TERA PLATFORM

Yuriy Ivanov (Vtools)
01 June 2019
progr76@gmail.com
(draft ver: 0.36)
attention: the information in this document is outdated

If you see blue text below - it means this part is not read and may be incorrectly translated, and so we need the help of native English speakers...

CONTENT

Abstract

Tera is a decentralized application platform. This is akin to an operating system. Tera consists of a repository of programs and data storage integrated into the Internet. The mechanism for publishing programs and data on this platform is free from censorship. Money is blood in the economy and blockchain moves it blood.

Consider the following layers:

```
Hardware > Software > UI > Database > Centralized Network >
Decentralized Network
```

In the 21st century, everyone has a computing device like a computer, a laptop, a smartphone, a smart watch, and so on. In itself, such a device is useless for a person so it is always running a program that performs something useful. The result of the program is displayed in the user interface. Often,results are persisted in the device's data layer to be able to access them again. Even greater usefulness is achieved by allowing other users to access this data over a network. Thus, each successive increases the usefulness for the user.

To communicate with each other, devices are combined to into a network topology in which each such device is called a node. The easiest way to combine nodes into a network is to use a single coordinating server, but such a solution is centralized with corresponding unreliability due to a single point of failure. There are other solutions in which all devices are equal, have the same rank and priority and which we will call a decentralized network. It is important to understand that the decentralized network works as a whole; nodes communicate with one another throughout the network as a well-coordinated mechanism. To achieve this, there are special algorithms for interaction of nodes with each other, which we will call consensus. It can be: time consensus, delivery consensus, or data chain consensus.

Tera is the next generation of human-software interaction.

Introduction

Problems with Modern Blockchains

Low Speed. No Breakthrough (Rocket Science) Technology

Back in 2017, the main bottleneck of the blockchain was clear - it was its slow work. The situation has not changed in the duration since then. With the exception of centralized Blockchains (to which we refer Blockchains having a fixed number of nodes block producers, for example 21) no scalable solutions have appeared. The industry needs a technology that enables hundreds of millions of people around the world to work with it, and that uses dynamic scalability.

The lack of such technology leads to the stagnation of the industry and to the loss of capitalization of cryptocurrencies on exchanges.

DApps and Centralization

The term Dapp stands for decentralized application, but at present, it is applied incorrectly. It is called a program that interacts with a smart contract in the blockchain and is actually located on a centralized server. That part which is on the centralized server is key because without the server it is not possible to use. Such a DApp can only guarantee the preservation of the user's funds, since they are on the blockchain. This situation is due to the fact that the current blockchains do not provide hosting services in their platform. There is no such thing as a user interface on existing blockchains (with the exception of the Tera blockchain).

Integration with the Web

Blockchain remains too virtual for ordinary users to comprehend; they do not see it before their eyes. It is difficult to believe in something you have never seen. Adding visualization interfaces to the blockchain will allow users to see and start working with it right now. The real distribution of the blockchain will be helped by the simplicity of software development. To do this, the language of the smart contract should be as simple and as familiar as possible. You need to use a simple language and modern, common technologies (Javascript and HTML) to maximize the adoption rate through basic familiarity. Web programmers are the largest group of blockchain users the IT industry. They will be able to quickly create popular applications on the blockchain and make them as convenient as possible for all users to make use of dapps.

