is approximately proportional to the BigTangle internal token market cap and is therefore decoupled from actual transaction volumes, theoretically resulting in downwards unbounded energy upkeep at the cost of increased confirmation times for constant economic risk. Adequate confirmation times can be achieved on a global scale.

ii. Fiat Money

The token issuance protocol can be used to issue bank-backed tokens denoting conventional fiat money. Since the issuance and usage requires no participation in the network, BigTangle is a low cost solution for all parties. Fiat money transactions can then feasibly be processed within seconds on a global scale.

iii. Stock Markets

Markets for stocks, bonds etc. can easily be realized by creating new token equivalents. Companies can publish stocks and use the BigTangle network, essentially substituting costly stock exchange processes by the feeless BigTangle processing network.

Examples for the largest segments that will be affected: Bonds, Swaps, Derivatives, Commodities, Unregistered/Registered securities, Over-the-counter markets, Collateral management, Syndicated loans, Warehouse receipts, Repurchase markets etc.

iv. Micro Transactions

Service fees can now be charged in microdollar range or alternatively via seconds of hashing power due to the departure from winner-takes-it-all, allowing for new business models, e.g. online newspapers with alternatives to commercial advertisement.

v. Supply Chain

Assuming suppliers issuing authenticity tokens, it is trivial to track product authenticity via token transfers. This use case extends into classic supply chain management, allowing the trustless tracking of inventories in supply chains.

VIII. Further Investigations

Proof-of-Work algorithm
ASICs exist for the currently proposed Equihash algorithm. Other Proof-of-Work algorithms may be considered to allow for a more ideal distributed Proof-of-Work on end-user clients.

References

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[2] BigTangle.net, User Guide: https://bigtangle.net

[3] Markov chain Monte Carlo (MCMC), https://en.wikipedia.org/wiki/Markov_chain_Monte_Carlo

[4] Popov, S. (2016). The tangle. https://iota.org/IOTA_Whitepaper.pdf

[5] Biryukov, A., & Khovratovich, D. (2017). Equihash: Asymmetric proof-of-work based on the generalized birthday problem. Ledger, 2, 1-30.

[6] nxtforum.org, (2014). DAG: a generalized blockchain. https://nxtforum.org/proof-of-stake-algorithm/dag-a-generalized-blockchain/

[7] Poon, J., & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.

[8] Sergio Demian Lerner (2015) DagCoin: a cryptocurrency without blocks. https://bitslog.wordpress.com/2015/09/11/dagcoin/

[9] Yonatan Sompolinsky, Aviv Zohar (2013) Accelerating BitcoinâĂŹs Transaction Processing. Fast Money Grows on Trees, Not Chains. https://eprint.iacr.org/2013/881.pdf

[10] Yoad Lewenberg, Yonatan Sompolinsky, Aviv Zohar (2015) Inclusive Block Chain Protocols. http://www.cs.huji.ac.il/~avivz/pubs/15/inclusivebtc.pdf

[11] Sheldon M. Ross (2012) Introduction to Probability Models. 10th ed.

[12] Popov, S., Saa, O., & Finardi, P. (2017). Equilibria in the Tangle. arXiv preprint arXiv:1712.05385.

[13] Kusmierz, B., Staupe, P., & Gal, A. (2018). Extracting Tangle Properties in Continuous Time via Large-Scale Simulations. working paper.

[14] Christian Decker, Jochen Seidel, and Roger Wattenhofer. Bitcoin meets strong consistency. In Proceedings of the 17th International Conference on Distributed Computing and Networking, page 13. ACM, 2016.

[15] Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. In 13th IEEE International Conference on Peer-to-Peer Computing (P2P), Trento, Italy, September 2013.

[16] Kubernetes Container Orchestration. https://kubernetes.io/

[17] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. The honey badger of bft protocols. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 31-42. ACM, 2016.

[18] Yonatan Sompolinsky and Aviv Zohar. Secure high-rate transaction processing in bitcoin. In International Conference on Financial Cryptography and Data Security, pages 507-527. Springer, 2015.

[19] Docker: https://www.docker.com

[20] Vitalik Buterin. 2014. Slasher: A Punitive Proof-of-Stake Algorithm. (January 2014).

[21] Protocol Labs, 2018. Filecoin: A Decentralized Storage Network. https://filecoin.io/filecoin.pdf

[22] block.one, 2018. EOS.IO Technical White Paper v2. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[23] ethereum, 2017. A Next-Generation Smart Contract and Decentralized Application Platform https://github.com/ethereum/wiki/wiki/White-Paper

[24] Colored coins whitepaper, https://docs.google.com/a/buterin.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit

[25] Secure property titles with owner authority: https://nakamotoinstitute.org/secure-property-titles/

[26] Mastercoin whitepaper: https://github.com/mastercoin-MSC/spec

[27] Apache Spark. Unified analytics engine for large-scale data processing. https://spark.apache.org/

[28] Apache Hadoop. Reliable, scalable, distributed computing. http://hadoop.apache.org/

[29] Apache Kafka, distributed streaming platform. https://kafka.apache.org

[30] Malewicz, Grzegorz, et al. "Pregel: a system for large-scale graph processing." Proceedings of the 2010 ACM SIGMOD International Conference on Management of data. ACM, 2010.

Inasset GmbH domiciled in Niddatal, Germany, intends to conduct a private and a public fundraiser for the BigTangle platform and the creation of a global market and a global ecosystem with maximum efficiency as further described the following and the BigTangle whitepaper also available on:

https://bigtangle.net/bigtangle.pdf

Intrinsic Value

Everybody loves security, trustlessness and decentralization in payment systems.
The cryptocurrency community has worked very hard on blockchain technologies in the past 10 years. However, it turns out that conventional blockchains cannot adequately solve current real world problems:

- As a payment system, we expect that the solution must be equal to or better than Paypal, Visa and Alipay in terms of scalability and cost-performance.
- As a decentralized market and exchanges, we expect the solution to be equal to or better than NASDAQ, the NY Exchange or Binance in terms of scalability and confirmation speed.
- As a decentralized supply chain management system, we expect that the solution is usable on a global scale.
- As a decentralized E-Commerce solution, we expect that the solution must be equal to or better than Amazon and Alibaba by eliminating fees and centralization overhead.
- Only a solution with a parallelizable architecture and an implementation based on Big Data technology can achieve all of the aforementioned properties at the same time. Without sufficient scalability and cost-performance, a cryptocurrency network cannot achieve ubiquity and become standard.

This is where BigTangle comes into play.

BigTangle

A scalable revolution of blockchains

BigTangle is a cryptocurrency network extending directed acyclic graph architectures with Markov Chain Monte Carlo (MCMC) as a consensus algorithm and distributed Proof-of-Work.

