

Rateless Coded Blockchain for Dynamic IoT Networks

Changlin Yang¹, *Member, IEEE*, Alexei Ashikhmin, *Fellow, IEEE*, Xiaodong Wang², *Fellow, IEEE*,
and Zibin Zheng³, *Fellow, IEEE*

Abstract—A key constraint that limits the implementation of blockchain in Internet of Things (IoT) is its large storage requirement resulting from the fact that each blockchain node has to store the entire blockchain. This increases the burden on blockchain nodes, and increases the communication overhead for new nodes joining the network since they have to copy the entire blockchain. In order to reduce storage requirements without compromising on system security and integrity, coded blockchains, based on error correcting codes with fixed rates and lengths, have been recently proposed. This approach, however, does not fit well with dynamic IoT networks in which nodes actively leave and join. In such dynamic blockchains, the existing coded blockchain approaches lead to high-communication overheads for new joining nodes and may have high-decoding failure probability. This article proposes a rateless coded blockchain with coding parameters adjusted to network conditions. Our goals are to minimize both the storage requirement at each blockchain node and the communication overhead for each new joining node, subject to a target decoding failure probability. We evaluate the proposed scheme in the context of real-world Bitcoin blockchain and show that both storage and communication overhead are reduced by 99.6% with a maximum 10^{-12} decoding failure probability.

Index Terms—Coded blockchain, decoding failure probability, dynamic Internet of Things (IoT) networks, rateless code, storage reduction.

I. INTRODUCTION

THE BLOCKCHAIN technology has found wide applications in Internet of Things (IoT) [1] due to its distributive, secure and integrated properties [2]. One of the key challenges that restricts the implementation of blockchain in IoT devices is the high-storage requirements for their users [3]. For example, a Bitcoin blockchain needs 380-GB hard-disk space in 2022 [4] and takes several days to download for a fully

functional Bitcoin core client [5]. This makes it hard for portable devices, such as smart phones and laptops, to serve as full nodes in a blockchain, which weakens the distributive property.

There are several ways to reduce the blockchain storage requirements, including simplified payment verification (SPV), pruning, and sharding [6]. An SPV client only stores the block headers and relies on the full nodes to verify transactions. The pruning scheme prunes old information that is not needed for verifying new blocks. However, the deleted information will eventually be inaccessible if all nodes employ pruning. The sharding approach divides nodes into groups and each group maintains a portion of the entire blockchain. However, the security level of the sharding approach is directly related to the group size [7]. Hence, all these solutions compromise on blockchain security or/and integrity.

Recently, coded blockchains have been proposed to reduce the blockchain storage requirements without loss of security and integrity [8], [9], [10], [11], [12]. They can also improve block propagation efficiency [13], [14], [15], [16]. In addition to storage and transmission cost reduction, the coded blockchains can improve the security of existing SPV client via fraud proofs [17], [18] or coded Merkle trees [19], [20], [21], and also the security of sharding solutions via coded shards [22], [23], [24], etc. In such blockchains, nodes encode the *data* of blocks using fixed rate error correction codes, such as Reed–Solomon codes [25], low-density parity-check (LDPC) codes [26], and polar codes [27], and distributively store the encoded blocks. In particular, a group of k blocks are encoded into n encoded blocks using an $[n, k]$ code. Then the storage at nodes reduces to about $1/k$ that of the replicated blockchain. When the *data* of a particular block is needed by a node, it can be recovered by collecting slightly more than k encoded blocks from other nodes and running a decoder of the error correction code. Nodes can encode only old blocks that are not needed for “mining,” which resembles the old block pruning approach, but without any loss of security and integrity.

In practice, an IoT blockchain network is dynamic and nodes frequently join or leave the network. Although for most of the time, the numbers of nodes joining and leaving are steady, sharp changes may occur sometimes. For example, the number of Bitcoin nodes dropped by 24% in September 2020 [28]. The encoding schemes in [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], and [24] are designed for networks with fixed number of

Manuscript received 29 August 2023; revised 23 September 2023; accepted 20 October 2023. Date of publication 8 November 2023; date of current version 7 March 2024. This work was supported in part by the National Key Research and Development Program of China under Grant 2023YFB2703600; in part by the National Natural Science Foundation of China under Grant 62032025; and in part by the Natural Science Foundation of Guangdong Province under Grant 2023A1515011474. (*Corresponding author: Zibin Zheng.*)

Changlin Yang and Zibin Zheng are with the School of Software Engineering, Sun Yat-sen University, Zhuhai 519000, Guangdong, China (e-mail: yangchlin6@mail.sysu.edu.cn; zhizbin@mail.sysu.edu.cn).

