TOLAR

Tolar HashNET: Beyond Blockchain Technology

Whitepaper **V.1.2**
Last updated on July 27, 2018
Subject to further review & update

TABLE OF CONTENTS:

1. DISCLAIMER

General terms and conditions governing the Tolar project, platform, products and services can be found here https://www.tolar.io/terms-and-conditions/

Please read these terms carefully and make sure you understand everything.

2. BACKGROUND

The arrival of the **blockchain technology introduced many advantages** to the world making its potential huge.

It allowed many computers to take part in a network, distributing the computing power, which helped reduce the risk in any tampering, fraud or cyber-crime. Furthermore, it allowed different parties to believe that transactions between them are indeed real and valuable. With immutable records of transactions this also ensured a possibility for a massive range of digital transactions to happen without any central authority. With significant reduction of monopolies or middle men, this also removed a lot of costs from the equation. Blockchain also ensured immutability, as any transaction can be confirmed and shared across the distributed network, while almost impossible to undo.

2.1. The problem

All of these are great advantages offered by blockchain and today we can see many projects trying to leverage them the best way they can. However, in recent years blockchain technology proved to have significant **problems**. Among them is a huge environmental cost in the way blockchain is being used today. One of the most famous examples of this is Bitcoin that uses computing power that consumes as much energy as used by 159 of the world's nations. Another major shortcoming is that Blockchain is slow and takes much longer time to process any transaction when compared to let's say "traditional" payment systems such as cash or debit cards. For example, bitcoin transactions can take a few hours to finalize which is truly unsatisfactory and significantly limits the potential for bitcoin as a payment mechanism. Another shortcoming is the DApps which, while having a huge potential, failed to revolutionise the market to this point.

These shortcomings inspired the founders of Tolar HashNET **to provide a solution that solves these major shortcomings of blockchain technology, while maintaining all of its advantages.**

2.2. The context

Blockchain is the fastest-growing digital technology since the evolution of internet. For the last few years, it is starting to change the face of business across the world. For that reason, we asked ourselves one simple question 3 years ago - what can we do to make the most of blockchain technology with the resources we have at our disposal?

The answer was facilitated by [COTRUGLI Business School.](#) COTRUGLI recognized the potential of blockchain technologies among the first in the region of SE Europe, provided crucial support from the start and turned out to be best resource we could use to make the most of blockchain technologies.

For this reason, we chose COTRUGLI as the strategic partner of the project.

COTRUGLI is the leading business school in SE Europe with amazing impact and influence in the business community. They have strategic collaborations with more than 2,000 MBA Alumni (middle and top managers from the region), and over 20,000 satisfied clients (leading companies across different industries). All of them stand to benefit greatly from the blockchain technology.

With campuses in Croatia and Serbia, and branch offices in Bulgaria, Montenegro, Romania, Slovenia and the UAE, COTRUGLI is significantly impacting business networks in most countries in SE Europe, while at the same time reaching cultures and business environments worldwide. To highlight this statement, COTRUGLI Fund alone has invested over 3 million EUR into MBA Scholarships for the best and the brightest candidates from the leading companies in the region.

2.3. The solution

Thanks to the full support of COTRUGLI, we were able to jumpstart several initiatives that ultimately gave birth to Tolar HashNET.

One of the first initiatives was the creation of Blockchain Adria, which became a central place for blockchain ecosystem in SE Europe. Here, in addition to regional conferences, meetups and hackathons, we also developed Blockchain Academy and the worlds 1st Blockchain EMBA Program and Program for Certified Blockchain Developers, helping our clients make the most of this fascinating technology.

The ongoing success of Blockchain Adria gave us the confidence and inspired the passion to move further. At the time, many projects in the blockchain arena were failing to deliver on their promises, in sense of becoming major solutions for businesses and governments around the globe. This inspired and empowered us to start our very own project, one that could leverage on the main advantages of blockchain technology, resolve some of its main weaknesses and dramatically impact the global business.

With the ongoing support from COTRUGLI, we started a process of incubating several ideas we found to be credible. All of them were guided professionally by the COTRUGLI Incubator, piloted and examined back and forth by prominent business experts, consultants and MBA graduates on one side, and blockchain professionals and enthusiasts on the other.

The one idea that prevailed was the one that received amazing support from the start, as it was deemed revolutionary, credible and attainable. The idea soon became an extremely serious and professional movement that skyrocketed from the start and received amazing support from both business and the blockchain community…

…we are proud to announce **Tolar.**

Based on HashNET – a revolutionary technology beyond blockchain, we are confident TOLAR will indeed revolutionise the global business.

3. THE VISION

We want to position **Tolar HashNET** as the global leader of all DLTs, and to become a favourable solution for enterprises and governments by providing an open, fast and extremely fair public ledger built on top of the revolutionary HashNET technology.

4. THE PRODUCT AND BUSINESS OVERVIEW

4.1. Introducing HashNET

HashNET is scalable, efficient and high-impact decentralised solution to social innovation challenges leveraging Distributed Ledger Technology (DLTs). This revolutionary algorithm features faster transaction time, masternodes and will have a community governed crypto-currency – Tolar.

DLT in its public, open and permissionless form is widely considered as a ground-breaking digital technology supporting decentralized methods for consensus reaching, as well as sharing, storing and securing transactions and other data with fewer to no central intermediaries.

HashNET consensus uses "redundancy reduced gossip" and "virtual voting" protocols based on a distributed computation and algorithms from theoretical computer science, which provides a fair and fast, byzantine fault tolerant consensus algorithm. It is a new consensus substitute platform and is designed to run on a non-permissioned (public) network thereby, reaching a larger community.

HashNET is designed to solve the blockchain scalability problem using the revolutionary algorithm discussed above. It is a new consensus substitute to blockchain, keeping all the good characteristics from blockchain (decentralized, transparent, pseudo anonymous) and increasing speed to more than 200.000 TPS.

HashNET is cost-efficient and environmentally friendly given that no mining is required, as it uses minimal computing resources. It is designed to solve the problem with Bitcoin, Ethereum and similar PoW systems, which now use more electricity than 159 countries including Ireland and most countries in Africa.

HashNET is scalable

Scalability is the biggest problem in the blockchain technology space. Projects like Bitcoin and Ethereum are simply not capable of transferring a large number of blockchain transactions in a short timeframe. HashNET, on the other hand, was built to support over 200,000 transactions per second, compared to Bitcoin, which can only manage 7 transactions per second. Also, even with a large increase in number of nodes, HashNET network will be able to process all transactions in a matter of seconds.

HashNET is fair

Why? Because no individual can manipulate the order of transactions. With HashNET, there is no way for the individual to affect the consensus order.

HashNET is fast

It doesn't require miners to create a chain of blocks in order to record transactions. This process of creating a chain of blocks is very slow and it consumes a large amount of electricity. HashNET uses Proof-of-Stake algorithm combined with masternodes to reach distributed consensus. The process of receiving and recording occurs as soon as transaction takes place, which allows the final confirmation to be ready instantly.

HashNET is 100% secure

HashNET can't be hacked due to the power of distributed algorithm, which is responsible for reaching consensus within the nodes. Also, combining Proof-of-Stake and masternode creates transparency, since the participants are compensated for correct voting.

4.2. HashNET Characteristics

Transparency of funds
Allocation of community funds and voting process is 100% transparent.

Speed
Network's throughput can process 200,000 transactions per second.

Mobile compatible
HashNET can be run as full node even on smartphone.

Ability to grow
Easily scales with number of users.

Completely decentralized
Every participant can contribute by voting.

4.3. Features

	TOLAR	Bitcoin	Ethereum	ICON	EOS	Ark	Lisk	Cardano	Hedera	
Interchain support	**YES**	NO	Yes	Yes	NO	YES	YES	YES	NO	
Speed	**200.000 / s***	2 / s*	20 / s*	unknown	100.000 / s*	5 / s*	3 / s	10 / s*	200.000 / s	
Dapps	**YES**	NO	YES	YES	YES	YES	YES	YES	YES	
Codebase language	**C++**	C++	Python	C++	WebAssembly	Javascript	Javascript	Haskell	Java	
Energy consumption	**Very low**	High	High	Low	Low	Medium	Medium	Low	Low	

* – predicted

4.4. The Governance System

Tolar has a governance system called Magnus Consilium in which stakeholders and investors will have the power of voting on proposals in order to participate in improvements of HashNET network.

Magnus Consilium will be a part of community in two ways:

1. Tenders

Tenders are budgeting plans which will be submitted to the Magnus Consilium where every proposal will need to have a majority of votes in order to pass.

2. Proof of Stake (PoS)

If a user decides to lock-in his coins, he/she will receive interest based on the number of coins staked, and the duration of time the coins were stored.

4.5. Tender eligibility

Tenders and budget plans are available to all Tolar holders. Magnus Consilium will select projects for voting, based on a solution that best meets the following criteria:

Social impact: Potential impact achieved by the implementation of the solution.

Decentralisation and governance: Allows voters to vote on future network developments.

Outreach: Adding value by spreading a word out to the community.

Contribution: Awarding improvements of Tolar network.

Extensiveness: Allowing voters to make decisions on further development paths.

5. THE TECHNOLOGY

5.1. Information transfer solution

HashNET provides a novel solution to computational and communicational difficulties of maintaining large-size public distributed ledgers. The key innovation is our efficient asynchronous distributed consensus protocol on an appropriately designed directed acyclic network structure. Our consensus protocol belongs to a class of gossip-based protocols, which provide advantages over structure-based group communication algorithms as they can handle large group sizes, sporadic sources, high user churns, and random network failures (for the details of the theoretical support, see e.g. [1, 2]).

To ensure history immutability through time, which is an important property for public distributed ledgers, network nodes are connected using hash pointers ([3] provides an introductory technical description). It is well established (e.g., [4,5]) that as long as the selected hash function is secure, already agreed upon history cannot be changed retroactively.

One of the primary goals in designing HashNET was a significant reduction of computational and communication resources needed to operate and maintain the system. With this goal in mind, we designed a variant of a Redundancy Reduced Gossip (RRG) protocol for information transfer on appropriately designed network.

