HashNET Blockchain Consensus for DLT Applications

.

ABSTRACT

Our modern world is becoming increasingly reliant on the processing, exchange and storage of information. This trend of so-called "digitalisation" is penetrating every pore of human civilisation, including nature, people, and machines; our economy and production, which must be as local as possible; and our global ecology. The use of information processing technology brings benefits to a wide range of endeavours. In this sense, many computing technologies and techniques must be used to achieve the goal of an integrated global service ecosystem, a Rainbow ecosystem of all hierarchical levels of computing.

One of the most important new developments in recent years is the development of blockchain technology. A blockchain can solve many problems of persistent and traceable storage, as well as enable direct coordination, compensation, etc. Therefore, in the Dew-Fog-Cloud hierarchy, blockchain technology is a promising new approach to enable novel applications in a variety of fields, from social and educational to scientific and industrial.

However, there are two important points in many implementations of the current blockchain which prevent them from being used for public service solutions. The first is the proof algorithm - the vast majority of proof-of-work algorithms do useless work and waste enormous amounts of energy. The second one is that proof-of-stake algorithm is not suitable for open public infrastructure.

The HashNET algorithm, which uses proof-of-authority combined with master nodes to achieve distributed consensus and ensure trust, is explained in detail in this paper.

As an example of future applications in science, education and society, we also briefly describe certificate validation and future application for scientific publications.

Keywords: distributed ledger, blockchain infrastructure, HashNet consensus, EBSI

1. INTRODUCTION

The development of modern civilisation, science, economy and society is based on real and fast information flow and availability. In the age of universal digitalisation, the phenomenon of distribution and parallelisation of procedures appears as a technical approach to the complexity of natural systems. In this context, network computing is emerging with the aim of creating secure information and processing flows using data and data deriven information as an important resource for the search for knowledge and innovative solutions, products and services. Following this evolution of digitalisation, the development of Blockchain technology began to influence the future of business and society, especially in the circular economy.

Blockchain technology implements shared and transparent data storage in a secure database that can only be accessed by authorised network members. Since it is a parallel distributed storage, the network members share a single view of true data, i.e. all of them can fully see all the details of the transactions, providing a system with new data processing capabilities and advanced security services. The established Blockchain network can track orders, payments, invoices, documents, votes, publications, decisions, production processes, etc.

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

With the advent of blockchain technology, the financial sector has shown intense development with the emergence of cryptocurrencies and secure transactions [1,2]. The blockchain is essentially a decentralised, distributed, replicated database. All transactions in the network are monitored by replication on all participating nodes [3]. The foundation is a distributed consensus protocol running on each node of the network that manages message exchange and local decision making to achieve consistency of information or data across the active nodes of the network. It is based on a consensus protocol, i.e., a set of rules by which active nodes determine the validity of transactions [4]. It enables collective monitoring and securing of the apparent shared transaction ledger.

On the database platform, the blockchain monitors data transactions in an ongoing and edited form to provide evidence against unauthorised changes to the content [5]. The term blockchain refers to distributed records of transactions within networks that are stored on nodes in a data format known as a "block." A sequential set of blocks linked with hash pointers in ascending order is called a chain of blocks. In a public blockchain network, there is no centralised authorisation point, interested participants (nodes) can join without any restrictions. In this way, a large number of nodes can participate in the consensus process [6,7].

As mentioned earlier, the initiator of blockchain technology is a process mechanism called consensus protocol. These protocols create a decision about which node may add a new block to the chain. Consensus protocols are divided into two main groups:

- evidence-based consensus protocols, which require entities to provide evidence of actions or resource consumption, and
- consensus voting-based protocols, where entities participating in the network exchange their new blocks or transaction verification results before making a final decision on which node may introduce a new block into the chain [8].

These main consensus protocols include Proof of Work (PoW) [9] or Proof of Stake (PoS) [10] and their derivatives [11].

The most famous application of blockchain technology is the cryptocurrency Bitcoin [12]. Transactions are signed with the private key of the address and sent to all other nodes in the network for verification. The records of these transactions are stored in the blocks. Participating nodes cannot delete the block, but they can add new blocks. The chaining of these blocks creates a shared, distributed database with an immensely growing list of transaction records that are irreversible and immutable. In practice, it is impossible to change the contents of the blocks, and other nodes cannot detect such a change [13]. Thus, a decentralised database is created, which is jointly managed by all participants (entities) of the network.

2. PROOF OF AUTHORITY

A major problem in the use of blockchain technology is the “proof”, by which transactions, ergo new chained blocks, are validated. Several methods exist to this effect. The main characteristic of the blockchain is its immutability after a certain block is validated. Actually, we can regard this technology as a way of simulating the behaviour of matter in the information space. However, the main problem of such simulation is that the viability of the blockchain disappears the moment no new validations (by “proof”) are done. Therefore to continue to be viable, constant new “proofs” have to be generated. In this sense, the blockchain has only past validity, as its future is always dependent on the already executed future “proof”. This is opposed to real matter, whose existence is (generally) guaranteed in the future.