Alexei Ashikhmin is with the Communications and Statistical Sciences Research Department, Nokia Bell Laboratories, Murray Hill, NJ 07974 USA (e-mail: alexei.ashikhmin@nokia-bell-labs.com).

Xiaodong Wang is with the Electrical Engineering Department, Columbia University, New York, NY 10027 USA (e-mail: wangx@ee.columbia.edu).

Digital Object Identifier 10.1109/JIOT.2023.3328648

nodes, but some nodes can be temporarily unavailable. These encoding schemes are not well-suited for dynamic networks with the following reasons.

- 1) In a dynamic network, the number of nodes may rapidly change. Thus, using an $[n, k]$ code of a fixed length n becomes very inconvenient. In contrast, rateless codes is a natural solution for this scenario.
- 2) The nodes in a dynamic network often permanently leave the network. Thus, if we use a fixed length $[n, k]$ code, but many of the n nodes, that were available at the time of encoding, permanently leave, then other nodes will not be able to reconstruct these k blocks.
- 3) One possible way of using fixed length codes in a dynamic network is to use an $[N, k]$ code with length N significantly larger than the number of network nodes n . So, when a new node, say node $n + 1$, joins the network it can compute its own parity check symbol. However, in this approach, the new node first has to download more than k encoded blocks from other nodes to decode the k original blocks, which means very large communication overhead and high-decoding complexity. This problem does not exist in the proposed rateless coded blockchain.

Rateless Luby transform (LT) codes [29] were used to encode the blockchains in [30], [31], [32], and [33]. Moreover, an attempt of raptor code is discussed in [34]. However, the parameter k is fixed in these works and as a result these schemes do not well fit dynamical blockchains. In addition, most of these works use nonsystematic LT codes. This forces a new joining node first to decode all previously generated codewords. The number of these codewords can be very large since they contain almost entire blockchain and decoding of even a single codeword takes visible computational resources. Thus, this approach results in very large computational and communication resources needed for new nodes.

In this work, we use rateless raptor codes [35]. These codes have a low-decoding failure probability than LT codes [35]. We use systematic rateless codes such that the original blocks are also stored at some nodes in the network. Thus, when a node joins the network, it only needs to collect a few original blocks and encode its own parity check (or original) blocks for each group of previously encoded blocks. We adjust parameter k based on the network condition, which allows us to find a good tradeoff between storage efficiency and blockchain reliability. We propose to use novel *enhanced blocks* to store the coding parameters of each group of encoded blocks. We evaluate the proposed rateless coded blockchain in the Bitcoin network. The results show that by ensuring a less than 10^{-12} decoding failure probability, the node storage and the communication overheads needed by a new joining node both reduce to 0.4% as compared with the replicated blockchain.

This article addresses a critical challenge that has not been considered by previous coded blockchain studies: how to ensure successful decoding when the number of nodes in the network changes. In particular, all existing coded blockchain works use a predetermined information symbol length k . If sufficiently many nodes involved in encoding a particular codeword eventually leave the network, and this is a very possible event, it will be impossible to recover

these k information symbols. As a result, many blocks will be lost, which is not acceptable in most blockchain applications. Existing works do not have mechanism to update k . In this respect, this article makes the following contributions.

- 1) This article proposes a novel enhanced block structure that is built on top of a traditional block. Such enhanced block ensures the coded blockchain parameters, e.g., k , reach consensus in the system.
- 2) This article presents a network maintenance algorithm (NMA) for new joining nodes, to ensure the coded blocks stored in the system are sufficient for decoding.
- 3) This article proposes a novel method to update parameter k to ensure successful decoding in a dynamic blockchain network.
- 4) This article performs numerical simulations to show that the proposed scheme reduces the size of Bitcoin blockchain by 99.6% with a maximum 10^{-12} decoding failure probability.

The remainder of this article is organized as follows. Section II presents the background on coded blockchains and rateless codes. Section III gives an overview of the proposed rateless coded blockchain. Section IV presents the structure of our novel enhanced blocks. Sections V and VI present the protocol for a new node joining the network and our algorithm for choosing parameter k , respectively. Simulation results are given in Section VII. Finally, Section VIII concludes this article.