Such RRG protocols achieve considerably lower traffic load than conventional push-based gossip protocols and conventional push-pull gossip protocols, while maintaining the same probability of successful delivery [6].
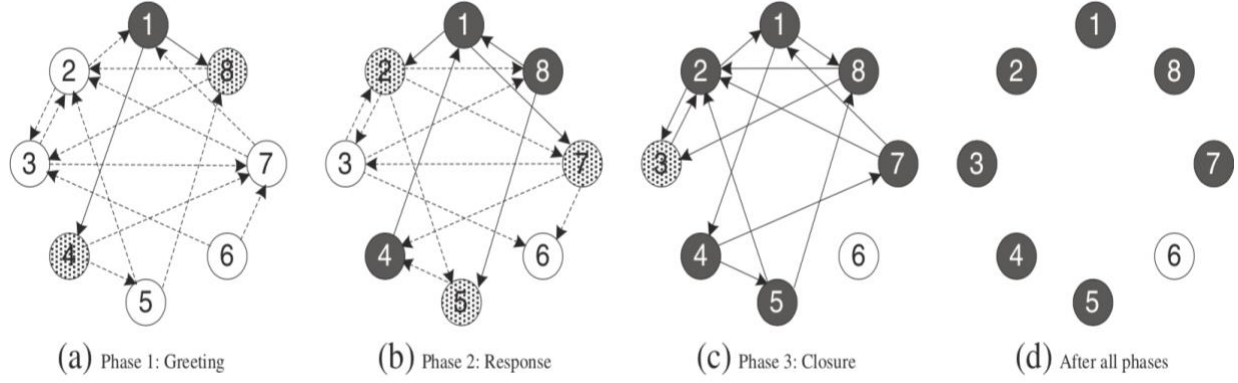
Figure 1: Information frame from peer 1 are diffused via gossip that are 3-phase message exchanges in one cycle: (a) Phase 1: Greeting, (b) Phase 2: Response, (c) Phase 3: Closure, and (d) After all phases; Fanout=2; Peer(s) shaded black is infected at the beginning of the phase; Peer(s) shaded grey is infected at the end of the phase; Peers shaded white remain uninfected at the end of the phase; A solid line refers to a message containing a frame; A dotted line refers to an empty message. [6]

Traffic load in Figure 2 is measured in terms of average number of copies of an information frame received by each peer. But each message contains protocol headers, and the resulting overheads for the two compared protocols are different. When n=100 and the average number of active peers is less than 3, with c=2, the overhead in RRG is around 20% of total traffic. Most of the overhead is contributed by the APL, where membership information is carried and requires 6 bytes per peer. In the same settings, the overhead of the conventional push gossip and the conventional push-pull gossip are around 40% of total traffic. Most of the overhead is contributed by the buffer-map, which is at least 12 bytes per gossip message.

It is important to note that our protocol generates a smaller number of messages than the fully connected peer-to-peer overlay approach in N-to-N communication. The number of messages in our protocol is only around 24% that of the fully connected overlay approach.
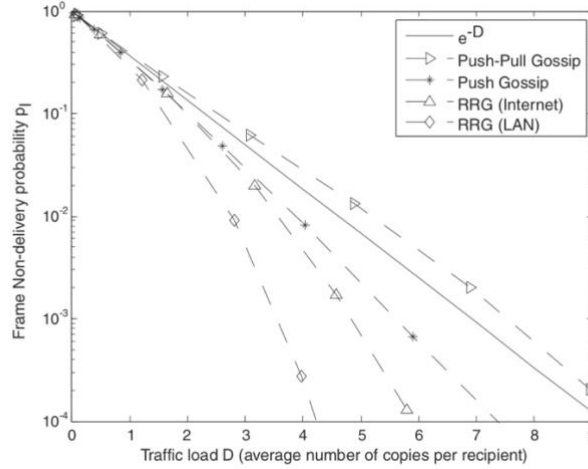
Figure 2: Performance comparison of redundancy reduced gossip (RRG), the conventional push gossip and the conventional push-pull gossip. [6]

5.2. Computational and communicational efficiency

While RRG and other asynchronous distributed consensus protocols provide communicational and computational efficiencies, additional implementation improvements are necessary to handle large fast-growing systems. A direct implementation of such protocols could require exchanging as much as $O(n^3)$ messages for reaching a consensus on a single binary outcome [7], which would make them not practical and unsustainable for systems where the number of nodes, n, is large. Thus, it is imperative to implement the consensus protocol in a way that minimizes communicational load due to information transfer among nodes.

However, we leverage the fact that every node has a sufficient information on the entire HashNET structure, including information about events and their propagation through the network. We use this information to compute content of the vast majority of messages required by our RRG protocol, thereby eliminating the need for sending them and, consequently, significantly reducing communication requirements. (A somewhat similar approach towards reducing communication requirements in an implementation of a different consensus protocol has been proposed in [8]. Unlike our system, a critical requirement in [8] is that the number of nodes is constant and must remain fixed constant throughout.)

An important prerequisite for an efficient computation of consensus is that the total number of nodes ("voters") needs to be known. This provides an inherent difficulty for an implementation involving public ledger, as the number of nodes can vary greatly. We overcame this difficulty by assigning to every node the vote weight that is equal to their stake at a given point of time. Since, at any given point of time, the current supply of coins in the network is known and fixed, this approach ensures proper consensus computations. Thus, by assigning node weight to be its stake in network, we achieve the ability to calculate votes instead of waiting for and/or sending actual votes over the network. As the protocol provides a Proof-of-Stake blockchain discipline, it offers qualitative efficiency advantages over blockchains based on proof of physical resources (e.g., proof of work).
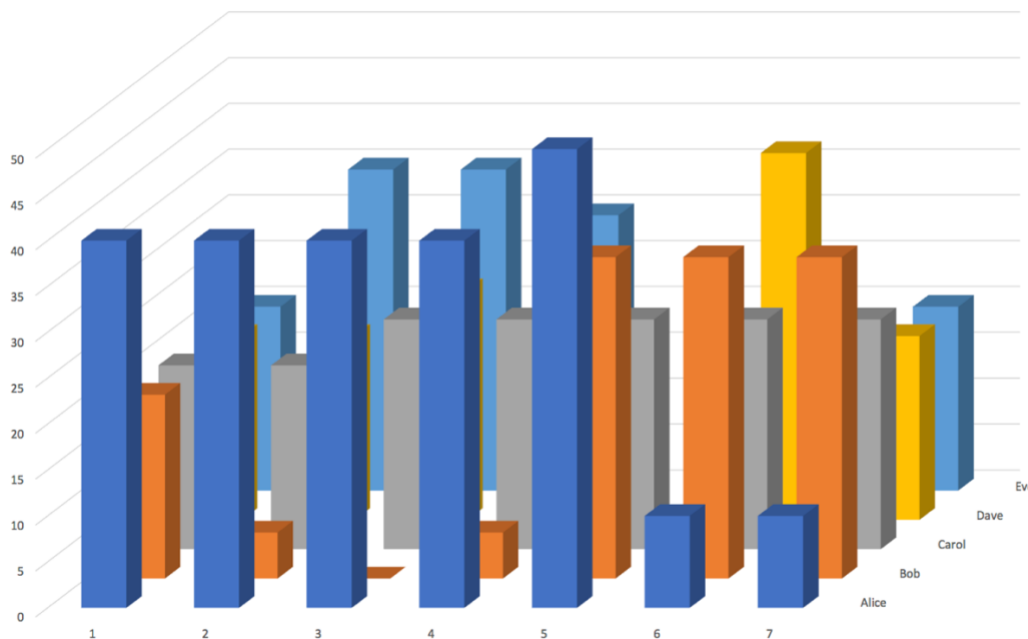

Figure 3: Illustration of HashNET voting weight and stake changes through the voting rounds as a result of transaction events. Do note that in each round some transactions happen that transfer Tolars from one participant to another, however total vote weight through the network stays the same in each round, enabling us to have virtual voting without knowing the number of nodes in advance.

Furthermore, with such weight assignment to nodes, incentives are perfectly aligned with the stakes, suggesting reduced strategy space for obstructive and malicious behaviour. Indeed, it can be shown that the reward mechanism for incentivizing Proof-of-Stake can be constructed in such a way that truthful behaviour is an approximate Nash equilibrium, thus neutralizing selfish-mining attacks [9, 10, 11].

5.3. Reputation based system

In addition to the Proof-of-Stake based discipline, a reputation-based system is introduced as an additional control and verification mechanism. This allows us to measure 'severity' of network protocol violations: some violations could simply be a consequence of sporadic unfortunate network conditions (small negative impact on reputation), while others could be attributed to a specific malicious intent (large negative impact on reputation). Similarly, for nodes which are consistently "fault-free", i.e. consistently communicate correct information and locally compute consensus correctly, a positive reputation is slowly built-up over time. All nodes whose reputation falls behind a certain negative reputation threshold are banned from the network for the amount of time decided by an exponential back off algorithm. (Such reputation-based systems have already been proven useful for self-regulating in many P2P applications [12].) Information about node reputation is realized as part of events distribution algorithms. The reputation score is computed iteratively and cumulatively and involves both pattern analysis for a behaviour over time of a single node, as well as randomized verification checks.

5.4. Achieving consensus

Potentially faulty or malicious nodes provide an additional challenge of implementing a consensus protocol in an asynchronous environment. In fact, it is well-known that it is theoretically impossible for any deterministic protocol to reach an agreement in such environments [16]. Thus, our implementation resorts to a class of so-called iterative randomized approximate consensus algorithms. The goal is to allow fault-free nodes to agree on values, overcoming the obstacle posed by (possibly incorrect or unreliable) information disseminated by faulty nodes.

Theoretically, the most challenging case are leader-based consensus algorithms, which rely on a small number of nodes that cannot be faulty (e.g., such as [8]). Such protocols are prone to failure and usually exhibit several unresolved issues in the case of a malicious node becoming a leader [13]. In contrast, fully distributed protocols (in which every node in the network could be decisive and in which no node is always decisive) allow for design of algorithms that overcome faulty nodes as long as fault-free nodes form a supermajority at any point of time. More precisely, the approximate consensus algorithm can be constructed even on fully connected graphs provided that the total number of nodes n > 3f, where f is the number of faulty nodes [17]. Our implementation leverages this result: if a consensus is not reached after a number of rounds of our RRG protocol, we initiate a sequence of "random rounds". In a random round, any non-faulty nodes will choose their votes at random and will have a non-zero probability of all choosing the same vote. The randomization is such that guarantees the correct agreement among non-faulty nodes with high probability. Thus, implementing a small number of random rounds results ensures convergence to consensus (i.e., the probability of failure is converging to zero at an exponential rate). Finally, we note that randomization does not need to pose a significant computational burden and can be manipulation-free, as bits provided by event hash (that need to be computed anyway) can be used as a source of pseudorandom data.

5.5. HashNET utxo storage requirements

In addition to aforementioned speed performance guarantees made possible by HashNET design, we are also able to guarantee improvements in the global data storage size. Specifically, HashNET data storage is designed by generalizing the approach laid out in MimbleWimble whitepaper [14]. The main benefit of this approach is that it manages to simultaneously handle security and versatility.