Early (and still a lot of) blockchain solutions use for the “proof” “Proof of Work” (PoW), the idea being that by investing a certain amount of work (computer time), the blockchain gains a certain “material” property, which in turn allows it to be expanded in a controlled way. At the beginning of this technology this was an obvious choice, and it was hard to imagine then

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

that computer time translates directly into energy consumption and that the huge pressure of more and more blockchain initiatives, and the extreme crypto market speculations and manipulations would push the amount of computing work necessary for a proof of block into global ecosystem threatening energy consumption figures. Just for example, to be viable, Bitcoin proof of work uses 123.55 TWh electrical energy per year (data from March 2021) [14]. That is constant consumption of 14.1 GW, which is enough power to energise 7,000,000 (seven million) electrical water boilers (per 2 kW). Productionwise this is the amount of electric energy which would be generated by approx. 28 Slovenian-Croatian nuclear plants in Krško.

To avoid this huge energy cost of Proof of Work (PoW) algorithms and improve security and privacy, Proof of Stake (PoS) [15] was introduced with certain tokens. The PoS consensus relies on the fact that certain “players” invest a specific resource in exchange for a certain amount of respective tokens, and that, by this investment, they are interested enough in keeping that blockchain (distributed ledger) uncompromised.

However, for democratic applications (like social brainstorming, collective decision making, voting etc.) the Proof of Stake is not a viable approach, as democratic applications must not be under the stress of a possibility that a certain amount of rich stakeholders take over the blockchain, therefore being able to directly influence those processes. Therefore we describe the HashNET algorithm and an appropriate infrastructure using the Proof of Authority (PoA), where transactions and blocks are approved by validators [16]. Theoretically, the PoA is the same as PoS, but with appointed equal stakeholders, with a stake of 1 each. The stakeholding appointees are trusted public institutions (educational, scientific, governmental).

3. NATIONAL AND EU BLOCKCHAIN SERVICE INFRASTRUCTURE

The HashNET algorithm requires trusted public institutions to provide the proof of authority necessary for the proper maintenance and use of the Blockchain. This allows the blockchain testing infrastructure of Si-Chain, CroBSI, and EBSI to be a public service maintained primarily by the academic community and individual interested partners from industry and society. This is achieved by Si-Chain and CroBSI being part of other existing infrastructures that integrate with the European Blockchain Service Infrastructure (EBSI), on which the Blockchain-as-a-Service (BaaS) approach is supported, enabling the building and deployment of blockchain applications. These services are a new development in the growing field of blockchain technology. The application of blockchain technology started with cryptocurrency transactions and expanded to secure transactions of all kinds. Therefore, there is a high demand for hosting services.

Blockchain-as-a-Service (BaaS) is part of the cloud infrastructure for customers who create and manage blockchain applications.

BaaS works similarly to a web host that performs back-end operations for a blockchain-based application or platform.

PoA is used instead of PoW or PoS - as explained earlier, this is more suitable for a public blockchain infrastructure.

The network consists of:

Masternodes - nodes that participate in consensus voting/computation, including maintaining and validating the full blockchain.

Full nodes - nodes that do not participate in consensus voting but keep and validate the full blockchain

Thin nodes - end-user clients that trust master nodes but do not participate in consensus themselves, nor do they keep full blockchain data. Convenient for users to interact via client

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

applications (e.g., desktop or mobile "wallet," scientific publishing, voting and decision making, logistics, etc.) without requiring specialised hardware or large amounts of storage.

Alerting/logging infrastructure - monitoring and alerting solutions that ensure the network is running without problems and alert support personnel when issues arise.

HashNET, an innovative consensus platform originally developed to operate on an unauthorised public network. It provides a novel solution to the computational and communication difficulties of managing large public distributed ledgers.

HashNET-based blockchain platforms include the Ethereum Virtual Machine (EVM), which allows applications written in Solidity for EVM to run on HashNET or to develop new, necessary smart contracts to define relationships and transactions between actors in social, environmental, and industrial applications.

4. HASHNET CONSENSUS ALGORITHM

One of the primary goals in designing HashNET is a significant reduction of computational and communication resources needed to operate and maintain the system. With this goal in mind, we propose an Improved Redundancy Reduced Gossip (Improved RRG) protocol for information transfer on a suitably designed network [17]. 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. This chapter will provide a detailed description of the main features and properties of the HashNET consensus protocol.