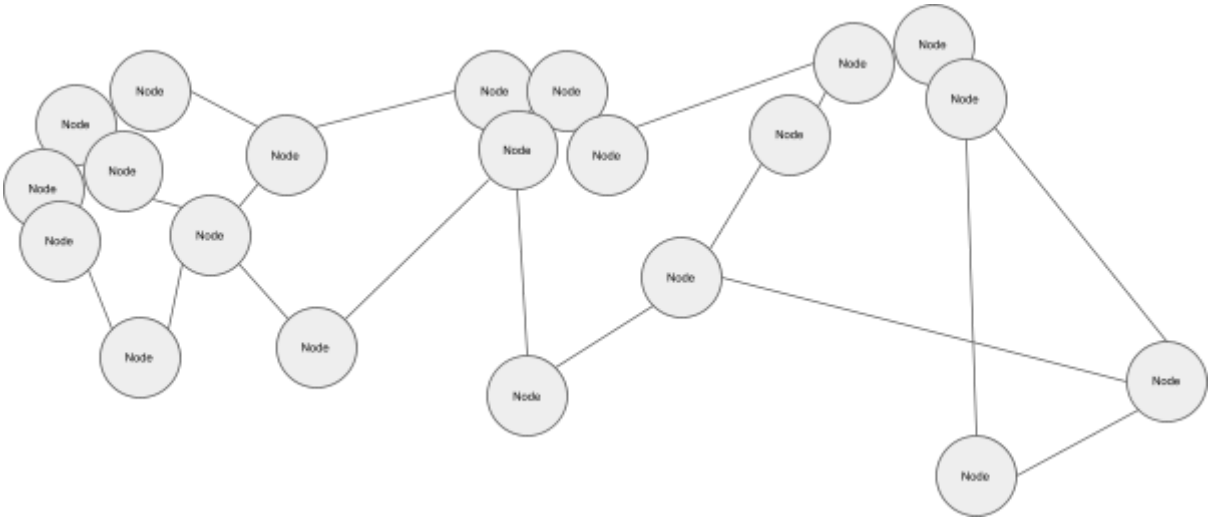
Implementation

Theoretical Aspects

To solve the problem of scaling, the classical approach to building a blockchain (for example, the one used in Bitcoin) is not suitable, a significant processing is required. Practically it is necessary to re-invent the blockchain. We proceed from the fact that the reader has already read the Bitcoin WhitePaper and fully understood its principle.

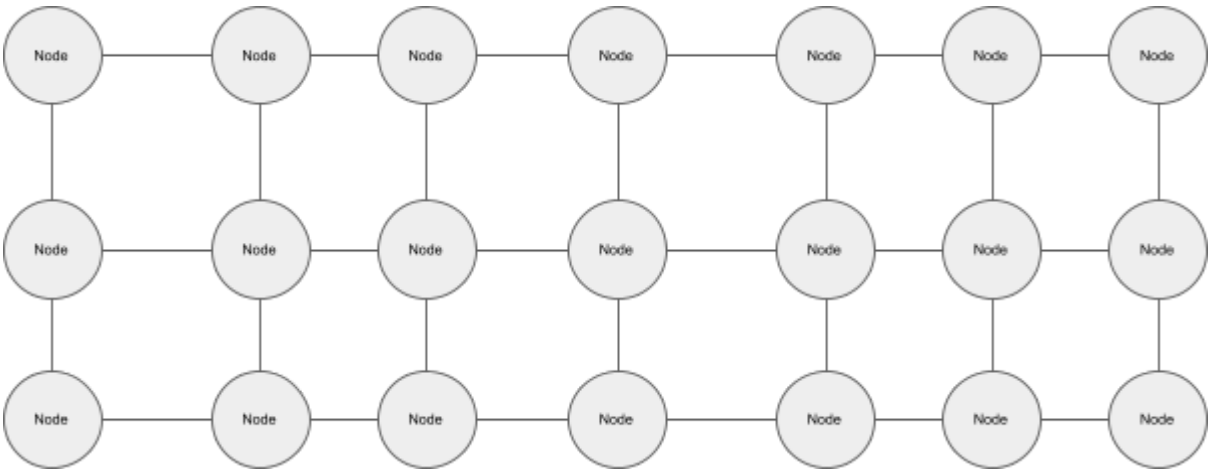
A Fast Routing Network

Traditional blockchains do not use the ordering of nodes with each other. They use the old **Gossip** protocol. The overall picture of the network looks randomized, like this:



This random organization of links does not guarantee fast delivery of blocks between all nodes.