We utilize concepts such as Confidential Transactions and "One-Way Aggregate Signatures" (OWAS), which are shown to provide private exchanges and better adaptability. The main idea behind OWAS is that when the outputs are created and destroyed, it is the same as they never existed. Consequently, to approve the entire chain, a client only needs to know when coins were inputted into the

framework and what are last unspent yields. We then utilize Confidential Transactions to conceal the sums and OWAS, thereby obscuring the exchange diagram. This approach utilizes less space than, e.g., Bitcoin to enable clients to verify the blockchain. For instance, the Bitcoin blockchain is currently about 160GB in size, while HashNET would require a small fraction of that amount for the same amount of transactions, thus allowing even today's standard smartphones to act as nodes.

In our approach (similar to MimbleWimble), the beneficiary of transaction creates the blinding element which is utilized to demonstrate responsibility for coins. This is done through the "excess value", which is the contrast between the information sources and yields. This overabundance esteem is an arrangement of arbitrary numbers that guarantee that only the individual who created the blinding factor (the collector/receiver) can spend the coins. Thus, the blinding variables don't indicate zero any longer, but instead another number, resembling a private key. The important feature of our approach is that it is not interactive, which in turn creates efficiencies by eliminating the need for storing any redundant information on history of individual transactions. Rather than containing complete history of all transactions, the blocks (analogous to MimbleWimble) only have a list of new inputs, a list of new outputs, and a list of signatures which are created from the aforementioned excess value (Note that the latter list provides sufficient record of all historical transactions).

In summary, generalizing, adapting and implementing MimbleWimble approach for use on a HashNET provides a chain format that has excellent scalability, privacy and fungibility properties.

5.6. Democratic user-governed system

One of the central features of HashNET design is a democratic governance system which allows for involvement the entire community and is open to everyone.Specifically, any node in HashNET network can propose tenders, and then Magnus Consilium decides and votes on each such proposal. Magnus Consilium is comprised of all the masternodes with positive reputation in HashNET. Voting is decided by simple majority.

6. MASTERNODE AND NODE INCENTIVES

6.1. Overview

Masternode owners are helping secure HashNET network by enforcing the following:
- Validating that all transactions have correct signatures for outputs being spent
- Transactions must be in correct data format
- Prevent double spending
- Outputs being spent are valid

If any event gossiped through HashNET contains a transaction that violates some of the rules, then it will be rejected.

In addition to securing the network, masternodes also provide some special functions:
- Participating in governance and voting
- Enable budgeting and treasury system of Tolar

Masternode is comprised of:
- A masternode operator (owner)
- Collateral held in Tolars that serves as guarantee to ensure masternode doesn't act maliciously
- Server used as a part of decentralized infrastructure of HashNET

6.2. Collateral

Since masternodes are critical for processing transactions and helping secure the network, there is need to ensure that masternodes won't act maliciously. That's why operators need to put in collateral in TOL which is then locked while masternode is active. In case of constant malicious behaviour of masternode (trying to vote-in invalid transactions, DoS attacks on rest of the network, constant invalid data), collateral will be frozen, and masternode kicked off the network. Required collateral for Tolar masternode is 500,000 TOL.

6.3. Masternode Server

Server in this case is computer or computing-cluster connected to a network which provides masternode services mentioned above.
Minimum requirements for server are:

- quad core 64bit processor

- 16 GB RAM

- 128 GB of available disk space

- 50 Mbps symmetrical internet connection

- Fixed and unique IP (only one masternode can run at one IP address)

While these are minimum requirements, it's recommended to have masternode on a better configuration, especially in higher network load scenarios. In case that your masternode starts lagging because of insufficient processing power or bandwidth, it will not receive masternode rewards for those rounds.

6.4. Masternode rewards

Since masternode operators are spending their resources to help secure the network, they will be incentivized to keep the masternodes running by getting masternode rewards.
Rewards will be comprised of:

- transaction fees of all transactions that masternode helped validate correctly and on time

- masternode incentives from Tolar monetary reserve fund

Since rewards depend on the transaction fees, it is clear that rewards will fluctuate depending on the network usage. The more people use the network and make more transactions, the more rewards will masternode owners receive. To insure best possible start of the network, for the first 3 years, if masternode rewards from transactions fee fall below 10%, then part of rewards will be taken from Tolar reserve fund to ensure a minimum of 10% ROI.

Example scenarios

Scenario 1: Network constantly running at 0.1% capacity on average
Around half of TOL supply in masternodes (around 1000 masternodes)
Generates:
(200 transactions/sec * 0.01 TOL (fee) * 31,536,000 sec (1 year)) / 1000 masternodes =
63,072 TOL / masternode 63,072 TOL / 500,000 TOL = 12,6 % In this case, masternode owners makes 12,6% ROI yearly

Scenario 2: Network just starting, running below 0.005% capacity on average
Only small part of TOL supply in masternodes (around 200 masternodes)
Generates:
(10 transactions/sec * 0.01 TOL (fee) * 31,536,000 sec (1 year)) / 200 masternodes =
15,768 TOL / masternode in this case, part of rewards be taken from Tolar reserve fund (up to 1% of supply per year reserved for masternode rewards):
7,000,000 TOL / 200 masternodes = 35,000 TOL / masternode Total: 50,768 TOL / masternode 50,768 TOL / 500,000 TOL = 10,15 %

Scenario 3: Network getting a lot of usage and traction (running at 0.2 % capacity on average)
Lot of TOL in masternodes (around 1500 masternodes)
Generates:
(400 transactions/sec * 0.01 TOL (fee) * 31,536,000 sec (1 year)) / 1500 masternodes =
84,096 TOL / masternode 84,096 TOL / 500,000 TOL = 16,8 %

6.5. Governance

In addition to masternode rewards, masternode owners get additional benefit of participating in Tolar network governance. Any node can submit a tender from one of the following categories:

- Social impact
- Decentralization and governance
- Outreach
- Contribution to network
- Extensiveness

After tenders are submitted, masternode owners then vote on each proposal, and accept or refuse it. This makes the masternode owner help the network in decision making process, as well as the technical validation.

7. USING TOLAR PLATFORM IN VERTICAL MARKETS

7.1. Introduction

Using Tolar platform based on HashNET protocol we can provide new features like scalability, high processing speed and security compared to present blockchain platforms. However, main goal of our development is to create ecosystem of solutions and partners that will use this unique technology to solve problems with existing systems or provide new functionality that was not available before. Here are several examples in vertical industries of potential use of Tolar platform with all the benefits and advantages over existing solutions.

7.2. Approach

Collaborate with biggest ICT companies in selected countries on DLT projects. Provide real use cases on use of DLT focused on most innovative areas: IoT, logistics, healthcare and government. To create real life projects, start relationship in the region on pilots with local ICT companies, providing material for whitepapers, web and presentations along with business development managers specialized for selected vertical industries. Using established pilot projects, we can promote Tolar platform and DLT usage thus engaging new ICT companies as our partners.

Key steps:

- Communicate core values that makes us different to other blockchain and DLT projects
- Influence some major public projects to use our technology
- Create SDK with examples and easy to read documentation and examples
- Build team of business development managers that will provide technology insight combined with real life examples

High speed platform

Our revolutionary algorithm HashNET enables the platform to have unsurpassed number of concurrent transactions, so it can be used in most challenging, high performance environments that require high processing speeds. Throughput of the platform does not depend on numbers of nodes and we can add or remove nodes to the network in real time thanks to the unique architecture including ledger, new consensus protocol and HashNET algorithm.

Healthcare

Tolar platform in healthcare industry can provide solution that will keep medical records secure and prevent any unauthorized access, while providing high performance and ease of use to all parties that are using it. Main advantage of Tolar platform is well documented and easy to use API that does not require previous knowledge of ledger technology and can be used by all partners already providing IT solutions in healthcare industry.

Supply chain logistics

Tolar enables supply chain management exchange between tiers using open, decentralized network on distributed ledger, which holds information of every transaction and performance history for all engaged parties. This information gives control of real time information to included parties, so they can optimize processes and save both time and resources for all transactions.

Procurement in Enterprise Environment

Procurement process using Tolar platform is open network for buyers and sellers using distributed ledger, which holds information of reputation, execution and sourcing history for all included parties. This information gives both buyers and sellers power to publish tenders and choose on which tenders to apply using distributed network. Fully digital, without any need of other, slow channels, tenders can be closed in matter of hours and days, not weeks, using the scalable, efficient and decentralized solution in open and public form.

Government

Government organizations can use the platform to build trust through open, transparent and collaborative network. This network will enable moving from bureaucracy into transparent and collaborative ecosystem in which citizens will interact easily, using all available digital channels for all of their needs, with government agencies. Tolar API will enable business partners to quickly build and deploy new applications in government ecosystem.

7.3. Examples of real use cases in development

Healthcare – partner A (hospitals, Ministry of Health)

Tolar platform in healthcare industry can provide solution that will keep medical records secure and prevent any unauthorized access, while providing high performance and ease of use to all parties that are using it. Our secure and immutable, distributed ledger can hold all patient records with enabled access only to authorized users (hospitals, doctors) for the private data part and public access to the data for the patients.

Supply chain logistics – partner B

Tolar enables supply chain management exchange between tiers using open, decentralized network on distributed ledger, which holds information of every transaction and performance history for all engaged parties. This information gives control of real time information to included parties, so they can optimize processes and save both time and resources for all the transactions. Using this unique technology, we can help partner B optimize partner network across all countries and save time and money using innovative supply chain management.

Government – partner C

Government organizations like partner C can use Tolar platform to build trust through open, transparent and collaborative network. This network will enable moving from centralized database secured on many layers but not open to other government entities to distributed database open to every agency or government body that requires data access without complicated integration and data duplication.

Telecom (IoT) – partner D

As part of new IoT narrowband network deployed by partner D for all sorts of IoT devices, distributed ledger with high speed and security like Tolar can help register, authenticate and track all devices connecting to the network and publish relevant information to the public space (like weather data from sensors). Using Tolar, there is no need for expensive interfaces in private networks, all data can be stored securely in public ledger and used according to the level of privacy required.

8. THE FUTURE OF HASHNET

8.1. Platform for new ICO Projects

Using high performance platform with smart contracts, we can enable new generation of ICO projects to use Tolar flexible API and instantly create new projects on our platform. Speed of Tolar platform will enable new projects with stable, safe and secure platform which is able to execute any transaction in matter of seconds.