II. BACKGROUND ON CODED BLOCKCHAIN AND RATELESS CODE

A. Background on Coded Blockchain

In this section, we briefly describe how coded blockchains are organized in [9] and [10]. We will generalize this approach for the case of using rateless codes later in our work.

We use B to denote a block. Let W be the index of the last block, and B^W be the data of this block (that is the W th block without its header). Slightly abusing notation, in what follows we will be calling by block both entire block (data + header) and its data part B^W . Let α be a sufficiently large integer such that with high-probability blocks $0, 1, \dots, W - \alpha$ do not contain forks that would grow. These blocks are called *confirmed blocks*. In a coded blockchain the confirmed blocks are partitioned into M groups, each of which has been encoded by the fixed rate code, as it is shown in Fig. 1. Each group consists of k blocks and each block B^w is divided into s symbols over the finite field \mathbb{F}_q , denoted by \mathbf{b}_w . Assuming that the m th group has blocks with indices $\{w_1, w_2, \dots, w_k\}$, this group can be represented by a matrix with k columns, denoted by \mathbf{b}_{w_i} , and each column forms the corresponding original block of the group

$$\begin{bmatrix} b_{w_1,1} & b_{w_2,1} & \dots & b_{w_k,1} \\ b_{w_1,2} & b_{w_2,2} & \dots & b_{w_k,2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{w_1,s} & b_{w_2,s} & \dots & b_{w_k,s} \end{bmatrix}. \quad (1)$$

The k entries of each row of (1) are information symbols. Each information symbol is denoted by $b_{w_i,j}$, where $1 \leq i \leq k$

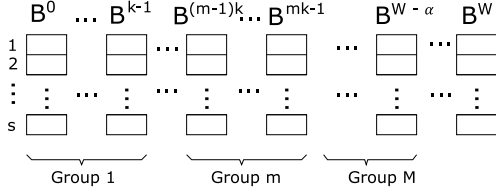


Fig. 1. Blocks are encoded by groups. Each group consists of k blocks. Each block is divided into s symbols.

and $1 \leq j \leq s$. So, each row of (1) is encoded into n coded symbols using a $[n, k]_q$ linear code over \mathbb{F}_q , where $q = 2^p$ and p is the number of bits in each symbol $b_{w_i, j}$, with a $k \times n$ generator matrix \mathbf{G} . The code length n is typically equal to the number of nodes in the network at the moment of encoding. The encoding is conducted by multiplication of each row of (1) by \mathbf{G} . As a result we obtain the encoding vector of the h th row of (1) as

$$[u_{1,h}, \dots, u_{n,h}] = [b_{w_1,h}, \dots, b_{w_k,h}] \mathbf{G}. \quad (2)$$

Thus, after encoding all rows of (1), we obtain the matrix

$$\begin{bmatrix} u_{1,1} & u_{2,1} & \dots & u_{k,1} & \dots & u_{n,1} \\ u_{1,2} & u_{2,2} & \dots & u_{k,2} & \dots & u_{n,2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ u_{1,s} & u_{2,s} & \dots & u_{k,s} & \dots & u_{n,s} \end{bmatrix}. \quad (3)$$

Each node stores only one column of (3), which greatly reduces the needed storage. We will denote the i th column of (3) by \mathbf{u}_i .

It is convenient to use systematic \mathbf{G} , such that the first k columns of \mathbf{G} form the identity matrix \mathbf{I}_k . In this case we have $\mathbf{u}_i = \mathbf{b}_{w_i}$, $i = 1, \dots, k$. If a node, say node j , needs block \mathbf{u}_i , for example for verifying a transaction, it broadcasts a request and obtains \mathbf{u}_i . If the node that stores \mathbf{u}_i is not available, then node j collects a few other columns of (3) and use a decoder of the $[n, k]_q$ code to repair \mathbf{u}_i [10]. On the other hand, when repairing in [10] fails or \mathbf{G} is a nonsystematic generator matrix, as in [9], node j needs to collect $(1 + \epsilon)k$ columns of (3) from other nodes and to decode all the information symbols $\mathbf{b}_{w_1} = \mathbf{u}_1, \dots, \mathbf{b}_{w_k} = \mathbf{u}_k$. Here, ϵ is the *decoding overhead* that varies for different codes.