So in TERA uses a special **Tera Protocol**, in which nodes organize themselves in an orderly connections form a multidimensional regular grid:



The blockchain takes no longer than 3 seconds to deliver data from the 1st node to the last one. Nodes form connections between themselves, which is based on the similarity of their ID. Each ID is a random variable with a length of 32 bytes and does not change during node operation. The number of connections with other nodes has a logarithmic dependence on the number of nodes in the network, thereby achieving a relatively constant time of transaction delivery. Thus, were the network to consist of 1 billion nodes, the delivery time between the nodes would still be no more than 100 milliseconds (ms), so the maximum time will be 30*100 ms = 3 seconds. The 100 ms delay time for delivery of transactions between nodes is the upper bound, but in practice, it is less than 100 ms because nodes with less mutual delay have connection priority.
In order to make successful connections more permanent, each node records statistics of successful exchanges with the node with which the contents of the blocks are exchanged. This statistic affects the connection priority.

Network Protocol

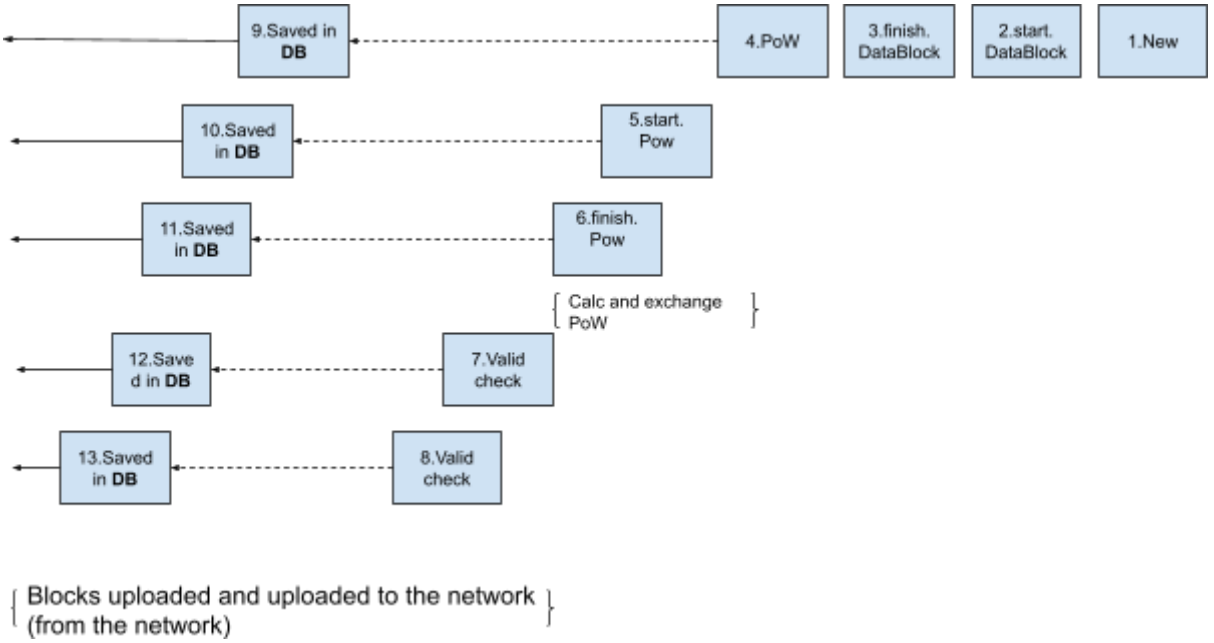
The transaction is sent by the user to N neighboring nodes (where N is from 5 to 16). The transaction is added to the newly formed block (the block of the current second). When the exchange stage comes, the transaction begins to move from one node to another, accumulating in the block. If a block contains more transactions than it can hold, then transactions with a large PoW are left - this is how DDOS protection is implemented. At the end of the block formation stage, the signature stage and the PoW block calculation (1 second) are performed, then the three-second stage of the leader block search with the maximum pow begins. The block gets added to the blockchain.