8.2. Decentralized applications

Once desired throughput is achieved, Ethereum Virtual Machine (EVM) will be deployed on top of the network. The EVM is meant be used in conjunction with a system that broadcasts transactions across network participants and ensure that everyone executes the same transactions in the same order. Ethereum uses a Blockchain and a Proof of Work consensus algorithm. Here, we will use HashNET. The combination of EVM and HashNET makes a fast and secure decentralized applications platform.

Once desired throughput is achieved, Ethereum Virtual Machine (EVM) will be deployed on top of network. The EVM is a virtual machine specifically designed to run untrusted code on a network of computers. Every transaction applied to the EVM modifies the State which is persisted in a Merkle Patricia tree. This data structure allows to simply check if a given transaction was actually applied to the VM and can reduce the entire State to a single hash (merkle root) rather analogous to a fingerprint.

8.3. Quantum resistance

The elliptic curve signature scheme used by Bitcoin is well-known to be broken by Shor's algorithm [17] for computing discrete logarithms. That is why in the next 5 years it will be imperative to switch to alternative signature schemes that are believed to be quantum safe. Exact scheme that will be implemented in HashNET is still being decided on.

9. CURRENT PROGRESS

We are pleased to report that we are meeting all our goals as set in the Roadmap.

9.1. Hype

In the past couple of months, Tolar has gained a lot of attention. Being featured on ICO Drops and receiving many reviews from top blockchain influencers has increased project's exposure and grown its Telegram group from a few hundred members to over 14,000 members.

Tolar has gained even more recognition after winning the Ian Ballina ICO pitch competition in Budapest during his Crypto World Tour in June.

Furthermore, Tolar's Founder and CTO, Josip Maricevic, has received the Beyond Leaders award at the Beyond 4.0 event, held in Ljubljana. During the same event, Tolar's Founder and the Principal of COTRUGLI Business School, won an award for the leading business school in the SEE region and received compliments from the Prime Minister of Slovenia, Miro Cerar and State Secretary of Slovenia, Tadej Slapnik.

Tolar reviews:

Tom H. Chase *(overall score: 90/100)*

Ian Balina (overall score: 79,56/100)
Tolar is my third best ICO. […] What I do like – it has a decent team, they do have prototype, they have all-star advisor,s which is good. It's a big idea - the fact that they are building an infrastructural project. They are competing with other blockchains. […] Their community is decent as well. To me, this is a border line all-star project.

OhHeyMatty (overall score: 87/100, upgraded from 84/100)
I think a project as a whole is pretty solid and I look forward to seeing what they have in store for the future and I'll definitely be following this project.
Tolar has recently had an AMA with OhHeyMatty after which he has updated his overall score to 87/100.

Andre Cronje
Great fundamental design, one that I look forward to seeing in the testnet, as soon as it is out. I think it can make a real difference in both finality and transaction throughput. It does lock them into Proof-of-Stake, since redesigning consensus will be a ground up design, but I don't think that is inherently bad. All in all, good code, novel design, excited to see where this goes.
Diddy Carter *(overall score: B+)*

Hacked *(overall score: 7.5/10)*
With a fairly large team, all-star advisors, an MVP, available masternodes, and a growing social media presence, Tolar is another blockchain project that has an excellent chance of doing well this year.

Coin Hunter *(SHRG score: GEM)*
Much lower cap Hashgraph competitor.
Code review by Andre Cronje looked great. Tolar has completed a live presentation of their test net on multiple nodes around the world and have achieved 150k TPS.

block42 (*overall score: B*)
The HashNET project together with the Tolar token looks like a promising DLT project. The team has blockchain experience and a comprehensive scientific background. With their prototype they have shown that they probably could reach their promise of 200.000 TPS. So the technical side of the project provides lots of future promise, but they also have to show that they can master the economical side of the project with real world partnerships and enterprises looking to build dApps on the HashNET.

Nebo @CryptoSeed_P and @LuxeEquity (overall score: 84/100)
Another solid-looking project aiming to solve the scalability and performance issues our current blockchain technology faces…

[Coindrift](#) *(overall score: 7.5/10)*
PROS: […] Large team of 24 total members with wide range of experience in research, founding tech companies, business development and marketing should help Tolar to achieve its goals. Founder Josip Maricevic was a core developer at cross-blockchain project Blocknet, though we struggled to find much more blockchain specific experience on the team. […]

[Why Crypto](#)
Positive side of HashNET are that it offers interchain support, smart contracts, Dapps, programing in c++ that is widely used. Governance system "Magnus Consilium", so on every proposals investors and stakeholders can vote. Next year they plan to deploy Ethereum Virtual Machine and Quantum resistant cryptography on their network.

[The Crypto Lifestyle](#)
[…] They have already proved themselves by developing their own protocol. It's not like if they took the already existing consensus mechanisms like proof of work, proof of stake. They took it to the next level and they went into hashgraph. So for them to say we are going to use hashgraph tech here that's one thing, but for them to actually show it here in front of this crowd and show that they achieved 136,000 TPS that to me is far better than some guy that worked for Google or worked for Microsoft or IBM but has no proof that he can make this actual product. […]

[Coin Bloq](#)
[…] Awareness of the project is definitely increasing but its slow at the moment with strong organic growth. Now that is actually a very good sign. As you know from my previous videos, organic growth is really something to watch, when it comes to investing in ICO projects. Tolar does not have a bounty campaign nor does it offer any airdrops which suggests that investors' sentiment is actually natural and not manufactured.[…]

[HT Crypto Detectives](#)
[…] The project has a big hype, this is promising because people are interested in it. […]
It's a nice project, It think its legit. […]

ICO Hunch

[…] We really like high throughput projects, as for our statistical analysis they tend to perform exceptionally well from our wide perspective… […] We will definitely keep an eye on this project and apply for whitlist once it is open[…]

Crypto Calibur (overall score 74/100)

We are excited to see the project's development among the upcoming months and find out whether Tolar can truly compete with the current heavyweights that are aiming to bring a scalable and rapid blockchain to the masses. Furthermore, we believe that Tolar's hype will steadily increase up until the crowdsale, however post-ICO, the team needs to step-up their marketing efforts if they want their product to remain relevant among investors and the cryptocurrency community as a whole.

Crypto Rand

Tolar provides a solution that solves major shortcomings of blockchain technology, while maintaining all of its advantages.

9.2. PROTOTYPE: demonstration of speed reaching up to 150,000 TPS!

On June 28, 2018 we organised a special event to show the progress of the Tolar project and explain the impact it can have on global scale. Josip Maričević, CTO and Founder, ran the TOLAR HashNET prototype to demonstrate the speed it can reach at this point of time.
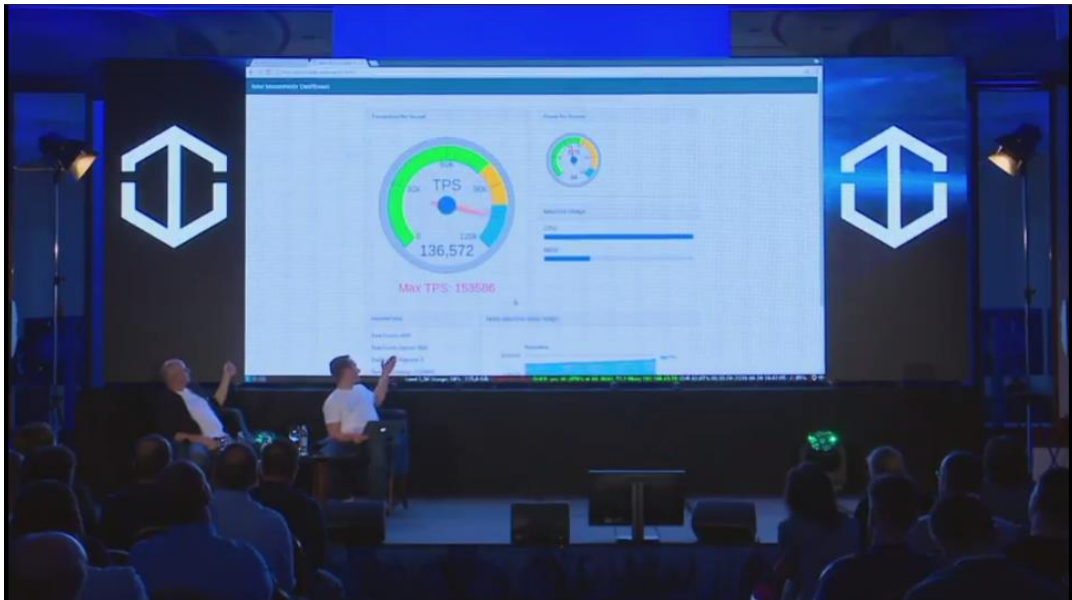
Maximum speed that the team was able to reach during the test runs exceeded **150,000 TPS**, being very close to the ultimate speed that the project aims to reach (200,000 TPS). As Mario Vojvoda, CIO, explains: "We are already able to do pilots on our platform, which shows stability and maturity of the platform in this early stage, but also our commitment to create unique ecosystem that will benefit our partners and developers ".

The event was held in Zagreb and all interested parties were able to watch the event livestream through Tolar's Youtube Channel. In order to watch the entire video please click **here.**

10. ROADMAP

Q2 2017

TOLAR project founded and funding received

Executive group established

Q3 2017

Blockchain Conference

Rovinj Initial network development

First cryptocurrency experiments conducted

Q1 2018

Launch of the Blockchain academy.

Recruiting process of key team members has started.

Core Tolar team created with 30 members.

Tolar introduce project publicly

Q2 2018

Initial version of HashNET whitepaper

Launch of initial mainnet chain with masternodes and staking system.

Start of the private sale phase and social media presence.