4.1 HashNET overview

Each node in the network keeps a representation of the HashNET in its memory. The HashNET that each node has can differ, but through the process of gossip, the yet, to the node, unknown events are added to its HashNET representation.

Next, we need to introduce the term of an event object as a data structure created by some node and containing the two hashes of the preceding events – one of the parent event created by the same node ("self-parent") and one of the parent event created by some other node ("other-parent"). The node that is the creator of the transaction also puts a timestamp to the event object at the creation time, and the event is thus digitally signed. Each event object can optionally contain zero or more transactions making the event a container for those transactions. When the event gets gossiped (as explained in the next paragraph) the signature is sent along with it. Events can have zero transactions either when a node receives a sync event (HashNET difference) or when the node has just been spawned, thus creating the first event with no self-parent and no other-parent, and there are no pending transactions that this node is aware of in its transaction pool.

The goal of the HashNET algorithm is for nodes in the network to come to a consensus. The consensus is defined as agreement on the order of events. Furthermore, by agreeing on the timestamps for each event, the order and timestamps for each transaction are determined as well. Nodes can call each other at random for syncing and determining which events they don't have recorded yet in their instance of the graph. This process is called "gossiping" and can be illustrated in the following example. Let us assume that nodes are named Bob, Dave, and Alice. Before nodes send each other the event-difference, Bob first tells Dave how many events were created by each node he has a record of, and Dave communicates to Bob the same from his point of view. For example, if Bob has 13 events by Alice and Dave has 10, then Bob sends Alice's last 3 events.

4.2 Building the HashNET graph

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

As nodes send out events to each other while gossiping, the directed acyclic graph connecting the nodes will grow. The graph is called HashNET because cryptographic hashes connect it. The entire graph is cryptographically secure since each event (vertex in the graph) contains the hashes of the events below it and it is digitally signed by the creator. The graph can always grow, but older parts are immutable.

If two nodes, in our example called Alice and Bob, contain the same event X in each of its HashNET representation, both Alice's HashNET and Bob's HashNET, it is guaranteed by digital signatures that all parent events from the event X in both HashNET representations are the same. This property is called the consistency of the HashNET.

Each event belongs to a group of events based on the round in which it was created. Let us define a round-created event as R, where R is the maximum of the round-created event by its parents. Round-created is R+1 if the event can strongly see a hyper-majority (true if at least 2/3 of stake pass a given requirement) of round R sentinels (sentinel is the first event created by a node in each round):

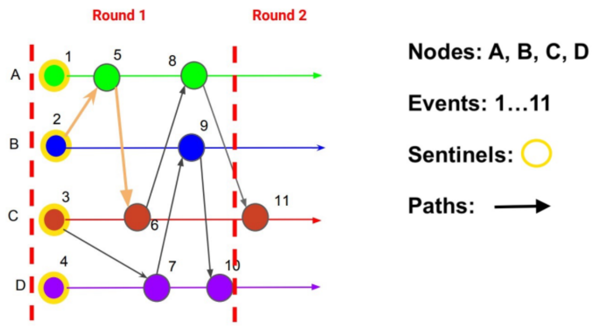
4.2.1 Function CalculateRoundCreated

Let S be a set of events that node A received from node B that node A is not yet aware of (HashNET difference determined from gossiping):

```
for each event x in S {
r max(round-created of self parent, round-created of other parent) or (1 if none parents exist)
if x can strongly see a hyper-majority of round r sentinels {
//see definition of StronglySees function in the next paragraph)
 x.round_created r + 1
} else {
 x.round_created r
}
x.is_sentinel (x has no self parent) or (x.round_created > x.self_parent.round_created)
}
```

4.2.2 Direct and Hyper path

The direct path exists if there exists any graph path in the directed acyclic graph. In Figure 2 there is a direct path from Event 2 to Event 6.

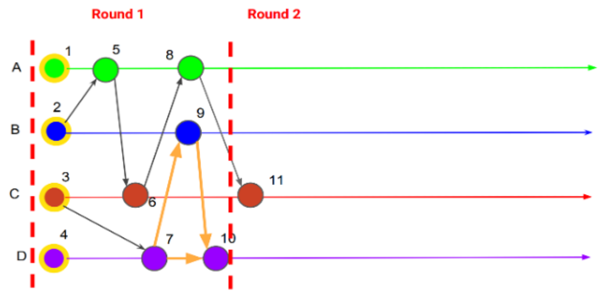


2 has direct path to 6

Fig. 1. Example of a single direct path

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

In Figure 2 there is also a direct path from Event 7 to Event 10. In this case, there are two different paths.



7 has direct path to 10

Fig. 2. Example of more direct paths

An event X strongly sees event Y if they are connected by multiple directed paths passing through a hyper-majority of nodes.