Conveyor Processing of Blocks

Blockchain: Forms blocks of times per second, but the time of confirmation of the block (i.e. the on-time of a block in the blockchain) is 8 seconds. In order to create blocks 8 times faster than the confirmation time, the pipeline processing of blocks is used. This can be thought of as 8 separate blockchains, with a formation period of 8 seconds. Each such blockchain is shifted relative to each other for one second. Thus, we create a block of the 1st blockchain for one second, a block of the 2nd blockchain for the next second, and so on up to the 8th blockchain. In order to connect these blockchains into one, they are glued together. In

traditional blockchains, the hash of the previous block is included in a single chain in the header of each block. In the Tera Blockchain, for these purposes, the hash of the previous block is calculated on the basis of several previous blocks of each of the 8 blockchains. At this stage, we get a logical binding of 8 chains into one.

Several blocks are processed in parallel, the order of processing depends on the current time (the current block):

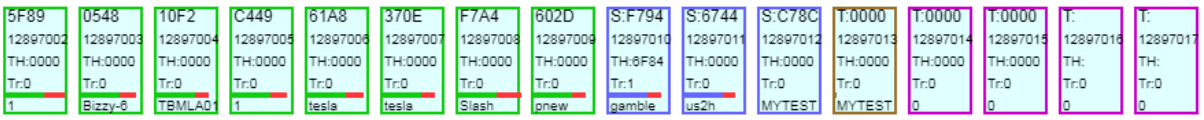


Timing:

1. New (current) block, loading transactions from MemPool, timer activation
2. The beginning of a synchronization unit (distributed unit of)
3. End of synchronization
4. Bundle data block with the previous blocks, the calculation of PoW
5. The search begins at the maximum PoW network
6. The end of the search max. PoW
7. Check the validity of the unit taking into account possible changes of the previous blocks due to download the new block chain with a large total PoW

From the diagram you can see that the block refers to the previous blocks but with a Delta of 8 blocks. Once determined valid and stored in the database, blocks from the 8th then participate in unloading in other nodes (similarly, they can be loaded from other nodes).

This is how blocks look in the Tera blockchain explorer page;



Separate layers: blockchain and cryptocurrency

We have separated the concept of blockchain and cryptocurrency. We have created two layers:

1. Blockchain layer
2. Cryptocurrency layer

What is blockchain: it is a computer network in which each node is equal, their number is unlimited, communication between is carried out through the organization of a single data chain, in which information is written block by block in the form of commands (transactions). In classical blockchains, only payment transactions are recorded in blocks, and it is not allowed to write to the transaction block, which is not valid (for example, does not have the correct digital signature or not enough money in the account or double spending, etc.). There is no cryptocurrency in the blockchain of the TERA platform, so it is allowed to record any information, the blockchain is used as a transport. Each record (hereinafter we will call them transactions) has its own strict numbering and is divided into blocks, blocks are connected to each other by means of an irreversible cryptographic hash function. On the first layer, the task of the blockchain is to ensure the same information in each node of the network. This problem is solved by the classic **PoW** consensus.

The interpretation of the correctness of the information lies on the following layers. On the second layer of support for cryptocurrencies - internal coins of **Tera**. Smart contracts are implemented on the same layer. The Tera coin is important to the network as it is used to motivate miners to maintain the network.
Since the first layer guarantees the same data, and since the program code on the second layer is the same on all nodes of the network, it is obvious that performing the same actions all nodes will have the same result: the same balances on user accounts, the same state of smart contracts. Thus, if these blocks contain invalid double-spending transactions, the validating layer will reject them equally on all network nodes.

Validation can be performed at another time and in another process without interfering with the blockchain. What's more is you can do it much faster due to the so-called batch processing (mass inspections) — we can group operations and to accelerate the work due to the smaller number of requests to the Database.