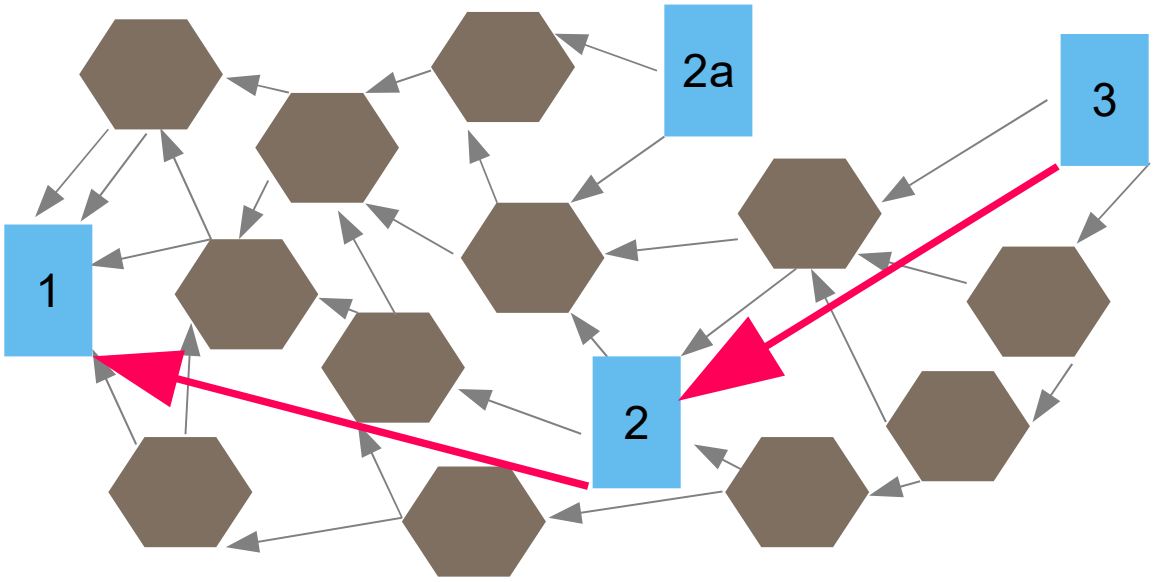
Through the use of industry standard big data technology in conjunction with the parallelizable architecture, BigTangle is a successor to conventional blockchains in the sense that it generalizes existing blockchain and smart contract architectures and makes them usable on a global scale.

Because of this and the unique design simplified pictured below, BigTangle has the potential to exist as the only platform of its kind comparable to the Internet.

BigTangle focuses on economically important key use cases. Custom token issuances, market exchanges, mining and smart contracts are supported.

To fully understand the BigTangle, it is worth it to read this whitepaper and referenced papers for technical details and mathematical proof. In simple terms, BigTangle is very similar to family trees with MCMC as natural selection process. The application is build on microservices and is very easy for use. You can test the application and inspect the source code.

Maximum security, decentralization, scalability by integration into a genealogical tree



Block with Transactions. Transactions are usually independent except for double spends. The MCMC consensus algorithm performs the selection process to solve conflicts.

Mining Reward Blocks are blocks with coinbase transactions only. Mining reward block must be in a chain over the Tangle. In the example above, blocks 1, 2 and 3 are such a chain. Let blocks 2 and 2a be in conflict. The MCMC consensus algorithm will solve this conflict by (in this case) having selected block 2 due to higher rating.

A scalable revolution of blockchains

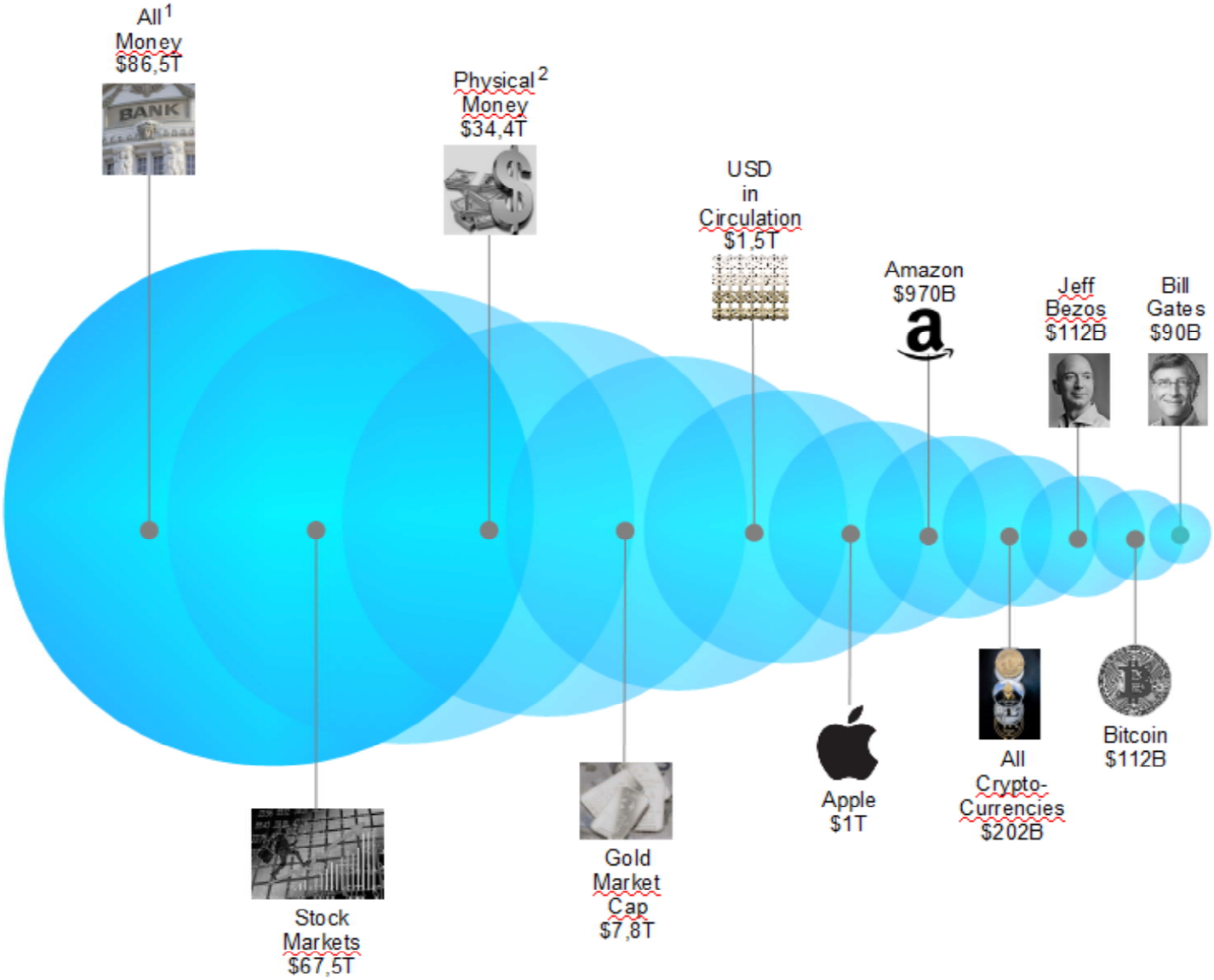
Key Features:
Ease of Use, Completely Feeless, Real-Time Transaction Confirmation, Infinite Scalability, Smart Contracts, Permissionless, Trustless, Decentralized App, Distributed Proof of Work and Quantum Security.

Power Consumption:
BigTangle is inherently a client and server architecture. There is no need for Pools, since the PoW-Mining is of low variance (almost all of the blocks are rewarded) and significantly reduces the need for pooling, while conventional blockchains exhibit a winner-takes-it-all reward scheme. The BigTangle requires the same power consumption as Bitcoin as any systems based on PoW.

However, comparing the transactions per seconds (TPS), e.g. 10 TPS in Bitcoin or 200 TPS in Ethereum, BigTangle with 10 server nodes in our clusters can achieve 1 Million TPS with the same power consumption. Big Data and blockchain parallelization are the only solution to get significant TPS at affordable costs.

Keep in mind that replacing other technical processes with the BigTangle network will also reduce total power consumption.

The Market for All Transaction Services



All figures are shown as of latest available data on September 2018

[1] All Money = money in any form including bank or other deposits as well as notes and coins

[2] Physical Money = money in forms that can be used as a medium of exchange, generally notes, coins, and certain balances held by Banks

Intranet and KYC

The BigTangle software can be deployed in private or other trusted environments, allowing one to run private, owned BigTangle networks with different rule sets.

These BigTangle networks are arranged in a hierarchy, i.e. they possess a parent Tangle such as the Mainnet between which a transfer of values is facilitated. For this purpose, each new Tangle has its own interface accounts (addresses) possessed by the private intranet operator from which it is possible to transfer funds into the parent Tangle and vice versa.

A user interested in transferring funds from the parent Tangle into one of its registered child Tangles can transfer tokens to one of the child Tangle's interface accounts, at which point they are either accepted into the child Tangle or returned by the trusted intranet owner.