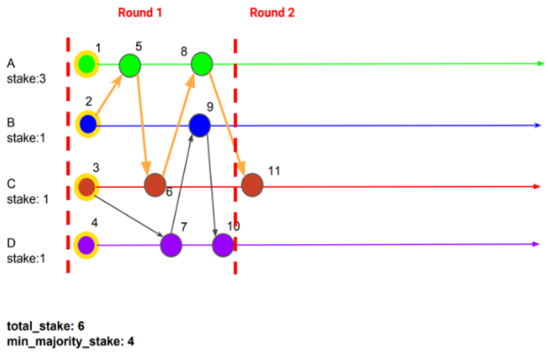
Stake in this context is the amount of cryptocurrency native to the network, deposited by the node as collateral. As mentioned above, if the network is Proof-of-Authority based, the stake for each node is always 1.

4.2.3 Function StronglySees

S collect all nodes that are on a path from node X to node Y and insert them into this set
qualified_stake accumulate stake of each unique node
return IsHyperMajority(qualified_stake, total_stake)

For example, as shown in Figure 3, the path from 2 to 11 goes through nodes A, B and C. The sum of the stakes for all nodes which it has been through is 5.

A_stake = 3
B_stake = 1
C_stake = 1
min_majority_stake = ⅔ * total_stake
path_stake = A stake + B_stake + C_stake = 5
IF path_stake >= min_majority_stake: path is Hyper path.



* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

Fig. 3. Example of Hyper path

If an event has a Hyper path to a hyper-majority of round R sentinel stakes, a new round has happened. In Figure 3, sentinel 1 has a Hyper path to event 11, and its stake is considered. Sentinel 2 has a Hyper path to event 11, and its stake is considered. Sentinel 3 has a Hyper path to event 11, and its stake is considered. Sentinel 4 doesn't have a Hyper path to event 11 and its stake is not considered.

The sentinels considered stakes are total to the sum of A_stake, B_stake, and C_stake which equals 5. With the function defined as IsHyperMajority(considered_stake, total_stake) in this example we have IsHyperMajority(5, 6) which is true and a new round is created.

Now we can show the example with sentinels in Figure 4. Sentinel 15 has a Hyper path to event 14, and its stake is considered. Sentinel 15 also has a Hyper path to event 13, and its stake is considered. Sentinel 15 also has a Hyper path to event 11, and its stake is considered. Sentinel 15 doesn't have a Hyper path to event 12, and its stake is not considered.

IsHyperMajority(5, 6) returns a True, and a new round is created for event 15.

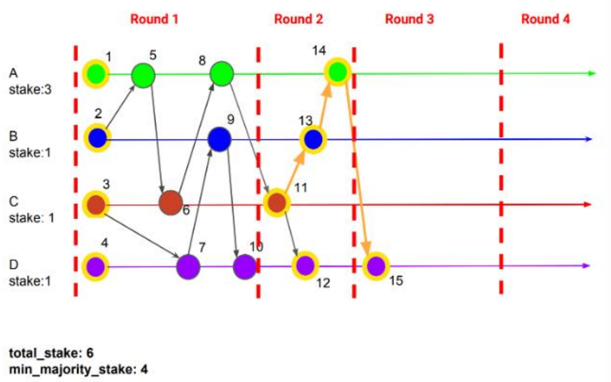


Fig. 4. Example of sentinels

4.2.4 Achieving consensus in a network

Consensus can be achieved by asking all nodes simple yes/no questions on whether an event X came before event Y. This can be done by running separate Byzantine agreement protocols which would require O(N log N) such questions. The much faster approach is to define some events as sentinels, and some sentinels to be wardens if most events see it fairly quickly after it is created. Then wardens can decide the simple yes/no question.

Whether a sentinel event X of a round R is a warden is determined earliest in round R+2 (and latest in the random round -> R + RANDOM_ROUND).

- For every sentinel event Y in R+1, a YES/NO vote is cast by event Y, based on event X seeing event Y (seeing means being an ancestor).
- Any sentinel event in R+2 (or later) collects votes from each sentinel event in round R+1 if a hyper-majority to the sentinel event Y in round R+1 exists (hyper-majority for this

case means that 2/3 of nodes are visited by going through a path or multiple paths from sentinel event in R+2 to sentinel event in R+1).

There is a well-known Sentinel theorem [18] showing that if any sentinel is able to make a yes/no decision, then that is the result of the election and it is guaranteed that all other sentinels that decide are going to decide the same way (the election for whether a sentinel is also a warden).