The Dependence of the Size of the Blockchain Database From User Settings

With large amounts of data that will inevitably occur at 1000 tps, new users should be able to quickly download the blockchain to validate it and start working with it. Therefore, the download order is changed - if it was previously from the beginning of the chain, it will now be downloaded from the end.

Loading information will depend on the user's settings - on the size of the disk memory that he has allocated for the blockchain. Depending on the size, the next download priority will be:

1. The chart of accounts
2. Block headers
3. The contents of blocks or transactions

How it will work:

1. For a super thin client: only part of the headers and a piece of the invoice table will be loaded.
2. For the average customer: the entire table of accounts and titles but only part of the content blocks
3. For the full client-all data (as it is done now)

Example:
The user allocates space for the blockchain on the disk, for example 12 GB
This disk space is divided into three parts:

- Regular block structure (starting from the end), for example 5 GB
- Other blocks that are not included in a regular structure but are required is stored on the node (determined by the DHT principle - i.e., the degree of similarity of the addresses of the nodes), for example 5 GB
- The last commonly used blocks, for example 2 GB

Security

We use the POW consensus to create an irreversible blockchain. At the moment, POW is the only decentralized consensus and it assumes that at least 51% of the owners of mining capacity are honest.

Protection from replay-attacks

The Tera blockchain uses PoW consensus. This allows all transactions to be arranged in sequential order. Transactions are also executed sequentially. When withdrawing from the account, the necessary amounts are checked. At the time of recordation, the counter "OperationID" is incremented. Each subsequent payment transaction must have the next "OperationID" number to prevent the same transaction from being applied multiple times.

Double Spending Protection

In the Bitcoin network, to protect the user against double spending, it is necessary to wait for at least 10 minutes, sometimes 1 hour.

In the Tera network, blocks are created every second, and the first confirmation time is 8 seconds, but if you want the same degree of reliability as in the Bitcoin network - you need to wait for the same duration. The duration of time you wait correlates to the degree of reliability. There is no magic here; in any PoW algorithm, you exchange time for reliability. In TERA, we have made a more flexible choice. You can wait 8 seconds, 1 minute, or 1 hour (if, for example, transferring sums worth millions of dollars).

Protection from DDOS Attacks

Limit on the number of transactions sent

Each transaction that is sent is verified on behalf of which account it was sent. This is done by checking the digital signature on the public key of the account. Users have a limit on the number of transactions within a certain time (for example, 1000 blocks), its value is floating - if the network is low, they can send more transactions. Implemented this through the transaction priority mechanism, transactions are sorted in order of priority, which depends on the total number of previously sent transactions, the greater it is - the lower the chances to get into the block. Thus, the accounts from which transactions are often sent begin to compete only with each other, and the accounts that are rarely sent - go out of turn.
If we assume that the attacker has created thousands of accounts and launched attacks by generating a large number of transactions in turn from each account, then from the second transaction they begin to compete with each other and the channel remains free for users who have not sent any transactions in the last 1000 seconds. At the same time, each subsequent transaction of the attacker reduces the effect of the attack, since it becomes lower and lower competitive for the right to be included in the block.

Pow

Each block has a limit of 130 KB; the average transaction size is 130 bytes, so an average of 1000 transactions per block is placed. Each transaction must have a PoW field, which records the work done to calculate the hash. This field is used to determine whether or not

this transaction is included in the block. It must be at least a certain value and must be sufficient to compete with other transactions. Only the first (approximately) 1000 transactions with the highest PoW values are included in the block.

Calculations:
The large capacity of the blockchain and the requirement for mandatory PoW execution in each transaction sent allows you to effectively organize DDOS protection with the following limits:

- The attacker has a processing power of 1,000 times the average user.
- The average network load is 50%, i.e. 500 transactions per second.