Q3 2018

Finalized version of HashNET whitepaper

Developers demonstration of HashNET

Presale

ICO

Exchange listing

Q4 2018

Chain explorer

Mobile wallets

Q2 2019

Public release of HashNET chain

Switch mainnet to HashNET protocol

SDK

Future development

Smart contracts

New ICO projects launch on top of Tolar HashNet

Quantum resistant cryptography

11. THE TEAM

11.1. Foundation Board
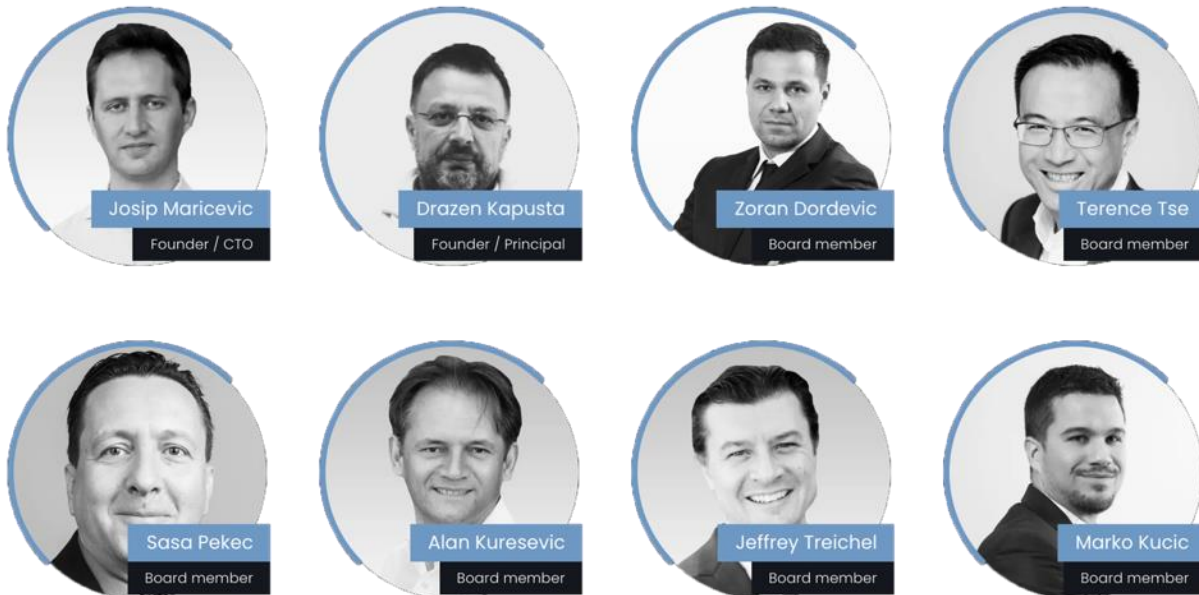
Josip Maricevic

Josip is the Founder and CTO of Tolar. He has been researching blockchain and related consensus algorithms, atomic cross-chain swaps and of- chain settlement protocols for the past 2 years. Also, Josip worked on development of a few significant blockchain products. He is interested in general algorithm research and development. He worked for Shazam on application that implements Shazam song recognition technology to identify songs in your iPod library and play them with synchronized lyrics and visualizations. Also, he is an owner of software development agency Moon Code, which is offering services of developing custom Blockchain based projects, alternative cryptocurrencies and Ethereum smart contracts.

Drazen Kapusta

Drazen Kapusta is the Founder and Principal of Tolar. He's an entrepreneur with 30 years of business experience. Drazen also serves as Principal of COTRUGLI Business School, the leading business school in SE Europe where he has successfully helped develop the world's first Blockchain MBA program and Certified Blockchain Developers Program.

Drazen is the President of Blockchain Adria, the most prominent blockchain conference and association in SE Europe. He serves as the President of the COTRUGLI Fund which is focused on organizing and leading numerous humanitarian projects.

Zoran Dordevic

He has more than 15 years of experience in education and consulting as well as passion for blockchain technology and its educational and business implementation. Zoran is one of the pioneers in introducing blockchain technology into regular MBA curriculums that set the foundations of the world's first Blockchain MBA program at COTRUGLI Business School. Besides his involvement in the educational business, he is very much involved in fostering entrepreneurial culture in the CEE region as consultant for large corporations, startups and ICO's. Zoran received his master's degree from University of Zagreb, Faculty of Economics and Business in Zagreb, Croatia and his MBA from COTRUGLI Business School in Zagreb, Croatia.

Terence Tse

Terence is the co-founder and CEO of Nexus FrontierTech, an artificial intelligence studio with years of experience in building and deploying AI for businesses. With more than 20 years of experience in financial corporate consulting, he continues to work closely with organizations like the EU and UN as well as commenting regularly on the latest current affairs, market and blockchain developments in the Financial Times, The Guardian, The Economist, CNBC, the World Economic Forum and the Harvard Business Review blogs. He obtained his PhD from the Cambridge Judge Business School, University of Cambridge, UK.

Sasa Pekec

Sasa Pekec is an Associate Professor in the Decision Sciences area at the Fuqua School of Business at Duke University. With more than 25 years of experience, he is currently teaching the core statistics course in the daytime MBA and the Cross-Continent MBA programs. His work on combinatorial auctions had been widely cited and had influenced design of a new generation of now standard procurement auction procedures in a variety of industries. His consulting experience includes banking, internet, pharmaceutical, retail, and telecommunications industries. Sasa serves on the Supervisory Board of Atlantic Group, one of the leading FMCG companies in SE Europe. He was a member of the Council of Economic Advisors to the President of Croatia. He holds a Ph.D. in Applied Mathematics from Rutgers University.

Alan Kuresevic

Alan is the Vice President, Engineering at SES TechCom, world-leading satellite operator and the first to deliver a differentiated and scalable GEO-MEO offering worldwide, with more than 50 satellites in Geostationary Earth Orbit (GEO) and 12 in Medium Earth Orbit (MEO). The company provides satellite communications services to broadcasters, content and internet service providers, mobile and fixed network operators, governments and institutions. With more than 20 years of experience, he successfully led a number of projects and technology development that provided foundation for the company's new service developments.

Jeffrey Treichel

Jeffrey is an entrepreneurial leader with 20+ years of experience and expertise in developing and rapidly operationalizing business models and brand strategies. He currently serves as Interim CEO of PaperKarma, one of Apple's top disruptive apps. He also founded and led Kolektiva, the first and largest daily deal site in the CEE region, raising $10+ million in VC and eventually building a $35 million business. Later on, he worked with Shoutem, a leading mobile app development platform for SMEs, where he successfully doubled revenues in his first year by securing new Enterprise deals with Fortune 500 media and communication companies. He earned his MBA degree from Harvard Business School and his BA from Tufts University.

Marko Kucic

Over 15 years of experience in business education and consultancy, his last position as Managing Partner at COTRUGLI Business School, the leading business school in SE Europe. Besides his strong experience in business education, he has a strong passion for blockchain technology. In this area, he has successfully helped jumpstart Blockchain Adria, the most prominent blockchain conference and association in SE Europe. Also, he helped develop the world's first Blockchain MBA program and Certified Blockchain Developers Program. Marko received his Master's degree from University of Zagreb, Faculty of Economics and Business in Zagreb, Croatia and his MBA from COTRUGLI Business School in Zagreb, Croatia.

11.2. HashNET Tech
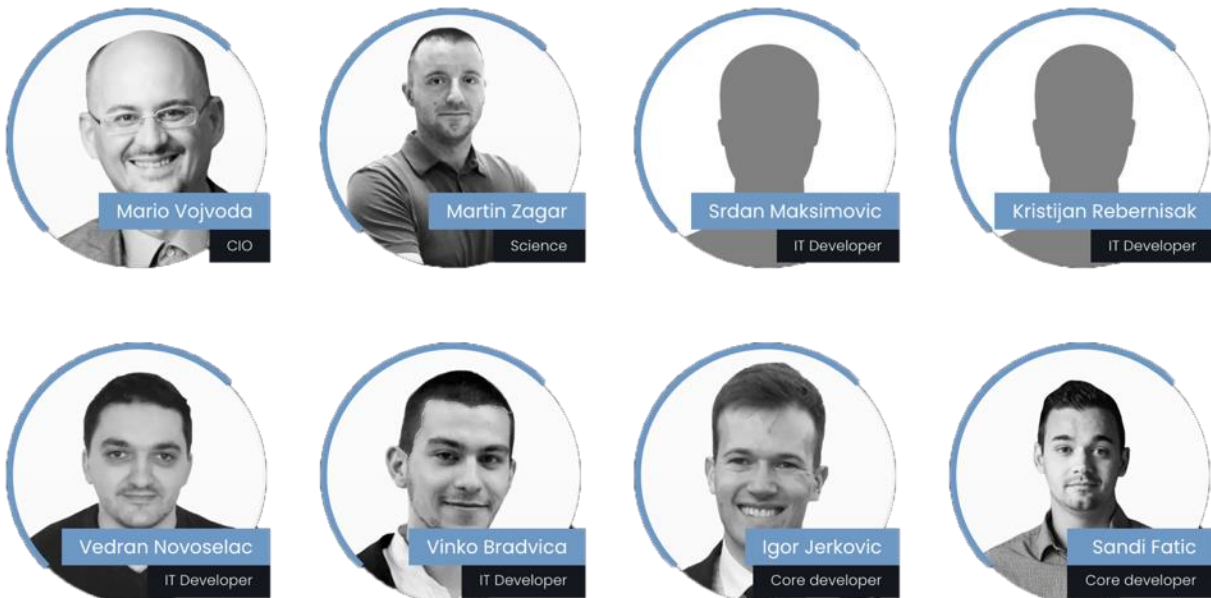
Mario Vojvoda

Mario is an IT Leader with more than 15 years of experience in the telecom industry, innovation, R&D and international business development within the challenging environment. Keeping up-to-date with new and emerging technologies, he has proven expertise in increasing revenues and boosting profitability of various projects and companies he has worked.

He was a board member of Combis, a renowned informatics company in the CEE region with market-recognised ICT solutions. With his strong technical knowledge in IT and telco areas, he also served as IT Director of T-Mobile Croatia and was CTO of Iskon.

Martin Zagar

His occupational fields are multimedia computer architectures and telemedicine. He has participated in several domestic and international scientific projects and also participated in supervising of the Information system in primary healthcare in the Republic of Croatia and is co-author of the Concept of Integrated Central System Authentication and Authorization. Martin Žagar has been awarded with EMBA from Cotrugli Business School and PhD in Computer Science from the UNIZG.

Srdan Maksimovic

Srdan holds a Master's degree in Computer Science and master's degree in Mathematics. He is a participant in International Mathematical Olympiads. He is an avid developer and researcher of different types of algorithms, from network flow to consensus. Does not believe in social media.

Kristijan Rebernisak

Kristijan's extensive experience includes working as a leader of the Software Engineering Team and as a Software Architect on challenging products in wearables, health, the music industry and other. Currently also co-founder of RunningBeta, company that builds unstoppable applications that run on open standards, leveraging the power of Ethereum.

Vedran Novoselac

Vedran is an experienced Linux backend developer and architect, whose skills cover topics such as: design and specification, Agile, code quality, implementation, testing, refactoring and maintenance, configuration, release management, code and package management, build automation, deployment, and documentation. He's also been fulfilling DevOps role as demanded by the past projects. Wider adoption of blockchain expanded his interests towards cryptocurrency trading and technologies, but also made him an avid explorer in area of blockchain cryptosystems and their applications in the real world. In total, he has more than 14 years of experience as a software developer.