4.2.5 Function DecideWarden

```
for each sentinel X for which is not yet decided whether it’s also a warden {
  X.is_warden UNDECIDED
  for each sentinel Y starting from (Y.round_created = X.round_created + 1) {
    round_distance Y.round_created - X.round_created
    if (round_distance == 1) {
      y.vote (y sees x)
    } else {
    yes_stake 0
    no_stake 0
    for each sentinel Z in round Y.round_created-1 {
      if y.vote == yes and HasHyperPath from sentinel Z to sentinel X {
        yes_stake += Z.stake
      } else {
      no_stake += Z.stake
    }
  }
  vote (yes_stake >= no_stake)
  winning_stake (yes_stake >= no_stake ? yes_stake : no_stake)
  if (round_distance % RANDOM_ROUND > 0) {
    y.vote vote
    if (IsHyperMajority(winning_stake, total_stake)) {
      X.is_warden vote ? WARDEN : NOT_WARDEN
    }
  } else {
  if (IsHyperMajority(winning_stake, total_stake)) {
    y.vote vote
  } else {
  y.vote middleBit(sentinelY.whitened_signature)
}}}}}
```

Wardens are defined in the following way: For a round R sentinel, every R+1 sentinel is voting whether the sentinel is a warden or not. If an R+1 sentinel has a Direct path to the R sentinel, it votes that the sentinel is a warden. From Figure 5, for Event 11 all the sentinels from R=3 (15, 16 and 17) vote that he is a warden because they have a Direct path to the Event 11. For an event to be a warden, the votes (stake based) are then collected by the first sentinel from R+2 (Event 20). If the first sentinel in R+2 has a Hyper path to an R+1 sentinel, then its stake based vote is considered. Event 20 has a Hyper path to all R+1=3 sentinels (15, 16 and 17) and their votes are considered. The total vote they have equals 3. If the majority (not hyper-majority) votes “yes” then an event is a warden; therefore Event 11 is a warden.

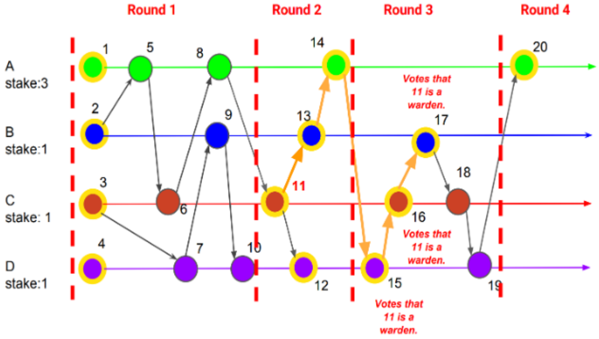


Fig. 5. Example of wardens

Once a round has the wardens decided for all of its sentinels, the round is received and a consensus timestamp can be determined. In order to get a consensus on an event, every warden has to see it (just ancestor, not function *StronglySees*). The round received for such an event is the round created by the warden.

The consensus timestamp is determined by going through each of the warden events and finding the earliest *event* T_i that is an ancestor of the warden and descendant of the event for which the timestamp is calculated. This is repeated for each warden, and *event* T_i timestamps are sorted at the end. The median is the consensus timestamp and the algorithm ends.

4.2.5 Function DecideConsensus

```
all_wardens_round last round that has all its sentinels decided whether they are wardens
for each event X {
  if X is an ancestor of every warden from all_wardens_round round {
    X.round_received all_wardens_round
    S set of all events Y where Y is a self-ancestor of all wardens from all_wardens_round and event X is an ancestor of Z but not of the self-parent of Z
    Z.consensus_timestamp median of all timestamps of events in S
  }}
return all events that have the round_received calculated, sorted by round_receieved; if there is a tie it is broken by the consensus timestamp. If a further tie happens, it is broken by a whitened signature.
```

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

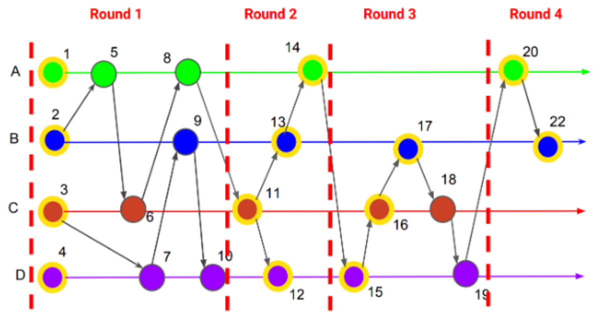


Fig. 6. Achieving consensus

Consensus can be achieved by deciding which events are wardens and which aren't. In Figure 6, all R=2 sentinels are wardens, but there can be cases in which they aren't. If all the wardens have a Direct path to an event, then the network has agreed on that event based on the consensus timestamp, which is determined by going through each of warden events and finding the earliest *event* T_i that is an ancestor of the warden and descendant of the event for which the timestamp is calculated. This is repeated for each warden, and then all *event* T_i timestamps are sorted. The median is the consensus timestamp.