In this case, the attacker can send 1000 transactions per second. When you first send in the network will have 1,000 transaction and attacking 500 regular users, only 1500 transactions. The blockchain will accept only 1000 transactions, so 500 will be discarded (regular users and attackers will each lose one-third of their transactions). But at the same time, the average power of PoW transactions will be increased and, therefore, in the next block ordinary users will spend more computing time to send a transaction (i.e. twice as long). At the same time, the attacker will not be able to increase the power of PoW transaction calculation, because he initially works at the limit (100%) of capacity. As a result, the average power of the PoW transaction of an ordinary user will double and the ratio in the block between ordinary transactions and the attacker's transactions will be already 500 to 500. That is, all user transactions will be accepted.

From these arguments it can be seen that the smaller the workload of the blockchain, the more difficult it is to apply DDOS. As soon as the average load of the blockchain exceeds 50%, we will increase the upper threshold of transactions. At the moment, each miner’s node actually supports transaction processing using only one thread. Given that at the moment, multi-core processors is the norm, it will not be difficult to multiply the transaction processing performance of each node.

Defense against Sybil's attack

All nodes in the network are equal and anonymous. They are randomly connected to each other to form a multidimensional lattice for efficient data transmission. But it is possible to attack the sibyl, when the attacker creates a large number of nodes and tries to conduct malicious actions:
A “good” node differs from a “bad” node in that it follows a clear protocol. “Bad” node can:

- do not transmit information when needed
- transmit information when it is not needed
- transmit false information

The purpose of each node in the network correctly transmit information. The result of correct transmission is a successfully synchronized block, no orphan chains. This indicator is visible

a few seconds after the exchange and it is objective, because it is protected by the consensus of the pow block, so it can not be faked without having 51% of the capacity (but we always assume that 51% of the capacity in the network is honest).
Thus we have in the presence of a sufficiently good mechanism to determine whether adherence to the Protocol of the nod, with whom we exchange. Therefore, in order to “cement” successful connections, each node records for itself the statistics of successful exchanges with another node, with which the contents of the blocks are exchanged. This statistic affects the priority of forming links when creating a network by the type of multidimensional regular lattice.

Economic Stimulus of Miners

Miners perform complex calculations of the hash for a block to create the immutability of the blockchain. The reward for the found hash block provides the economic incentive to the miner. This reward is calculated as follows: one billionth (0.000000001) of the balance of the Unallocated amount of coins remaining multiplied by the hundredth part of the square of the logarithm of the miner (net) power. Initially, the total Unallocated amount was equal to 1 billion coins (the total issue of the tera), so over time the reward will fall, but this will be compensated by the real exchange rate on the exchanges, as well as the reverse replenishment of the Unallocated balance of coins due to paid transactions:

- 10 Tera - creating a new account for users out of the restrictive queue
- 100 Tera - creating a smart contract/DApp
- 10,000 Tera - creation of smart token (i.e. own currency)

Payment goes to the account 0 (i.e. back to the Unallocated balance for mining).
The price of the transaction will continue to change through the DAO mechanism of voting.

Practical Aspects

Specification

Consensus: PoW
Algorithm: Terahash (sha3 + Optimize RAM hashing)
Total supply: 1 Bln
Reward for block: one billionth of the remainder of undistributed amount of coins
Block size 350 KB
Premine: 5%
Development fund: 1% of the mining amount
Block generation time: 3 second
Block confirmation time: 8 seconds
Speed: from 1000 transactions per second
Commission: free of charge
Cryptography: sha3, secp256k1