Inside of such intranets, consensus protocol, transparency, permissiveness and other rules are set by the trusted intranet owner. Transfers of value can be performed internally as it is pleased. For example, in a work agency intranet it would be possible for clients to pay values to work forces in private and in arbitration of the owning work agency.

In general, enterprises and governments can deploy the software internally and e.g. do KYC (Know Your Customer) as well as privacy protection while remaining compatible with BigTangle's Mainnet.

This allows BigTangle to offer a holistic and flexible approach to value management, enabling privacy, transparency and accountability wherever needed by banks, stock exchanges or enterprises.

Ecosystem: Gold Digital Currency

BigTangle is “THE” technology to build market and exchange applications for value objects and their transferral. The key for BigTangle's success is to establish an economic system.

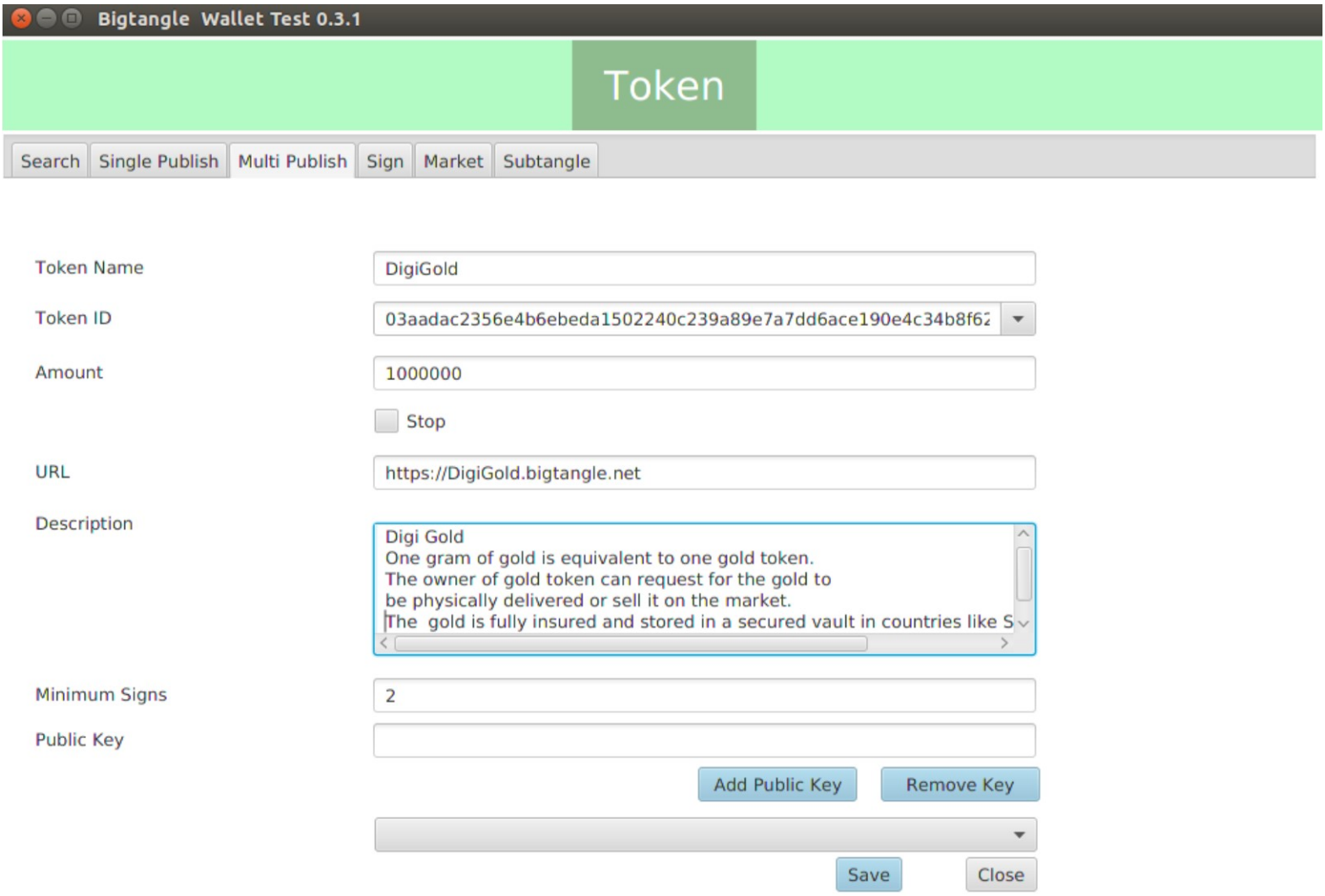
BigTangle is the best platform to build e.g. a gold-backed token. More and more investors are now interested in gold based tokens, which is further encouraging countries around the world to issue their very own gold-backed cryptocurrencies. For instance, one gram of gold is equivalent to one gold token.

The owner of gold token can request for the gold to be physically delivered or sell it on the market. The gold is fully insured and stored in a secured vault in countries like Swiss or Singapore. The BigTangle platform enables the gold token as base payment unit.

The token issuance protocol in BigTangle can be used to issue gold-backed tokens. Users must trust the backer of the token, but exchange transactions can then feasibly be processed trustlessly within seconds on a global scale.