5. HASHNET COMPATIBILITY STATUS

The HashNET platform is EVM compatible. EVM stands for the Ethereum Virtual Machine. Tolar is the native token of the HashNET platform. As all state changes happen through transactions, for which gas needs to be paid in the native Tolar token, the non-zero value of the token itself disincentivizes malicious behaviour, as economic losses would occur to actors misusing the network. In a broader sense, there are two types of transactions: simple value transfers and contract interactions. Contracts, also known as smart contracts, are Turing complete programs, through which more complex logic can be performed on the blockchain. In this sense, Tolar is compatible with the Ethereum platform, which is de-facto standard in DLT. Also, in 2021, there was a test performed to show compatibility with EBSI, in which standard APIs were shown to work as expected, such as: fetching blocks by index and hash, balance inquiries and verifying data existence on chain.

6. SCOPE OF APPLICATION AND GLOBAL PERSPECTIVE

A HashNET based infrastructure can be a catalyst that leads to wider penetration of blockchain technology into various social and industrial sectors in the form of secure service applications. ISO has approved a new standard for blockchain and distributed book technology (ISO / TC 307). In addition, cybersecurity legislation should be considered in integrated IoT-blockchain systems, such as the EU Directive on Network and Information Security (NIS), adopted by the European Union.

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

It is time to address the General Data Protection Regulation (GDPR) at a systematic level. Furthermore, the blockchain is structured around connecting people from different countries for whom there is no global compliance law so far. On the other hand, the IoT network is growing tremendously in terms of application types and number of devices. This has created many challenges that require urgent solutions in order to realise the full potential of IoT in the future. Blockchain technology has emerged as a distributed, unchanging transparent decentralised and secure technology that plays a promising role in many sectors. The characteristics and structure of the blockchain make it a strong candidate for solving IoT system problems by integration and adaptation through the Dew Computing paradigm [19]. The integration process has attracted the attention of many researchers who have devised various integrated IoT-Blockchain architectures and designs. However, none of the proposed studies was able to address most of the challenges, or to explore the full potential of the blockchain for benefits in the domain of IoT. Therefore, systematisation was approached through the Dew Computing paradigm.

Dew Computing allows for seamless integration of different information sources and processing levels, starting from the lowest, non-internet connected, elements, which must be fully self standing, but also ready to communicate and cooperate in the vertical distributed service hierarchy. The hierarchical extension from Dew, through the Edge/Fog layers, towards the Cloud, enables extremely wide heterogeneity of people/equipment/approaches, and also an important stratification of communication, processing and responsibilities. In the Dew Computing paradigm, the highest direct responsibility is on the lowest level of computing hierarchy, i.e. on the level of Dew. Theoretically speaking, the Dew droplets are in direct contact with the information space, which is the physical or intellectual space that the droplets are processing, reporting on or controlling.

The system described in this article is a major contribution to the future emerging Rainbow Global Information Services Environment [20] in the fields of ecology, economy, science and scientific collaboration, information dissemination and education, as well as society, particularly in the necessary development of direct democracy (public problem solving and solution finding, voting and direct governance).

We regard the Rainbow ecosystem as a fully recursive and hierarchically hyper-traversable non-dimensional space [21]. In this sense, we can think of Dew droplets as “neurons” of the Rainbow Global Information Services Environment.

The Rainbow ecosystem paradigm, i.e. the hierarchical integration of information processing levels, from Dew over Edge/Fog up to the Cloud, enables seamless integration of the emerging blockchain (DLT) infrastructure with a wide variety of future uses on a global scale.

Preliminary work on blockchain implementation from the aspect of Dew Computing was done recently [22].

It is envisaged that the Blockchain Service Infrastructure will be one of the major building blocks in this new integration towards a Local, Regional and Global Information Services Ecosystem.

As an example of a novel application that utilises the above thesis, we propose a new scientific publishing system which is designed to involve all features of the current publishing system but with some advancements, like categorising papers from various fields, defining a

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

predicted impact factor, as well as real valorisation of articles and reviews, and all participants in the publishing chain (editors, authors, reviewers). The publishing system should have the function of including authors and reviewers (as well as chairs and editors) in the valorisation system of rewards and records of contributions in the process. This can be achieved with virtual monetisation in the field of scientific publication.

The publishing platform can be managed and governed by a steering committee which is deployed as a variant of a Democratic Autonomous Organisation (DAO) [23], with the steering committee as the main decision making organisational unit. Although DAO as a governance model has its challenges, being a trustless model [24], we aim to enhance the model with few points-of-trust that will be represented as masternodes in the EBSII infrastructure. The proposed reward system is partially based on the European Alliance for Innovation (EAI) recognition scheme [25].