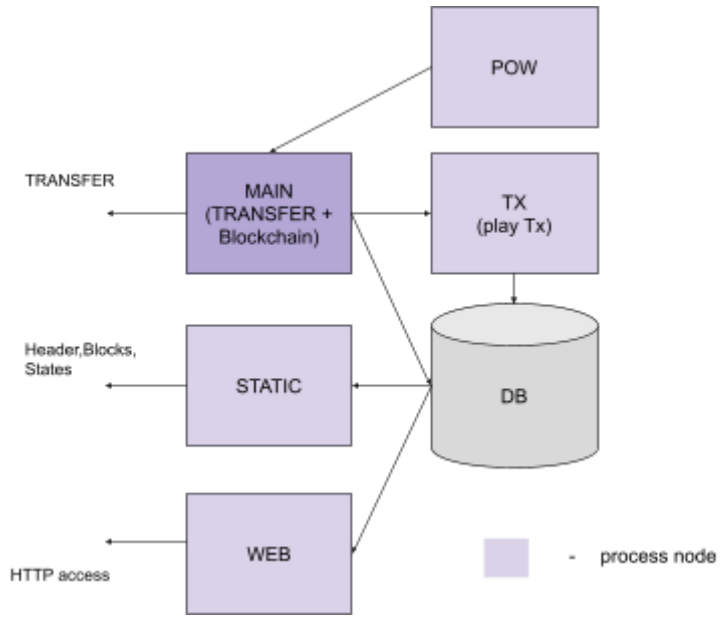
Protection against DDoS: PoW (hash calculation)
Platform: Node.JS

Composition of processor threads

An important point of the blockchain in Tera is the continuous operation of the network. The network is formed by creating a multi-dimensional lattice topology with dynamic structure support. The exchange is performed every second. The node must continuously exchange information on new blocks with its neighbors (this task will be referred as TRANSFER). Such exchange should be performed even if the node is in the blockchain loading mode (i.e. not synchronized)..

When you start a full node, the following processes are created (node):

1. **MAIN** - the Main thread of the program + TRANSFER. Writing new blocks to the database. Loading history when out of sync.
2. **STATIC-Giving** static information to other nodes (headers, blocks, States)
3. **TX**-executing transactions (changing the state table).
4. **Web**-data Retrieval via HTTP for full integration with the WEB
5. **POW**-mining processes. Memory pumping with hashes and quick search for a given match.



Links

Website: https://terafoundation.org/
Bitcointalk ANN: https://bitcointalk.org/index.php?topic=4573801.0
Repo: https://gitlab.com/terafoundation/tera2

Tools

Tera Decentralized Exchange: http://teraswap.io/
Online Node Map: https://teraexplorer.org/map.html
Web Wallet: https://terawallet.org/
Top Miners: https://teraexplorer.org/dapp/100

API-1: https://gitlab.com/terafoundation/docs/-/blob/master/develop/API.md
API-2: https://gitlab.com/terafoundation/docs/-/blob/master/develop/API2.md
Constants: https://gitlab.com/terafoundation/docs/-/blob/master/develop/CONSTANTS.MD
Release2468:
https://gitlab.com/terafoundation/docs/-/blob/master/develop/release2468.md
Release2600:
https://gitlab.com/terafoundation/docs/-/blob/master/develop/release2600.md

Docs

DApps Paper:
https://docs.google.com/document/d/1PXVBbMKdpsAKPkO9UNB5B-LMwIDjylWoHvAAzzrXjvU/edit?usp=sharing

TERAHASH mining algorithm:
https://docs.google.com/document/d/18DtASGhrbRwXCAkQR1hQG0lVdrStp4CgA-pd6hicwfo/edit

RUS - Обновлённый протокол консенсуса TERA - JINN
https://docs.google.com/document/d/1wV9bFUHeLA-u7y1eM9wQkLkzQ9OJf82rEbCFITXPTg8/edit#heading=h.6wabh3sbxwv5

Social Media

Telegram: https://t.me/terafoundation
Twitter: https://twitter.com/terafoundation
Discord Invite Link: https://discord.gg/CvwrbeG
QQ: https://jq.qq.com/?_wv=1027&k=5KpN5fw
Youtube: https://www.youtube.com/channel/UCMrK6jEqhudlV9XzS2l3rVQ