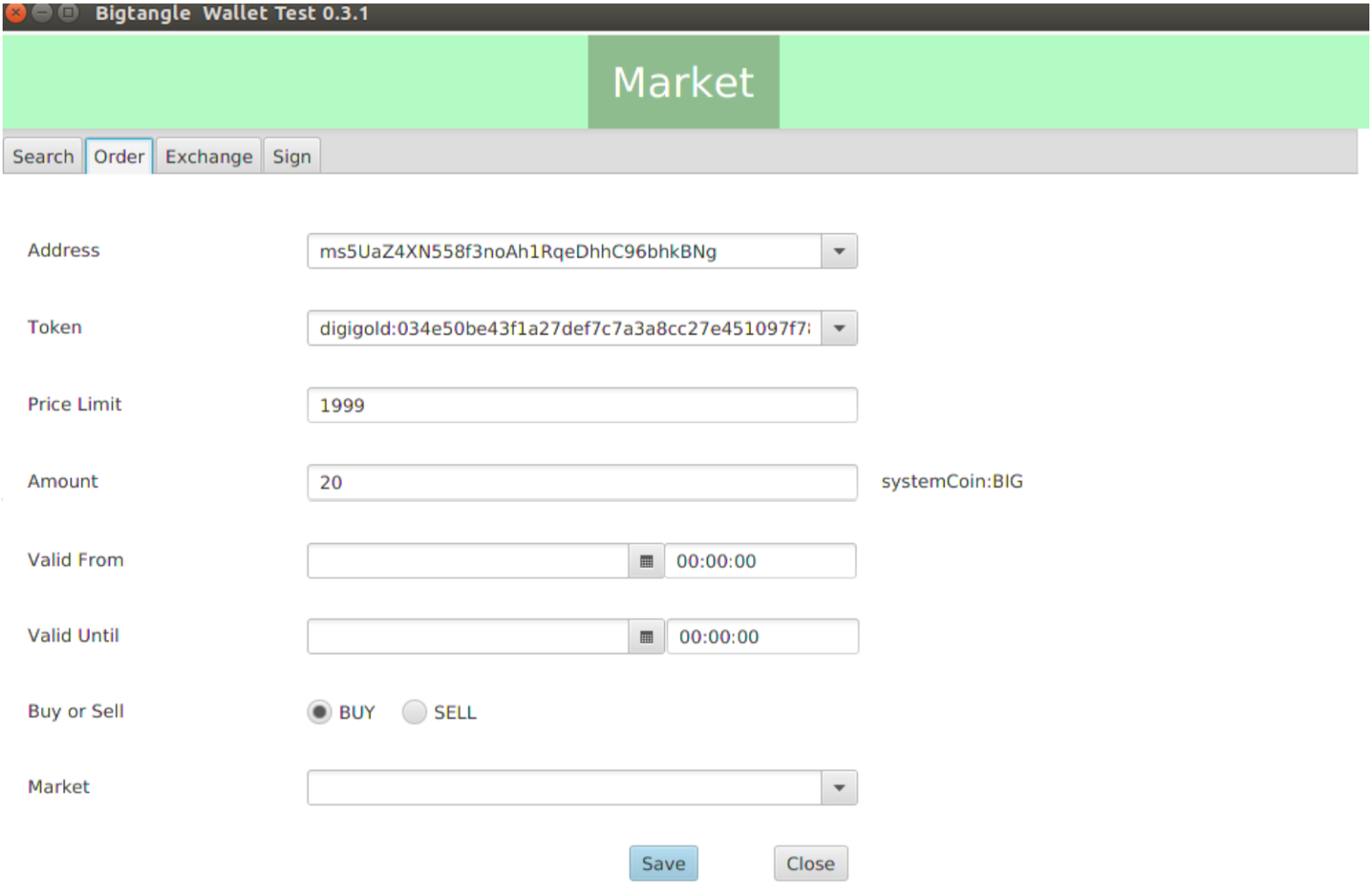
Economic System: Gold Digital Currency

(one exampel)



Market and Exchange

BigTangle has a built-in decentralized OTC market and exchange. All tokens can be traded with low latency and high scalability without any fees. The gold-backed tokens can be traded and booked very easy.



Economics

BigTangle is “THE” technology to build market and exchange applications for value objects and their transferral. Analogous to the Internet, eventually there will only be one such public internet-of-value.

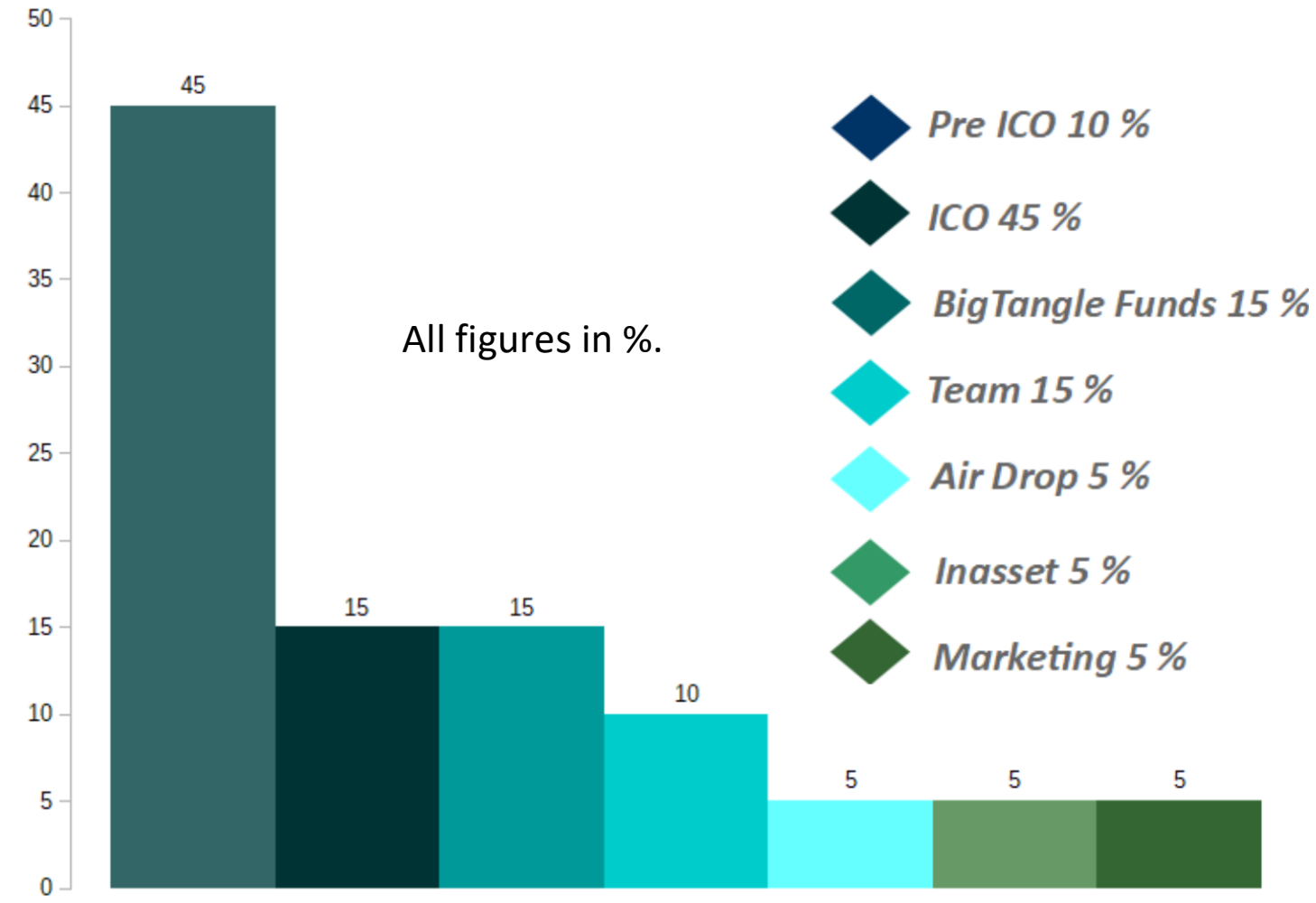
Using BigTangle, we can not only use a public internet-of-value, but also run Intranets in permissioned environments. After establishing a market economy, the BIG tokens shall be the singular payment method for all services and achieve a market capital of perhaps billions to trillions of USDs.

An investment return cannot be projected into the future.
For the famous Bitcoin history, refer to e.g.
https://en.wikipedia.org/wiki/History_of_bitcoin
This historical return on investment shows that the early Bitcoin investor invested 30 USD in 2011 and got 1 million USD in 2018.

Economics

Name of token:	BIG
Total initial offering:	1 trillion BIG (100 %)
Hard Cap:	open
ICO:	450 billion BIG (45 %)
Issue value:	open
Issue period:	15.11.18 - 15.3.2019
Settlement platform:	Ethereum ERC20
Accepted currencies:	ETH
Token supply per 0.2 ETH	1 million BIG
Mining Rewards p.a.:	1 billion as Basis + 2% p.a.

Distribution of BIG Token



Comparison with other cryptocurrencies

BigTangle is a successor to Bitcoin and Ethereum with blockchains as a platform.

BigTangle inherits all functionalities provided by Bitcoin and Ethereum. That are the special cases of BigTangle. The multidimensional BigTangle can be reduced to a blockchain by disallowing multiple block predecessors. The implementation of BigTangle shares a common base with Bitcoin, UTXOs, Script stack language and ECKeys.

The main problems of blockchains are low confirmation speed and scalability. The reason for this is the mixing of coinbase (mining rewards) and user transactions in one block, even though user transactions are highly parallelizable due to their independence from each other.

Indeed, the mining rewards must be a chain to allow for reward and difficulty adjustments as well as ensure a game-theoretically stable consensus. Here, classical blockchains use the simplest consensus algorithms: the longest blockchain wins and chains are mutually exclusive to each other.

Instead, BigTangle splits user transaction blocks from mining rewards and allows parallel conflict-free user transaction blocks to be unified in the consensus. To achieve this, BigTangle allows blocks to have two predecessors and uses the MCMC algorithm to rate and build new blocks, thereby establishing consensus without forcing parallel blockchains to be mutually exclusive.

BigTangle therefore generalizes existing blockchain and smart contract architectures and makes them usable on a global scale.