One of the first dapps (decentralized applications) on the HashNET platform was the Diploma app. Each diploma that gets issued and for which there is a need to be publicly verifiable on the public blockchain - which is a desired property, as diplomas are generally publicly available information - a QR code is attached to the digital version of the diploma (the pdf file). Next step is taking the hash of such pdf, and sending the hash through a transaction to a previously deployed smart contract on the Tolar HashNET blockchain. The contract itself has straightforward logic, it's basically a hashmap that holds all hashes of the diplomas. Only the contract admins can perform adding new hashes of diplomas, e.g. principle of a university. The admins can add new admins. The verification part can be checked by anyone, by simply checking the hashmap with the hash of a diploma you have at hand. The main goal of the Diploma app is preventing diploma forgeries. While such behaviour is highly unethical, it still happens, and the Diploma app on HashNET platform is a showcase for fighting it as data stored on the blockchain is public, open, censorship resistant and immutable.

7. CHALLENGES AND FUTURE WORK

After our civilisation had created and established the global, world wide flow of information, people and things, more than a decade ago Satoshi Nakamoto laid the foundations of blockchain technology that form the foundation of valuable connections and trust in the digital world.

Establishing trust mechanisms in digital technology is essential, and blockchain is a new platform that can significantly boost economic growth and ecological appropriateness. Therefore, the future of blockchain development is extremely important. The European Union has recognised that and launched systematic development within Horizon Europe and Digital Europe. A partnership on the European Blockchain Services Infrastructure (EBSI) is being opened, which is being established by integration of national infrastructures on a federal basis.

The development of blockchain technology will take place according to a specific scenario applicable under extremely safe conditions. That scenario has the following properties: multilateral interaction; credibility; intermediation; individuality; privacy.

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

It is assumed that a potential chain of blocks could improve industrial sectors, business processes, government structures, direct democracy as well as economic systems and the preservation of the global ecosystem as a whole.

In today’s time of many socio-economic and ecological crises, blockchains can bring transparency to opaque or corrupt systems, and the verifiability and immutability of processes. It ensures security and resilience on the vulnerable digital infrastructure, ensures the privacy of individuals while guaranteeing autonomy, and encourages cooperation building trust in society as a whole. The deepest impact of blockchain development could be found in the more subtle impacts on broad social values and structures.

Therefore, further development on a systematic and functional level creates a new step forward in our civilisation, and that requires great effort. The development should mobilise the huge intellectual capital that is developing on the establishment of a range of distributed service systems. Such general and specific (sub-)systems should become an operating platform for new service applications based on AI and cooperative systems using advanced blockchain platforms. This will lead to a new Industrial Revolution 5.0, the introduction of Circular Economy, and the global Ecosystem coordination, which will significantly positively change social relations and life on earth.

However, it is essential that in further development of all aspects of computer science and information technology we do not forget our huge responsibility towards the well being of nature and humans. Unfortunately, many past experiences have shown that often even well meaning ideas, intentions and developments proved to be harmful to a wider (eco-)system. This, as scientists, inventors, researchers and developers, we have to avoid at all costs.

8. CONCLUSIONS

In this paper, we have presented a novel HashNET algorithm based on the Proof-of-Authority (PoA).

PoA has significant advantages over previously used PoW and PoS algorithms, using trusted public institutions (educational, scientific, government) to control of the blockchain usage. The need for moving from the PoW to more efficient algorithms can also be seen with Ethereum, which is transitioning to PoS.

The HashNET algorithm is used to enable nodes to reach a consensus. As a core of the HashNET algorithm, we have proposed a novel Improved Redundancy Reduced Gossip algorithm, which lowers the traffic load while maintaining the same probability of successful delivery.

Envisaged usage of the presented service infrastructure includes industrial applications, social systems oriented applications and generic digital services for citizens where a secure distributed information database is needed to be trusted and transparent. Exemplary usage of the BaaS service is in the implementation of Dew Computing with blockchain architectures, democratic applications (social brainstorming, collective decision making, voting, etc.).

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

ACKNOWLEDGMENTS

This research has been supported by the European Regional Development Fund under the auspices of KK.01.1.01.0009 (DATACROSS) and the Ministry of Science and Education of the Republic of Croatia with the support of 533-19-15-0007 (Centre for Research Excellence in Data Science and Cooperative Systems).

REFERENCES

[1] Iansiti M, Lakhani KR. The truth about blockchain. Harv Bus Rev. 2017:95(1):118-127

[2] Yu J, Kozhaya D, Decouchant J, Esteves-Verissimo P. RepuCoin: Your Reputation Is Your Power. IEEE Trans Comput. 2019:68:1225–1237. doi:10.1109/tc.2019.2900648.

[3] Zou, J.; Ye, B.; Qu, L.; Wang, Y.; Orgun, M.A.; Li, L. A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services. IEEE Trans. Serv. Comput. 2019:12:429–445. doi:10.1109/tsc.2018.2823705.