Vinko Bradvica

Vinko received his Master of Science degree from University of Zagreb, Faculty of Electrical Engineering and Computing. Vinko is the founder of Information Technology and Services company RunningBeta.
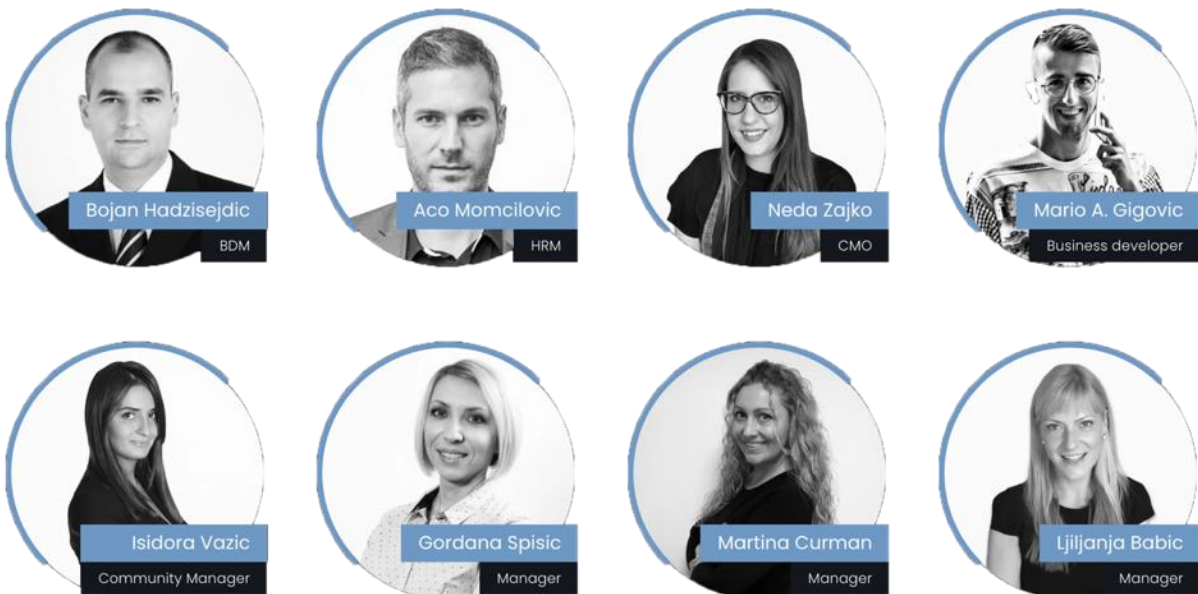
Igor Jerkovic

Igor is coming from algorithm competitions background, but currently mostly interested in how to use the ongoing crypto and distributed ledger advancements into something of a broader use. Worked for Facebook as Software Engineer for several years.

Sandi Fatic

Sandi is researching new distributed consensus algorithms and implementing them. Worked as Software Engineer at Memgraph – high performance, in-memory, transactional graph database. Also has experience of working in Google, first as Technical Associate and later as Site Reliability Engineer.

11.3. HashNET Bizz

Bojan Hadzisejdic

Serving as Business Development Manager of TOLAR.io, Bojan is an experienced sales professional with strong business and technical skills gained through 15

years of experience in the IT industry, both corporate and SME level. He started his professional career as a BDM at Microsoft (2003-2015), eventually becoming a cloud transformation consultant as well as director of Nephos, a company dedicated to help businesses transform and grow, implementing digital transformation. This means developing a comprehensive concept of using modern technologies that is consistent with strategic business development goals. Bojan received his Master's degree from the Faculty of Electrical Engineering and Computing, University of Zagreb and his Executive MBA from COTRUGLI Business School.

Aco Momcilovic

With more than 10 years of experience in strategic organisation of Human Resources, including the responsibility for staff members as well as budget balance, Aco serves as Human Resources Manager of Tolar, guaranteeing strategic HR objectives as well as functional and disciplinary guidance of the HR department. Among being a blockchain consultant, lecturer and ICO investor, Aco also serves as President of MBA Croatia, gathering all Croatian MBA Alumni from all domestic and foreign MBA Programs. He was also Chief HR Officer at Rimac Automobili, and has worked with numerous companies in matters of HR and consulting. Aco holds a Master's degree in Psychology from the University of Zagreb and an Executive MBA from COTRUGLI Business School.

Neda Zajko

With more than 8 years of experience in marketing and communications Neda serves as CMO of Tolar. With her vast knowledge of digital and strategic marketing, Neda is in charge of marketing strategies and campaign management while supervising a team of social media experts and following blockchain marketing trends. She received her Bachelor of Commerce Degree in Marketing from Concordia University (JMSB) in Canada and her Executive MBA degree from COTRUGLI Business School.

Mario A. Gigovic

Mario Gigović is a creative project management consultant, actively working in marketing, PR, business and communication strategies development. In the last five years, he contributed to over 70 local and international projects cooperating with clients spanning from many business areas - from culture, government and public services, tourism, health and education, management to public relations and international communication. With a dose of creativity and with his entrepreneurial background, he is in charge of developing special projects based on Tolar/HashNET. Received his masters degree from the Department of Production at the Academy of Dramatic Arts in Zagreb with thesis. Owns a certificate from London School of Public Relations and is one of the first fully certified digital communication experts in Croatia. Currently attending the International MBA program at COTRUGLI Business School. Holds an assistant position at the Academy of Dramatic Arts, University of Zagreb. He is an active member of Croatian Public Relations Association.

Isidora Vazic

Isidora is responsible for all social media communications at Tolar. She has 4+ years of experience in sales and communication. Isidora holds a Bachelor's degree in Communications from Megatrend University.

Gordana Spisic

Gordana is in charge of communication with strategic partners and customers on a regular basis while also integrating customer and partner product needs as well as contract requirements with business operations and product roadmaps. With 10+ years of management experience, she is responsible for achieving strategic account targets and conducting research to identify and validate new markets and customer needs.

Martina Curman

Martina's current position is Business Development Manager at Tolar where she communicates with clients on a daily basis and keeps track of administration and contracting issues in general. Additionally, Martina is very experienced in Team leadership, Office management and Business planning. She has 10+ years of experience in business administration.

Ljiljana Babic

Ljiljana is charge of communication with partners and customers on a regular basis and responding to specific queries. She is responsible for achieving strategic account targets and scope/design approaches to capture business development opportunities, integrate customer and partner product needs and contract requirements with business operations and product roadmaps. Ljiljana also has 10+ years of experience as a Business Development Director for Serbia, Bosnia and Herzegovina, Montenegro, Romania, Bulgaria and Macedonia at COTRUGLI Business School.

11.4. Advisors

Manuel Alonso Coto — PhD	Peter Merc — PhD	Petko Karamotchev — Advisor	Naviin Kapoor — Advisor
Nicholas Ang — Advisor	Lester Lim — Advisor	Lingya Gong — Advisor	Hsiung Yen-Hsiang — Advisor
Goran Miko — Advisor	Nick Ng — Advisor	Daniel Kochan — Advisor	Min Wang — Advisor
Valerio Opacic — Access and Security Services			

Manuel Alonso Coto

Manuel Alonso Coto, PhD is visiting professor at COTRUGLI Business School. He has received PhD in Economics (Thesis about digital business in Spain), King Juan Carlos University, Top Management Program (AMP), and Chicago Graduate School of Business &IE Business School. He graduated Executive MBA at IE Business School and Master in Foreign Trade, EOI Business School. He completed the Postgrad in Business Administration (with a focus on Finance), UNED University, Postgrad in Psychology (with a focus on Advertising), and UNED University. During his career he has worked as a Director of Marketing, Executive Education, IE Business School, Director of Digital Marketing, Executive Education, IE Business School, Director of Customer

Oriented Services, IE Business School, Director of Operations, ielearning.net, Director of IT/IS, US Department of Spain, Spain & Portugal and Director of Manufacturing, Agrapisa. He is an author of the Books: **"**Political Marketing", "Direct Marketing 2.0", "Blended Marketing. The Digital Marketing Plan as an integrator of on and offline actions", "Conversational Capital" (Spanish version), "From Second Life to Metaverses Marketing: Business in 3D", "I have 30,000 fans; so now what?", "Social Media Marketing Plan", "s-Internationalization

Peter Merc

A sharing economy and blockchain enthusiast, Peter is a co-founder of Lemur Legal, a legal consultancy and digital transformation advocacy company based in Ljubljana, Slovenia. He is lead coordinator of Blockchain Think Tank Slovenia, an NGO with the main goal to serve as a platform for blockchain knowledge in Slovenia and as a link between the private and public sector. The American Chamber of Commerce in Slovenia established The Circular and Sharing Economy Committee, where Peter acts as a co-chair. Before moving to the startup and fintech world, he worked in the banking sector where he's still active as a member of the supervisory board of Slovenian systemic bank. Along with TOLAR.io, Peter also advises several ICO projects. He received his Master's degree in Corporate law and his PhD in Banking law from the University of Ljubljana.

Petko Karamotchev

As one of the founders of the enterprise blockchain/DLT consultancy and development company INDUSTRIA.tech, Petko Karamotchev has 20 years of experience in the financial services and the enterprise IT. Holds degrees from University of Portsmouth, UK and COTRUGLI Business School, Croatia. Free market advocate and part-time social theorist.

Naviin Kapoor

Naviin Kapoor, a blockchain consultant and a business transformation leader with more than 12 years of experience in project management and business analysis and more than one year of experience in ethereum, bitcoin, hyperledger, EOS, consensus protocol and distributed/shared ledger technology. He has also attained various industry certifications such as PMP, CBAP, ITIL & Professional Scrum Master Level 1. He had worked on various banking transformation projects - "sustainable and disruption", which were initiated in various domains such as Retail Banking, Cash Management, Integrated Liquidity Management (ILM), Corporate Banking, Asset & Wealth Management, Financial Messaging, Regulatory Sanctions Filtering and Local and International Payment Systems. His proficiency in handling Project Life-Cycle Management, requirement elicitation, feasibility study, planning, scheduling, tracking, assessment/design, testing, change management and implementation support in both Waterfall and Agile environment.

Lester Lim

Lester is an active advisor for ICOs, including projects like Cardstack, HybridBlock, Dock.io, Ink Protocol, CoinFi and Banca. He advises token projects on marketing strategy and tokenomics, in addition to fund raising activity. He is also a cryptocurrency investor and founder of a global private syndicate investing in top ICOs, and an online business owner, digital marketing strategist and Facebook Ads specialist - having sold information & software products to customers from all over the world.