Comparison with other cryptocurrencies

BigTangle is a successor to Bitcoin and Ethereum with blockchains in regards to scalability, finality and decentralization.

Scalability:

1) BigTangle is a cryptocurrency network extending directed acyclic graph architectures with Markov Chain Monte Carlo (MCMC) as a consensus algorithm, that allows for blocks created in parallel to be unified later.

2) BigTangle is implemented with Big Data technologies: Kafka, Spark and Hbase.

In our cluster with 5 server nodes, more than 1 million transactions per seconds (TPS) can be achieved. Big Data and blockchain paralllelization is the only solution to get significant TPS at affordable costs.

Finality and Confirmation:
Assume that the network is synchronous, then BigTangle can achieve confirmation for finality in real time. MCMC ensures that when the network hash power has voted on a transaction, it will continue to stay in the consensus with extremely high probability. Bigtangle is a client and server architecture and enables the clients to make transactions and check balances on different servers.

Comparison with other cryptocurrencies

BigTangle is a successor to Bitcoin and Ethereum with blockchains in regards to functionality.

BigTangle natively implements a protocol for self-issuing custom tokens. Users can issue custom tokens and use them on BigTangle to serve their needs.

BigTangle implements container technology for smart contracts written in many computer languages, e.g. Ethereum VM.

BigTangle realizes a variety of economically important key use-cases: Beyond the decentralization of payment processing, the network can be used as a base service layer for the decentralization of markets in general, transfer and ownership management, authenticity proofs for assets of any kind or supply chains and ownership management.

As a protocol for the internet of value, The BigTangle software can be deployed in private or other permissioned environments, allowing one to run private, owned BigTangle networks with different rule sets. BigTangle defines a protocol and interface for value transfers from private BigTangles to the public or other private BigTangles and vice versa.

Protection of Investment

BigTangle's source code must be published openly on GitHub. However, the source code will be copyright protected. The BigTangle team is currently applying for patents for key technology components of BigTangle. This will ensure that the stakeholders of BIG Tokens will not see viable competitors before the building of an economy in BigTangle is finished.

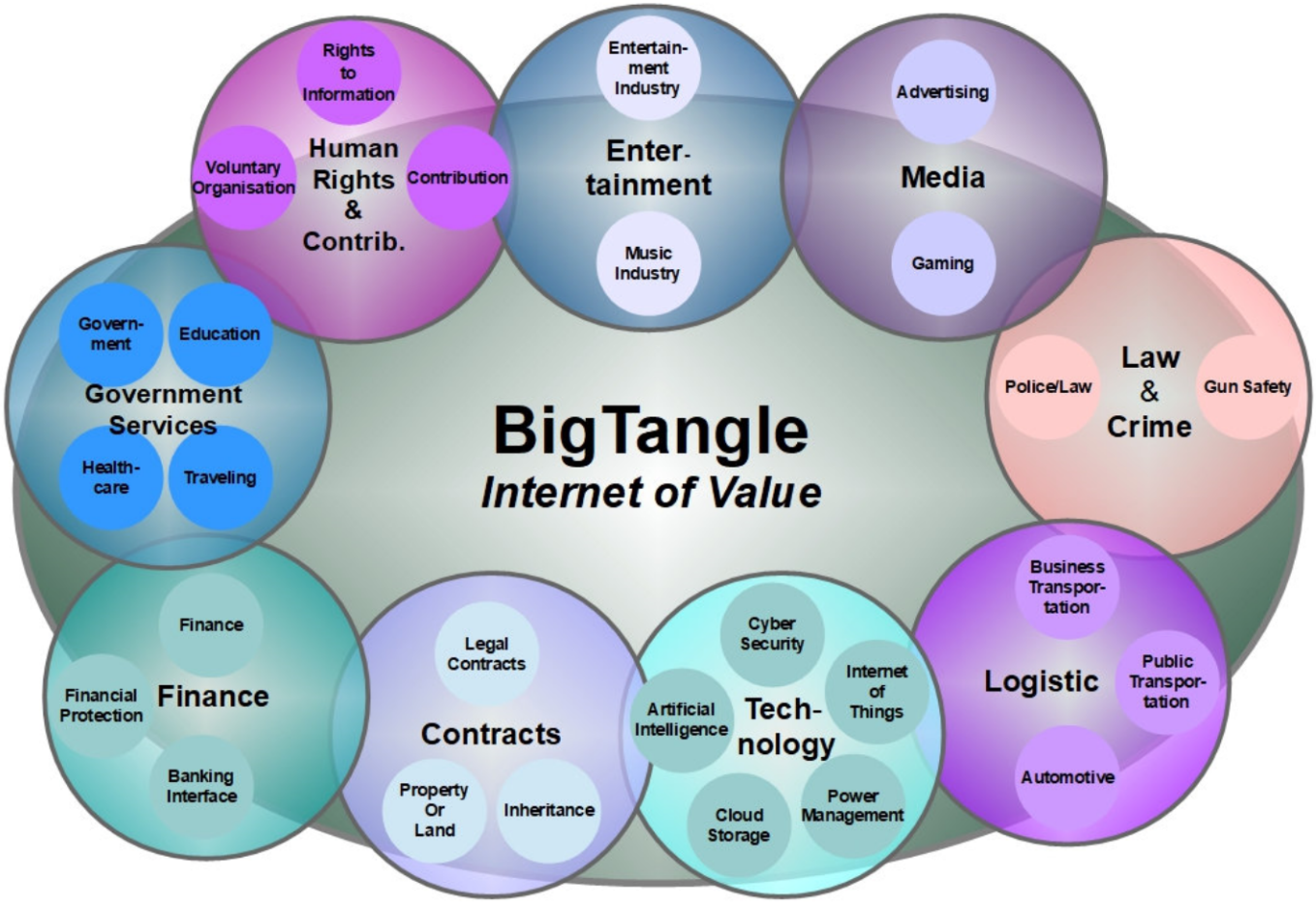
In two years, it is expected that the source code will be open source and the patents will be removed. The copyright and patent can forbid any forks of the BigTangle system and thereby protect investments.

As per date September 2018, the software development of BigTangle is 80% finished. There is a running testnet with 2 clusters operating interconnected. The cluster with name bigtangle.org is operated in a cloud environment in China and bigtangle.de is operated in Germany. The team will operate MainNet nodes.

BigTangle is initially funded by Inasset GmbH in Germany and Yuanyun in China.

Protocol for the Internet of Value

BigTangle triggers enormous synergies in all areas



Risks

Supervision:
BigTangle has a unique technology able to work together with central banks. It enables the issuance of Fiat money by design. However, crypto-assets have been supervised by many national regulatory agencies. Thus, BIG may be forbidden to trade or hold in some countries.

Building the market:
The key for BigTangle's success is to establish a market economy where users can transfer all kinds of values via a single public instance of the BigTangle network.

Other risks:
There are other general risks related to BigTangle: software weaknesses, vulnerabilities or bugs.

Please note: This is the description of the functionalities and use cases of BigTangle “The Revolution in Blockchain Technology”.
It does not include the solicitation of any neither type of investment.

Application of funds

Completion of the first applications	5 %
Implementation planned applications	7 %
Marketing	75 %
Administrative costs	3 %
Network extension	6 %
Miscellaneous	4 %
Total	100 %

BigTangle

Outstanding expertise in all specialist areas

CEO
Dr. Jianjun Cui

30 years in development: Big Data, Web Application, Cloud Computing, Distributed Database and Bitcoin.

Finance + Communications
Dr. Pu Zhou

Marketing + Organization
Wolfgang Blumenthal

30 years Bank- and Insurance-Marketing, Venture Capital Marketing.