[4] Alzahrani N, Bulusu N. Towards True Decentralization: A Blockchain Consensus Protocol Based on Game Theory and Randomness. In Lecture Notes in Computer Science. Springer International Publishing. 2018:465–485. doi:10.1007/978-3-030- 01554-1_27.

[5] Liu B, Liu M, Jiang X, Zhao F, Wang RA. Blockchain-Based Scheme for Secure Sharing of X-Ray Medical Images. In Security with Intelligent Computing and Big-data Services. Springer International Publishing, 2019:29–42. doi:10.1007/978-3-030-16946- 6_3.

[6] Domenico MD, Baronchelli A. The fragility of decentralised trustless socio-technical systems. EPJ Data Sci. 2019:8. doi:10.1140/epjds/s13688-018-0180-6.

[7] Yavuz E, Koc AK, Cabuk UC, Dalkilic G. Towards secure e-voting using ethereum blockchain. 6th ISDFS. IEEE. 2018. doi:10.1109/isdfs.2018.8355340.

[8] Nguyen GT, Kim KA. Survey about Consensus Algorithms Used in Blockchain. J. Inf. Process. Syst. 2018:14:101–128. doi:10.3745/JIPS.01.0024.

[9] Sharkey S, Tewari H. Alt-PoW: An Alternative Proof-of-Work Mechanism. DAPPCON. IEEE, 2019. doi:10.1109/dappcon.2019.00012.

[10] Puthal D, Mohanty SP. Proof of Authentication: IoT-Friendly Blockchains. IEEE Potentials. 2019:38:26–29. doi:10.1109/mpot.2018.2850541.

[11] Lu Y. Blockchain: A Survey on Functions, Applications and Open Issues. J. ind. integr. management 2018:25(05):1850015. doi:10.1142/s242486221850015x

[12] Chen Z, Chen S, Xu H, Hu B. A Security Authentication Scheme of 5G Ultra-Dense Network Based on Block Chain. IEEE Access 2018:6:55372–55379. doi:10.1109/access.2018.2871642.

[13] Shen C, Pena-Mora F. Blockchain for Cities—A Systematic Literature Review. IEEE 2018:6:76787–76819. doi:10.1109/access.2018.2880744.

[14] Digiconomist, Bitcoin Energy Consumption Index - Digiconomist, https://digiconomist.net/bitcoin-energy-consumption, accessed 31. May .2021

[15] Kiayias A, Russel A, David B, Oliynykov R. 'Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol'. Advances in Cryptology – CRYPTO 2017, edited by Jonathan Katz and Hovav Shacham, Springer International Publishing. 2017:10401:357–88. doi:10.1007/978-3-319-63688-7_12.

[17] Luk VWH, Wong AKS, Lea CT, Ouyang RW. RRG: redundancy reduced gossip protocol for real-time N-to-N dynamic group communication. J. Internet Serv. Appl. 2013:4(1):1-19.

[18] Cormen TH, Leiserson CE, Rivest RL, Stein, C. , Introduction to Algorithms, Third Edition, The MIT Press, Cambridge, Massachusetts; 2009

[19] Skala K, Davidović D, Afgan E, Sović I, Šojat Z. Scalable distributed computing hierarchy: cloud, fog and dew computing. OJCC. 2016:2(1):16-24. ISSN 2199-1987.

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.

[20] Skala K, Šojat Z. The Rainbow Global Service Ecosystem, DEWCOM 2018: The 3rd International Workshop on Dew Computing, Toronto, Canada; 2018.

[21] Šojat Z. From Dew Over Cloud Towards the Rainbow: Ecosystem of the Future: Nature—Human—Machine, In: Intelligence in Big Data Technologies—Beyond the Hype, Edition: Adv. Intell. Syst. Comput., Chapter: 1, Publisher: Springer Nature; 2020., doi: 10.1007/978-981-15-5285-4_1

[22] Wang Y. Dewblock: A Blockchain System Based on Dew Computing. Proceedings of The 3rd International Workshop on Dew Computing. 2018:34–38. DOI: 10.13140/RG.2.2.30585.31849.

[23] Chohan UW. The Decentralized Autonomous Organization and Governance Issues . Acessed December 4, 2017. http://dx.doi.org/10.2139/ssrn.3082055.

[24] Morrison R, Mazey NCHL and Wingreen SC. The DAO Controversy: The Case for a New Species of Corporate Governance? Front. Blockchain 2020:3:25. doi: 10.3389/fbloc.2020.00025.

[25] Anonymous, EAI Recognition - How it Works, https://eai.eu/#!/recognition/how-it-works, accessed 14 July 2021.

* Ruđer Bošković Institute, Centre for Informatics and Computing,
+385 98 209 816, E-mail skala@irb.hr.