Nick NG

Nick is a family office fund manager responsible for managing assets over USD Billions in Hong Kong for up to 10 years. He specialises in different financial investments, including different countries' stocks, bonds and financial derivatives. He is extremely experienced in asset/portfolio management, with rich experience in trading with many top rated investment banks, e.g Goldman Sachs, UBS. He graduated from the University of Hong Kong with Degree in Information Engineering and Master's Degree in Industrial Engineering and Logistic Management. Founder of crypto fund BlackCastle Capital. Portfolio includes ICON, WANCHAIN, etc.

Faisal Shehzad Khan

Faisal is an IT Professional with 16 years of diversified experience in the field of Alternate delivery channels with sound knowledge of Enterprise system, Architect and Project Management with a blend of technical and business skill set. Extensive experience of middleware, internet banking, ATM, SMS banking, dot coms and enterprise application where his key involvements have been in the roles of project management, analysis, planning, system architecture designing, systems Implementation, solution evaluation, vendor coordination, administration and technical resource.

Valerio Opacic

Valerio, as a member of the Tolar team, is in charge for the Security of the Hashnet protocol. He has more than 26 years of working experience mostly dealing with Global Identity, Access and Security Services Manager at McDonald's Corporation. He is experienced in building globally scoped enterprise systems, with prime focus to computing platforms and underlying systems such as compliance, directories, security, platforms and applications. Besides technical expertise and historical development, he is managing complex IT systems from business perspective is also a strong asset. Integral part of engagement in his profession was always linked to non-technical aspects of primarily technical function, such as procurement, service buying or selling, consulting and alike. His recent education and interest is focused toward general management, with emphasis to implementation and alignment of technology and business, crowned by completion of MBA at COTRUGLI Business School.

12. PARTNERS AND INVESTORS

blockoxfund   BlockGround CAPITAL   萬布資本 WANDARIN   POD CAPITAL

BLOCKMATRIX CAPITAL   CARNABY CAPITAL INVESTORS IN A BLOCKCHAIN FUTURE   GC CAPITAL   CRYPTOCALIBUR

DIDDY CARTER   Capital   BlackCastle Capital   ANGFUND

13. FINAL REMARKS

We want to position **Tolar HashNET** as the global leader of all DLTs, and to become a favourable solution for enterprises and governments by providing an open, fast and extremely fair public ledger built on top of the revolutionary HashNET technology.

We are confident that this vision is possible and achievable, due to key reasons stated below:

1. 1st DLT prototype in the world with 150.000 TPS on multiple nodes, on all continents.
2. Excellent global team with successful track record and more than 40 members.
3. Powered by COTRUGLI Business School, the leading business school in SE Europe, with more than 2,000 MBA Alumni and over 20,000 satisfied clients.
4. High ratings from leading ico experts
   - Ian Balina – 82.21%
   - Tom H. Chase-83%
   - Oh Hay Matty – 87%
   - Diddy carter – b+
   - Coin hunter – gem
   - Icoreviews – 88.49%
   - Crypto wolves-lambo (860 hp)
   - The kript keeper-84.13%
   - Darkwing duck-81%
   - Swish spreedsheet-80%

   Hacked – *"Tolar project has an excellent chance of doing well this year"*
   Crypto rand – *" a solution that solves major shortcomings of blockchain technology, while maintaining all of its advantages."*
5. In top 3 highest rated ICO's. Ranking is based on average scores achieved from many ICO review websites and prominent crypto influencers (10 reviews or more).
6. Great code review by Andre Cronje.
7. Great new tech with amazing speed and low energy consumption.
8. Long term project with huge development and scalability potential.
9. Platform adapted to governments, multinationals, ICOs.
10. Fair approach to all investors. Hard cap 45000 eth, max bonus 20%.

14. TOLAR PRESALE, ICO AND TOKEN METRICS

14.1. Presale

Presale will be running until the end of August.

How to participate in presale?

- In order to register, visit https://www.tolar.io/presale/
- In case of acceptance, you will receive a confirmation e-mail from tol@tolar.io with further instructions
- Our e-mail contains link which will lead you to our password protected web https://www.tolar.io
- This webpage will have our ETH address and video with 4 Tolar management members which additionally show our ETH address
- We are never sending our ETH address via email. Our ETH address is only visible on our website

14.2. ICO

ICO will start on September 15, 2018 at 14:00 GMT and it will end on September 20, 2018 at 14:00 GMT, or before if hard cap is reached.

14.3. Token Economics

- Token name: Tolar (TOL)
- Hard cap: 45,000 ETH
- Soft cap: 20,000 ETH (already reached)
- Total supply of TolarZ generated: 1,000,000,000
- Private sale bonus: 20%
- Presale bonus:10%

Prices in ETH for presale are as follows:

- For contributions of more than 50 ETH price is 0,000120879 ETH per TOL (20% bonus included in price)
- For contributions between 10-49 ETH price is 0,000131868 ETH per TOL (10% bonus included in price)
- ICO price and presale price for 1-9 ETH - 0,000145055 ETH per TOL

How much TOL do you get for 1 ETH in presale?

- If you contribute more than 50ETH for 1 ETH you will get 8,272.74 TOL
- For contributions between 10-49 ETH for 1 ETH you will get 7,583.34 TOL
- For contributions between 1-9 ETH for 1 ETH you will get 6,893.94 TOL

14.4. Token Allocation

- 35% Investors (40% Private sale, 35% Presale and 25% Public ICO)
- 20% Founders
- 32% Tolar Development Fund
- 8% Proof of Stake Network Start Nodes
- 2,5% Developers
- 2,5% Advisors

14.5. Token lock

- 35% Investors: No lock on main tokens, 3 Months after ICO for bonus tokens
- 20% Founders: 36 months after ICO with 5% vesting possible after 24 months
- 32% TOLAR Development Fond: 36 months with 5% vesting possible after 12 months
- 8% Proof of Stake Network Start Nodes: 36 months after ICO
- 2,5% Developers: 24 months after ICO
- 2,5% Advisors: 24 months after ICO

14.6. Funds distribution

- 55% for carrying out operations
- 30% goes to the research and development team
- 10 % is allocated for the marketing campaigns
- 5% for conducting legal compliance

Gas price recommendations:

Check current gas price on https://ethgasstation.info

TOLAR ICO GRAPH DATA:	% OF TOTAL TOKENS	TOKENS
Private sale	14%	140.000.000
Pre-sale	12,25%	122.500.000
ICO	8,75%	87.500.000
Founders	20%	200.000.000
Developers	2,50%	25.000.000
Advisors	2,50%	25.000.000
Proof of Stake network start nodes	8%	80.000.000
Tolar Development Fund	32%	320.000.000

- Private sale
- Pre-sale
- ICO
- Founders
- Developers
- Advisors
- Proof of Stake network start nodes
- Tolar Development fund
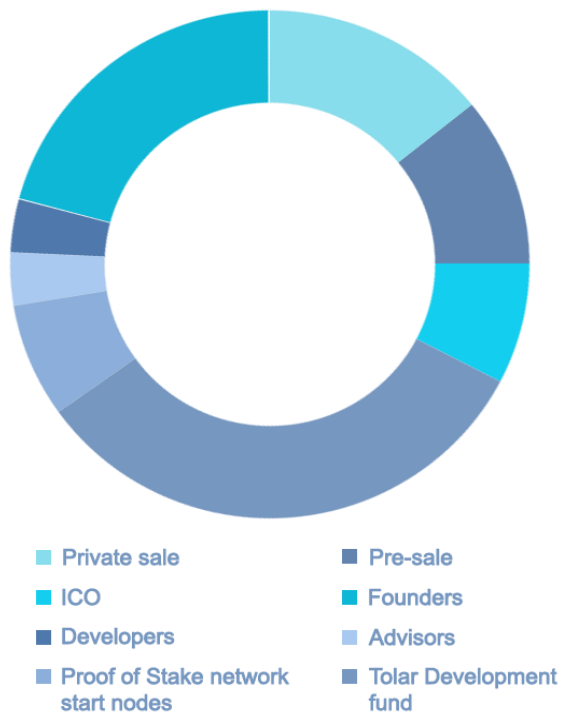
15. FAQ

15.1. Technology

What is HashNET?

HashNET is scalable, efficient and high-impact decentralised solution to social innovation challenges leveraging Distributed Ledger Technology (DLT). This revolutionary algorithm features faster transaction time, masternodes and will have a community governed cryptocurrency – Tolar.

Can Tolar become a major payment network?

Yes, Tolar is designed to become worldwide payment network from the start.

Can you tell us some future plans?

We want to compete with Ethereum and Hyperledger. Our goal is to offer faster, more scalable solution featuring masternodes and proof of stake.

What are the HashNET consensus mechanics?

Each member of the network has a copy of the HashNET - information structure that keeps record of who propagated which event to whom, and in what sequence. Those events are spread between HashNET members using gossip protocol and the validity of events is decided by voting. However, in order to increase speed and reduce bandwidth needed, every member that has a copy of HashNET can calculate what would be the vote that other member sent to him and if they had been running a traditional Byzantine agreement protocol that involved sending actual votes.

Is Tolar a smart contract platform just like ETH?

Yes. On the top of HashNet we will deploy Ethereum Virtual Machine.

Do you have a GitHub?

Yes, but it is not yet open to public. We will announce it once it happens.

Do you have some MVP?

We had a live demonstration of our prototype on June 28 with more than 150.000 TPS on multiple nodes.

How is interchain support implemented?
Interchain support will be done through contracts running on top of HashNET.

When is mainnet schedule?
Q2 2019.

Will Tolar launch first as an ERC 20 or straight to MainNet?
ERC 20.

MainNet launch Q2 2019, will we receive ERC20 token until MainNet?
There will be ERC20 tokens issued before native token.

Will you have a blockchain mainnet and then change it to another technology?
We now have a custom Blockchain testnet and for ICO ERC-20.

On what platform will you issue tokens?
We will issue ERC20 tokens as placeholder tokens at ICO and then exchange for mainnet tokens when mainnet is released.

When do you plan to have token tradable?
It is planned for after ICO, and ICO is will start .

Where can I see whitepaper?
You can see our whitepaper on our website tolar.io.

Is Tolar the first currency being built on HashNet infrastructure?
Yes, it is.

Is this an infrastructure project?
HashNet is infrastructure project that will allow people to build dApps.

15.2. Sale and presale

What sale phases will you have?
Private sale, Presale and ICO phase

Did you start the airdrop campaign?
No.

Any excluded countries?
Yes. USA and China.