Business Analyst
Martin Drees

30 years in development: Distributed Application

Core Developer
Yang Liu

10 years in development: Web Application and Blockchain

Core Developer
Tao Jiang

20 years in development: Web Application and Cloud Computing

BigTangle

Outstanding expertise in all specialist areas

Core Developer
Kai Cui
3 years in development of Web Applications and Bitcoin

Core Developer
Maximilian Hensel
3 years in development: Web Applications

UI Developer
Maximilian Lowin
3 years in development of UI Applications

Core Developer
Xiao Mi
10 years in development: Web Application and Bitcoin

Core Developer
Dr. Xiaojin Wang
20 years in development: Data Analyst and Data Scientist

Business Analyst
Frank Lu
10 years in development: Kershner Trading Group Akuna Capital

Special experts on the advisory board

Advisor
Prof. Dr. Willi Freeden

Advisor
Dr. Mike Lee

Advisor
Max Zhang

BigTangle

Special thanks to Bitcoin contributors

Aaron Voisine, Adam Mackler, Alexander Lolis, Alex Taylor, Alon Muroch, Amichai Rothman, Andreas Schildbach, andrewtoth, Bennett Hoffman, Carlos Lopez-Came, Carsten Otto, Chris, cyberzac, Dave Collins, dexX7, Diego Basc, elbandi, eleetas, En-Ran Zhou,Erik Tierney, Fireduck, freak, Gary Rowe, Giannis Dzegoutanis, Glenn Marien, GreenAddress, gubatron, Harald Hoyer, Jakob Stuber, Jameson Lopp, Jarl Fransson, Jim Burton, Jiri Peinlich, Johnathan, Jonny Heggheim, Justas Dobiliauskas, Kalpesh Parmar, Ken Sedgwick, Kevin Greene, Kirill Vlasov, Kosta Korenkov, kushti, langerhans, Loco, Manfred Karrer, Marc-André Tremblay, Martin Zachrison, matija.mazi@gmail.com, Matt Bogosian, Matt Corallo, Michael Bell, Michael Bumann, Mike Hearn, Mike Rosseel, Miron Cuperman, monk, Mora Zyx, mruddy, ollekullberg, Oscar Guindzberg, Pavol Rusnak, peacekeeper, Peter Dettman, Peter Stockli, Peter Todd, Piotr Włodarek, Richard Green, Robin Owens, Ross Nicoll, Sean Gilligan, Sebastian Ortega, Simon de la Rouviere, Simon Vermeersch, Stephen Reed, troggy, Tyler Houlihan, Willem Noort, Will Shackleton, Wojciech Langiewicz, Xiaofeng Guo, Ximo Guanter

Roadmap

Q3 2018

Start of internal testnet,
Going public and building community,
PRE-ICO: up to 10% BIG
are prepared for initial investors

Q4 2018

Simulation tests: Running test agents for automated tests with large numbers of clients. frequent updates for test clients and server nodes Performance, load and attack tests, GraphX implementation

Late Q4 2018

Release of Testnet with GraphX implementation.
Source will be made available in Github.
Public ICO for BIG on Ethereum is started.

Q1 2019

Production Test: Production software release for testing in Testnet

Late Q1 2019

Mainnet launch

References

Website
https://bigtangle.net

Whitepaper
https://bigtangle.net/bigtangle.pdf

Telegram
@bigtanglenet

Email
info@bigtangle.net
sale@bigtangle.net

BIG Token Creation, BIG Project Creation and Crowd Contribution Conditions: Explanatory Note & Governance Terms

Inasset GmbH ("Company") domiciled in Niddatal, Germany, intends to conduct a smart-contract based public fundraiser for the development of the BigTangle platform (the "Platform") and the creation of a global ecosystem with a high level of scalability and decentralization (together, the "Project") as further described in the BigTangle whitepaper (the "Whitepaper") available on https://bigtangle.net/bigtangle.pdf, amended from time to time, at the Company's sole discretion. These Governance Terms (together, the "Terms"), which may be amended from time to time at the Company's sole discretion, govern the creation and allocation of the Company's cryptographic tokens ("BIG Tokens") by one or several smart contract software codes (together, the "Smart Contract System") created by the Company and operating on the Ethereum blockchain as well as the contribution by third party individuals and entities (each a "User") to such Smart Contract System regardless of whether the contribution was made directly to the Smart Contract System or via third parties.

The Crowd Contribution ("Public Sale") is intended to commence on the 15th of November 2018. These Terms may, at the Company's sole discretion, be amended from time to time.

1. Crowd Contribution Principles

1.1. By transferring Ether ("ETH") to the Smart Contract System, creating BIG Tokens, and by accepting such BIG Tokens, the User understands and accepts that he/she makes a contribution into a Smart Contract System ("Contribution") for the development of the Project as further described in the Whitepaper. The information contained in the Whitepaper and on https://bigtangle.net are of descriptive nature only, are not binding and do not form part of the Terms as set forth hereinafter.

1.2. The User understands and accepts that while the individuals and entities assigned to this task, including the Company, will make reasonable efforts to develop and complete the Project, it is possible that such development may fail and User's BIG Tokens become useless and/or valueless due to technical, commercial, regulatory or any other reasons (see also Section 4 regarding Risks). The User is aware that the Project and the Smart Contract System are still under development and that – in particular due to regulatory reasons – its functionality may undergo substantial changes and modifications throughout the future development process.

1.3. The User understands and accepts that depending on the popularity of the Crowd Contribution, it cannot be guaranteed that the User's ETH transferred to the Smart Contract System are included in the Crowd Contribution, and that the User finally receives BIG Tokens. No certain allocation of BIG Tokens is guaranteed.

1.4. The User is also aware of the risk that even if all or parts of the Project are successfully developed and released in full or in parts, due to a lack of public interest, the Project could be fully or partially abandoned, remain commercially unsuccessful or be shut down for lack of interest, regulatory or other reasons. The User therefore understands and accepts that the transfer of ETH to the Smart Contract System, the creation of BIG Tokens by the Smart Contract System and/or and the acceptance of BIG Tokens carry significant financial, regulatory and/or reputational risks, including the complete loss of value of created BIG Tokens (if any), and attributed features of the Platform.

1.5. This document or any other materials provided by the Company or relating to the Project do not constitute a prospectus of any sort, is not a solicitation for investment and does not pertain in any way to an initial public offering or a share/equity offering and does not pertain in any way to an offering of securities in any jurisdiction. Neither this document nor any other materials have been (or will be) registered as a prospectus with any governmental authorities.

1.6. By transferring ETH to the Smart Contract System, creating BIG Tokens, by accepting such BIG Tokens or by any other act undertaken between the parties in connection with the contributions, no form of partnership, joint venture or any similar relationship between the Users and the Company and/or other individuals or entities involved with the deployment of the Smart Contract System and the setting up of the Project is created.

1.7. The User acknowledges and understands that the Company may at its discretion at any time change the name of the BIG Tokens and/or its symbol. The Company shall use all reasonable efforts to ensure that such change of name

and/or symbol will not adversely affect the rights of the User or the BIG Tokens held by the Users.

2. BIG Token Creation Function

2.1. BIG Tokens Functionality

2.1.1. BIG Tokens are only for use in connection with the Project and only constitute a transferable representation of attributed functions specified in the System.

2.1.2. Ownership of BIG Tokens carries no rights, express or implied, other than the limited right to use BIG Tokens as a means to enable usage of and interaction within the Platform, if and to the extent successfully completed and deployed.

2.2. No Ownership, Revenue or Governance Rights

2.2.1 User understands and accepts that BIG Tokens do not represent or constitute any ownership rights or stake, shares or security or equivalent rights nor any rights to receive future revenues, shares or any other form of participation or governance rights in or relating to the Project and/or Company. The BIG Tokens do not create or confer any enforceable contractual or other obligations against any party (including the Company, the BIG team members or other developers, auditors, contractors or founders associated with the Project, the Platform and/or the Company).

2.2.2. In addition, the User understands and accepts that he/she has no right to claim as holder of BIG Tokens any intellectual property rights, equity or equivalent rights or any other form of participation in or relating to the Project and/or the Company.

2.3. Contribution

2.3.1. Public Contribution Period: The Public Contribution period lasts from the 15. November 2018 till 15. March 2019 or until the Maximum Contribution Amount, as defined below, has been reached, whichever occurs earlier.

2.3.2. Maximum Contribution Amount: The maximum possible contribution amount for the Crowd Contribution ("Maximum Contribution Amount" or "Hard Cap") will be 90,000 ETH.

2.3.3. Accepted Funds: Contribution into the Smart Contract System during the Crowd Contribution will only be possible in ETH.

2.3.4. Total BIG Initial Supply and Mining Reward: The total supply of BIG Tokens will be 1,000,000,000,000 ("Total BIG Supply"). The mining reward is set to 2% of the above per annum.

2.3.5. Creation and Allocation of BIG Tokens: The creation and allocation of BIG Tokens by the Smart Contract System are initiated by the User sending an amount of ETH to the Smart Contract System, located on the Ethereum blockchain at the addresses set forth under Section 2.5., which triggers a smart contract operation. The Smart Contract System prepares the BIG Tokens in an amount corresponding to the user's effective contribution and allocates them to the User's wallet address from where the User's Contribution was sent from. The User, therefore, shall ensure to make his/her Contribution using an ETH address which the user controls and to which the Smart Contract System can send back BIG Tokens and/or ETH. The Company shall not be liable for any losses caused by the User attempting to contribute from an exchange platform (such as Bitfinex or Coinbase), smart contract, or other non-standard single access address.

2.3.6. Refund: The User understands and accepts that in general all Contributions are final and may not be reversed. A refund in specific cases is possible. The management of BIG decides about refunds. In general contributions that entitle a User to BIG Tokens are non- refundable. Contributions that do not entitle the User to BIG Tokens (e.g. due to the amount of contributions exceeding the Maximum Contribution Amount) will be automatically sent back to the User's wallet address from where the Contribution was sent from. Subject to the above, by contributing to the Project, the User acknowledges that he/she has no right to request a refund for any reason, and that he/she might not receive money or other compensation for any ETH that is not used or remains unused.

2.3.7. Assurance to use the original Smart Contract: Only the Smart Contract(s) existing at the addresses set forth under Section 2.5. will issue BIG Tokens during the Contribution Period. To the extent that any third-party website, service or smart-contract offers BIG Tokens during the Contribution Period or facilitates the allocation or transfer of BIG Tokens in any way during the Contribution Period, the User understands and accepts that such third-party websites or services are not authorized by the Company and have no relationship in any way with the Project.

2.3.8. Transferability of BIG Tokens during and after the Contribution Period: The BIG Tokens are transferable during the Contribution Period.

2.4. Representation and Warranties of User

2.4.1. By transferring ETH to the Smart Contract System, creating BIG Tokens, and/or by accepting BIG Tokens, the User represents and warrants that:

2.4.2. the User is not a citizen or resident of a country whose legislation conflicts with the present allocation of BIG Tokens and/or the Project in general;

2.4.3. the User is not a citizen or resident of the USA or Canada;

2.4.4. the User is not a resident of, citizen of or located in a geographic area that is subject to UN-, US-, EU-, Swiss or any other sovereign country's sanctions or embargoes;

2.4.5. any Funds used for the contribution are (a) good, clean, clear and are of non-criminal origin; (b) completely free and clear of any liens or encumbrances of any kind of any rights of third-party interests; and (c) have no origins that may be connected to any breach of money laundering regulations whatsoever, as defined in the jurisdiction of origin, or internationally;

2.4.6. the User is not being listed, or associated with any person or entity being listed, on any of the US Department of Commerce's Denied Persons or Entity List, the US Department of Treasury's Specially Designated Nationals or Blocked Persons Lists, the US Department of State's Debarred Parties List, the EU Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions or the Swiss SECO's Overall List of Sanctioned Individuals, Entities and Organizations;

2.4.7. all information provided within any KYC-procedure linked to his or her Contribution is true and accurate and that the User does not act on behalf of any third party;

2.4.8. the User has a deep understanding of the functionality, usage, storage, transmission mechanisms and intricacies associated with cryptographic tokens, like Bitcoin (BTC) and Ether (ETH), and blockchain-based software systems;

2.4.9. the User understands and accepts that there is no warranty or assurance that the network of miners will allocate the BIG Tokens to the Users as proposed by these Terms;

2.4.10. the User has carefully reviewed the code of the Smart Contract System located on the Ethereum blockchain at the addresses set forth under Section 2.5. and fully understands and accepts the functions implemented therein;

2.4.11. the User is legally permitted to (financially) support the development of the Project, as well as create and obtain BIG Tokens in the User's jurisdiction;

2.4.12. User will use a wallet or wallet service provider that technically supports BIG Tokens;

2.4.13. User understands and accepts that contributing ETH from a wallet or wallet service provider that does not technically support BIG Tokens may have the result that User will not gain access to his BIG Tokens;

2.4.14. the User is legally permitted to receive software and contributing to the Smart Contract System for the development of the Project;

2.4.15. the User is of a sufficient age to legally create and obtain BIG Tokens;

2.4.16. the User will take sole responsibility for any restrictions and risks associated with the creation of BIG Tokens by the Smart Contract System;

2.4.17 the User is not supporting the development of the Project to obtain BIG Tokens for the purpose of speculative investment;

2.4.18. the User is not obtaining or using BIG Tokens for any illegal purposes;

2.4.19. the User is receiving the functionality of the BIG Tokens issued by the Smart Contract System (and triggered by the Company) primarily to support the development, testing, deployment and operation of the Project, being aware of the commercial risks associated with the development of the Project;

2.4.20. the User understands that participation on the contribution does not involve the purchase of shares, securities exchangeable into shares or any equivalent in any existing or future public or private company, corporation, or other entity in any jurisdiction;

2.4.21. the User understands that submitting ETH to the Smart Contract System, creating BIG Tokens, accepting BIG Tokens and the development of the Project carries significant financial, regulatory, and reputational risks as further set forth in section 4;

2.4.22. the User understands that the User has no right against any other party to request any refund of ETH submitted to the Smart Contract System for the allocation and distribution of the BIG Tokens under any circumstance; and

2.4.23. the User understands that with regards to BIG Tokens, no market liquidity (including the existence of a marketplace where BIG Tokens can be transferred) may be guaranteed and the value of BIG Tokens (if any) may over time experience extreme volatility or depreciate in full.

2.5. Contribution Address and Control over Private Keys

2.5.1. As part of the Contribution process, the User must use his/her own account (address) on the Ethereum blockchain, with a private key or password associated to this address. Following the creation of BIG Tokens by the Smart Contract System, the BIG Tokens will be transferred to the User's address by the Smart Contract.

2.5.2. In order to receive the BIG Tokens, the User shall not use third party addresses of exchange platforms (e.g., Poloniex, Coinbase, Bitfinex, etc.). The User understands that the User must keep his/her password or private key safe and that the User may not share them with anybody. The User further understands that if his/her private key and/or password is lost or stolen, the BIG Tokens associated with the User's account (address) will be unrecoverable and will be permanently lost. Furthermore, the User understands that there is no recovery mechanism for lost keys and passwords, so no one will be able to help the User retrieve or reconstruct a lost password and private keys and provide the User with access to any lost BIG Tokens.

3. BIG Project Execution

3.1. The User understands and accepts that the development and execution of the Project will be assigned to the Company, by releasing the amount of contributed ETH by the Smart Contract System to the wallet of the Company. The Company has the right to engage subcontractors to perform the entire or partial development and execution of the Project.

3.2. The User understands and accepts that for the purpose of the development and execution of the Project, the Company receives the full amount of ETH transferred to the Smart Contract System during the Contribution Period. This amount covers expenses, charges and other costs that may arise by the Company and/or its subcontractors as part of the development and execution of the Project. It remains at the Company sole discretion to decide how to allocate the funds in order to develop and execute the Project.