What do you need 45,000 ETH for?
We want to globally scale HashNET with different solutions for enterprises and governments. We also want to position Tolar HashNET at the top of all DLTs. On the other hand, the competition is fierce, and they have much more money than 45,000 ETH.

When are the main tokens tradable?
After ICO when they come to first exchange

Who can I speak to about public sale?
You can find all the information on our web or PM our admins on Telegram and by sending email to info@tolar.io

Do you have KYC process?
Yes. Presale and whitelist process for ICO is now open. KYC form can be accessed through our official website.

When are we likely to get the KYC email regarding the private sale or presale from the application?
KYC process is currently on for presale and ICO whitelist. If you applied, you will get an email soon.

Will there be a different KYC process for presale and ICO?
It is the same.

When is TGE?
In ICO time.

What will happen to unsold tokens?
We will keep them for business development.

Where can we send a business proposal?
Send an email to info@tolar.io

15.3. Masternodes

Will masternode owners receive rewards?
Yes, they will be rewarded for helping secure the network.

When will masternode go live?
We cannot confirm that at the moment, so please stay tuned. We will inform you.

What are the server requirements for owning a masternode?
Server in this case is computer or computing-cluster connected to a network which provides masternode services mentioned above.

Minimum requirements for server are:
- quad core 64bit processor
- 16 GB RAM
- 128 GB of available disk space
- 50 Mbps symmetrical internet connection
- Fixed and unique IP (only one masternode can run at one IP address)

While these are minimum requirements, it's recommended to have masternode on a better configuration, especially in higher network load scenarios. In case that your masternode starts lagging behind because of insufficient processing power or bandwidth, it will not receive masternode rewards for those rounds.

What will be the reward for masternode owners?
It is described in whitepaper.

Can I earn rewards even if I am not the owner of masternode?

Yes, but there will be significant difference in rewards.

How many coins for the masternode?
You will need 500,000 TOL

What will be the maximum number of masternodes?
System can tolerate any number of nodes that connect to it. For regular node, there are no special requirements, you just download Tolar client and connect to the network. As for masternodes you are required to lock up 500,000 TOL. And total supply is 1,000,000,000 TOL. Whole supply will probably never be in masternodes. Technically it is not a problem to have more than 10,000 masternodes without performance lost. At this point we are sure about huge power savings compared to PoW currencies.

What's the purpose of arbitrary nodes? Who and how decides who'll be arbiter in the network? And how many arbitrary nodes does network need?
The arbitrary number of masternodes provides much better decentralization of the network. To be clear, there are no nodes acting as arbiters, the number of nodes can be arbitrary.

Where can I get info about masternodes? If there is one group of masternodes confirming everybody's transactions and executing all the smart contracts then it's not really a DAG, is it?
It is a DAG because a masternode collects transactions in their pool and then sends it to a random node. As the network events propagate through the network, they create a DAG locally on every master node, which is eventually consistent across the network and based on that DAG. Every masternode can calculate the same states as every other network without trusting others.

What is the role of regular nodes to propagate transactions through the network?
Regular nodes will also be able to do staking however, if they choose to do so, their reward percentage is less than that of masternodes. However, if they don't decide to stake anything, then yes, they will just propagate events and verify correctness of graph.

15.4. HashNET vs. Hashgraph

What is the difference?
The main difference is that HashNET is a proof of stake public ledger which doesn't have a fixed of number of masternodes and which is actually decentralized. Moreover, we are adding a governance system on top, where masternodes can vote on the future of the ledger. The way nodes are coming to consensus is different because of an arbitrary number of masternodes. Anyone who has enough stake for the master and the tech requirements can be a masternode. Hedera Hashgraph has a council composed of 39 preselected big companies that decide on funds and network future. In Tolar network, any member of community running a masternode can propose tenders and vote for them. Also, our voting mechanism is different since it includes weighted votes proportional to stake and a reputation mechanism. For Hashgraph to function, it needs to know the number of nodes in the network in advance, that's why it was initially intended for permissioned networks only. Our algorithm doesn't need to know number of nodes in the network in advance, on the contrary, you can join or leave any time you want. That's why we started the project as a public ledger. Our project will be open-source where you can see exactly what's happening, while Hashgraph is closed source.

Has a license been obtained from Hashgraph (Swirlds Ink)?
There are enough differences in our algorithm not to warrant any special licensing.

Are you using the same technology as Hashgraph but open source?
Similar tech but better algorithms, HashNET is a public proof of stake ledger with arbitrary number of masternodes with a governance and a reputation system.

15.5. Technical

How come you don't just use Rust and minimize your security issues?
We are more comfortable using c++ because all our developers are experienced in c++ and we use best practices to make sure that doesn't happen. But we use go as well for the more high-level stuff and networking.

How many TPS were you able to achieve on your testnet and how many TPS are expected to be achieved in HashNET mainnet?
200K is the theoretical number we calculated that is possible to achieve but right now we can confirm that we showcase more than 150K TPS on multiple nodes. We will continue to improve and optimise our algorithm until we can achieve our maximum.

Are you more decentralized than Ripple and less decentralized than BTC?
Ripple is probably the one which is the most centralized. So, the answer is yes, it is hard to say how much is BTC really decentralized. We want to provide a really decentralized ledger which has a masternode governance system and where the majority stakers can vote on the changes.

What programming language do you use?
We are using both c++ and go. Go is used for the high- level networking layer, all other stuff, which is computationally heavy and can be optimized, is in c++.

What are the implications of using C++ or Java? What are pros and cons?
C++ is much more efficient, and we can dig into the low-level stuff to optimize everything from memory management, execution speed, etc. Also, as we are solving algorithmic problems on a high number of nodes, c++ provides us with the ability to optimize many things on the data structures we are using, and, in that way, we can achieve better throughput than many others.

In what ways is this coin different from all other PoS with Masternodes, they are all cheap, fast and scalable?
We are also fair in a sense that there are no blocks, so miners and masternodes cannot decide on the order of transactions. Time to finality is a few seconds. In addition to all of that, there is a virtual machine on top, making it possible to run smart contracts and dApps without hitting performance limits any time soon.

How do you plan to showcase the progress of TPS for the network as progress is being made?
At first, tests will be run on developer's network, where we can deploy several dozens of masternodes and nodes that will be sending large pools of random transactions. Results of our developers testing will be periodically published on our Medium and other channels (Telegram,

FB, Twitter, LN). Since we plan to switch repository to public mode, anyone with some technical or developer experience should be able to replicate our test setup and verify the numbers for himself, if he wishes. Also, as the program interface gets more user-friendly, we will start HashNET testnet, were even non-technical users will be able to try out everything they want.

When could we start to study and develop dApps on testnet?
DApps, as per roadmap, will come at later point (after HashNET protocol is fully implemented).

Will the formal verification be out on Arxi or just on the whitepaper?
We are still deciding on it, but if it turns out to be significant scientific article, we will publish it and make it available on Arxiv as well.

15.6. Business

Do you have official announcement channel on Telegram?
Yes, our official announcement Telegram channel can be accessed here: https://t.me/tolario

In which country is the company based?
Legal entities that run Tolar HashNET project are based in Slovenia and Croatia.

Will you translate whitepaper to other languages?
Yes.

16. REFERENCES

[1] Jelasity M., Montresor A. and Babaoglu O. 2005. **Gossip-based aggregation in large dynamic networks.** ACM Trans. Comput. Syst. 23, 3 (August 2005), 219-252.
DOI=http://dx.doi.org/10.1145/1082469.1082470

[2] Allavena A., Demers A., and Hopcroft J. 2005. **Correctness of a gossip based membership protocol.** In Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing (PODC '05). ACM, New York, NY, USA, 292-301.
DOI: https://doi.org/10.1145/1073814.1073871

[3] **Hash pointers and data structures**, http://learningspot.altervista.org/hash-pointers-and-data-structures/, retrieved 23.03.2018.

[4] Rogaway P., Shrimpton T. (2004) **Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance**. In: Roy B., Meier W. (eds) Fast Software Encryption. FSE 2004. Lecture Notes in Computer Science, vol 3017. Springer, Berlin, Heidelberg

[5] Coron JS., Dodis Y., Malinaud C., Puniya P. (2005) **Merkle-Damgård Revisited: How to Construct a Hash Function.** In: Shoup V. (eds) Advances in Cryptology – CRYPTO 2005. CRYPTO 2005. Lecture Notes in Computer Science, vol 3621. Springer, Berlin, Heidelberg

[6] Wing-Hei Luk V., Kai-Sun Wong A., Chin-Tau Lea, Wentao Ouyang R., **RRG: redundancy reduced gossip protocol for real-time N-to-N dynamic group communication**, *Journal of Internet Services and Applications* 2013 4:14

[7] Correia M. M., Veronese G. S., Neves N. F., and Verissimo P. **Byzantine consensus in asynchronous message-passing systems: a survey. International Journal of Critical Computer-Based Systems**, 2(2):141–161, 2011.

[8] Leemon B. **The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance**, *SWIRLDS TECHREPORT SWIRLDS-TR-2016-01, 2016.*

[9] **PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake**, https://pdfs.semanticscholar.org/0db3/8d32069f3341d34c35085dc009a85ba13c13.pdf

[10] Bentov I., Gabizon A., Mizrahi A.: **Cryptocurrencies without proof of work**. CoRR, abs/1406.5694 (2014)

[11] Kiayias A., Russell A., David B., Oliynykov R. (2017) **Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol**. In: Katz J., Shacham H. (eds) Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science, vol 10401. Springer, Cham

[12] Damiani E., De Capitani di Vimercati, Paraboschi S., Samarati P., and Violante F. 2002. **A reputation-based approach for choosing reliable resources in peer-to-peer networks.** In Proceedings of the 9th ACM conference on Computer and communications security (CCS '02), Vijay Atluri (Ed.). ACM, New York, NY, USA, 207-216. DOI=http://dx.doi.org/10.1145/586110.586138

[13] Cachin C., Vukolić M., **Blockchain Consensus Protocols in the Wild,** https://arxiv.org/abs/1707.01873v2

[14] Tom Elvis Jedusor, **MimbleWimble**, July 2016, https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt

[15] Mouton Y. H., **Increasing Anonymity in Bitcoin**, retrieved on 18.02.2018. https://download.wpsoftware.net/bitcoin/wizardry/horasyuanmouton-owas.pdf

[16] Fischer M. J., Lynch N. A., and Paterson M. S. **Impossibility of distributed consensus with one faulty process**. Journal of the ACM, 32(2):374–382, Apr. 1985.

[17] Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Review, 41(2):303–332, jan 1999.