3.3. The User understands and accepts that the creation of BIG Tokens does not involve the purchase of shares or any equivalent in any existing or future public or private company, corporation or other entity in any jurisdiction. Thus, the User understands and accepts that he/she will have no influence over governance on the Project and that the Company has the right to assign the execution of the Project and the development of the Platform to a third party.

3.4. The User understands and accepts that the Project will need to go through substantial development works as part of which it may become subject of significant conceptual, technical and commercial changes before release. The User understands and accepts that as part of the development, an upgrade of the BIG Tokens may be required (a so-called hard-fork of the BIG Tokens), and that, if the User decides not to participate in such upgrade, he/she/it may no longer use their BIG Tokens and that any non-upgraded BIG Tokens may lose their functionality in full.

3.5. The User understands and accepts that smart contract technology is still in an early development stage and its application of experimental nature which carries significant operational, technological, financial, regulatory and

reputational risks. Accordingly, the User understands and accepts that no warranty is given, including direct or indirect warranties that the Smart Contract System and the BIG Tokens are fit for a particular purpose or do not contain any weaknesses, vulnerabilities or bugs which could cause, inter alia, the complete loss of ETH, other (financial) support of the Project and/or BIG Tokens.

4. Risks

4.1. The User understands and accepts the risks in connection with making a Contribution to the Project and/or transferring ETH to the Smart Contract System and creating BIG Tokens as exemplary set forth above and hereinafter In particular, but not concluding, the User understands the inherent risks listed hereinafter:

4.2. Risk of Software Weaknesses: The User understands and accepts, the underlying software application and software platform is still in an early development stage and unproven. The User understands and accepts that there is no warranty that the process for creating BIG Tokens will be uninterrupted or error-free and acknowledges that there is an inherent risk that the software could contain weaknesses, vulnerabilities or bugs.
The User understands and accepts that the underlying protocols and/or any other software involved may either delay and/or not execute a Contribution due to the overall Contribution volume, mining attacks and/or similar events.

4.3. Regulatory Risk: The User understands and accepts that the technology allows new forms of interaction and that it is possible that certain jurisdictions will apply existing regulations on, or introduce new regulations.

4.4. Risk of Abandonment / Lack of Success: The User understands and accepts that the creation of the BIG Tokens and the development of the Project may be abandoned for a number of reasons, including lack of interest from the public, lack of funding, lack of commercial success or prospects. The User therefore understands that there is no assurance that, even if the Project is partially or fully developed and launched, the User will receive any benefits through the BIG Tokens held by him.

4.5. Risk of Loss of Private Key: The User understands and accepts that BIG Tokens can only be accessed by using a BigTangle wallet with a combination of User’s account information (address) and private key or password. The User understands and accepts that if his private key or password gets lost or stolen, the BIG Tokens associated with the User's account (address) will be unrecoverable and will be permanently lost.

4.6. Third-party Risk: The Company may use third parties to manage and operate the contribution processes. The Company has no visibility into, or possibility to control the software or mechanisms used by such third parties, and cannot verify or guarantee the proper functionality of the third-party software or operations.

4.7. Risk of Theft: The User understands and accepts that the Smart Contract System concept, the underlying software application and software platform may be exposed to attacks by hackers or other individuals that could result in theft or loss of BIG Tokens, other (financial) support of the Project, or ETH, impacting the ability to develop the Project.

4.8. Risk of Mining Attacks: The User understands and accepts that, as with other cryptocurrencies, the blockchain used for the Smart Contract System is susceptible to attacks, including but not limited to denial of service attacks, exploits of consensus nodes, and byzantine attacks on the consensus nodes. Any successful attacks present a risk to the Smart Contract System, expected proper execution and sequencing of BIG Tokens transactions, and expected proper execution and sequencing of contract computations.

4.9. Risk of Incompatible Wallet Service: The User understands and accepts that the wallet used for the Contribution has to be technically compatible with the BIG Tokens. The failure to assure this may have the result that User will not gain access to his/her BIG Tokens.

4.10. Risk of Depreciation: The User understands and accepts that with regard to BIG Tokens no market liquidity may be guaranteed and that the value of BIG Tokens over time may experience extreme volatility or depreciate in full.

5. Taxation

5.1. The User bears the sole responsibility to determine if his/her Contribution to the Project and/or for the development of the Project, the transfer of ETH to the Smart Contract System, the creation, acceptance, ownership or use of BIG Tokens, the potential appreciation or depreciation in the value of BIG Tokens over time (if any), the allocation of BIG Tokens and/or any other actions or transactions related to the Project has tax implications for the User.

5.2. By creating, holding, or using BIG Tokens, and to the extent permitted by law, the User agrees not to hold any third party (including developers, auditors, contractors or founders) liable for any tax liability associated with or arising from the creation, ownership or use of BIG Tokens or any other action or transaction related to the Project.

6. No Warranty

The User understands and expressly accepts that there is no warranty whatsoever on BIG Tokens, the Smart Contract System and/or the success of the Project, expressed or implied, to the extent permitted by law, and that the Smart Contract System is used and BIG Tokens are created and obtained at the sole risk of the User on an “as is” and “under development” basis and without, to the extent permitted by law, any warranties of any kind, including, but not limited to, warranties of title or implied warranties of merchantability or fitness for a particular purpose.

7. No Liability

7.1. The User acknowledges and agrees that, to the extent permitted by any applicable law, the User will not hold any developers, auditors, contractors or founders of the BIG Tokens, the Smart Contract System and/or the Company liable for any and all damages or injury whatsoever caused by or related to the use of, or the inability to use, BIG Tokens or the Smart Contract System under any cause or action whatsoever of any kind in any jurisdiction, including, without limitation, actions for breach of warranty, breach of contract or tort (including negligence) and that developers, auditors contractors or founders of the Smart Contract System, the Company and/or the Project shall not be liable for any indirect, incidental, special, exemplary or consequential damages, including for loss of profits, goodwill or data, in any way whatsoever arising out of the use of, or the inability to use of the Smart Contract System, the Platform and/or the BIG Tokens.

7.2. The User further specifically acknowledges that developers, auditors, contractors or founders of the Platform, Smart Contract System and/or the Project are not liable, and the User agrees not to hold them liable for the conduct of third parties, including other creators of the Company, and that the risk of creating, holding and using BIG Tokens rests entirely with the User.

7.3. By creating, accepting, holding or using BIG Tokens, and to the extent permitted by law, the User agrees not to hold any third party (including developers, auditors, contractors or founders) liable for any regulatory implications or liability associated with or arising from the creation, allocation, ownership or use of BIG Tokens or any other actions or transactions related to the Project.

8. Miscellaneous

8.1. The Smart Contract System is located in Germany. Consequently, the BIG Tokens creation and allocation and the assignment of the development and execution of the Project to the Company are considered to be executed in Germany.

8.2. The User agrees that if any portion of these Terms is found illegal or unenforceable, in whole or in part, such provision shall, as to such jurisdiction, be ineffective solely to the extent of such determination of invalidity or unenforceability without affecting the validity or enforceability thereof in any other manner or jurisdiction and without affecting the remaining provisions of the Terms, which shall continue to be in full force and effect.

8.3. The Terms govern the creation, allocation, ownership and use of BIG Tokens and supersede any public statements about the launch of the BIG Tokens and/or the Smart Contract System made by anyone in the past, present and future.

8.4. The applicable law is German law. Any dispute arising out of or in connection with the creation of the BIG Tokens and the development and execution of the Project shall be finally settled by the ordinary courts of the registered domicile of the defendant.

8.5. To the fullest extent permitted by law, the User waives the right to participate in a class action lawsuit or a class-wide arbitration against the Company or any individual involved with the creation of the Project and/or BIG Tokens.