B. Background on Rateless Codes

We now briefly review the rateless codes and their variances. By using the rateless codes, the transmitter uses n information symbols to generate potentially unlimited number of coded symbols, and sends them to one or more receivers. As soon as a receiver collects any $(1 + \epsilon)n$ coded symbols, it can decode, with a high probability of success, the n information symbols.

1) *LT Code* [29]: Let $\{u_1, \dots, u_n\}$ be n information symbols over \mathbb{F}_q , $q = 2^p$. The reason why we use the same notation u_i , that we used for coded symbols in the previous section, is that later we are going to combine a linear $[k, n]$ code and $[N, n]$ LT code to get a raptor code for our blockchain. The summation \oplus of such symbols is conducted by bitwise XOR operation. Note that since $q = 2^p$, the

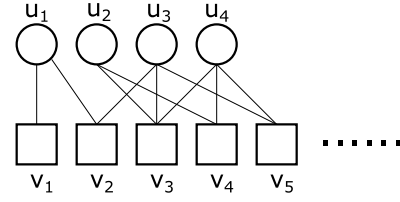


Fig. 2. LT encoding: Four information symbols (circles) are encoded into five coded symbols (squares) with degrees $d = 1, 2, 3, 2, 2$, respectively.

subtraction \ominus coincides with \oplus . With an LT code, one generates each coded symbol v_j as follows. It first chooses a degree d from a *generator degree distribution* $\Omega(d)$. It then randomly chooses d information symbols $\{u_{i_1}, \dots, u_{i_d}\}$ from $\{u_1, \dots, u_n\}$ with equal probability. These d information symbols are *neighbors* of v_j . We denote the set of indices of these neighbors by

$$\mathcal{N}(v_j) = \{i_1, \dots, i_d\}. \quad (4)$$

Finally, the coded symbol is calculated via the XOR operation

$$v_j = \sum_{i \in \mathcal{N}(v_j)} u_i = u_{i_1} \oplus \dots \oplus u_{i_d}. \quad (5)$$

The coded symbol v_j is the *edge* of the information symbols $\{u_{i_1}, \dots, u_{i_d}\}$. The set of all edges of u_i is denoted by

$$\mathcal{E}(u_i) = \{j : i \in \mathcal{N}(v_j)\}. \quad (6)$$

An information symbol u_i can be calculated using an edge coded symbol and its other neighboring information symbols as

$$u_i = v_j \oplus \sum_{h \in \mathcal{N}(v_j) \setminus \{i\}} u_h, \text{ for any } j \in \mathcal{E}(u_i). \quad (7)$$

An example of encoding four information symbols into five LT coded symbols is shown in Fig. 2. In this example we have $\mathcal{N}(v_1) = \{u_1\}$, $\mathcal{N}(v_2) = \{u_1, u_3\}$, $\mathcal{N}(v_3) = \{u_2, u_3, u_4\}$ and so on; and $\mathcal{E}(u_1) = \{v_1\}$, $\mathcal{E}(u_2) = \{v_3, v_4\}$, and so on.

The receiver can start decoding when it receives $(1 + \epsilon)n$ coded symbols. The decoding of the LT code is a “peeling” process. First, the decoder finds a coded symbol of degree one, that is v_j with $|\mathcal{N}(v_j)| = 1$. This coded symbol in fact is an information symbol with index $\{i\} = \mathcal{N}(v_j)$. Having decoded the information symbol u_i , the decoder removes u_i from the set of neighbors of all coded symbols from $\mathcal{E}(u_i)$, updates these coded symbols, and also decreases by 1 their degrees. For example, if $j' \in \mathcal{E}(u_i)$, then $v_{j'}$ and its set of neighbors are updated as follows:

$$v_{j'} \leftarrow v_{j'} \oplus u_i, \quad \mathcal{N}(v_{j'}) \leftarrow \mathcal{N}(v_{j'}) \setminus \{i\}. \quad (8)$$

The decoder continues finding coded symbols of degree one and peeling the information symbols until no coded symbol of degree one left or all information symbols are successfully decoded. If there are still undecoded information symbols, the receiver collects more coded symbols and restart the peeling process. For example, as shown in Fig. 3, for the LT code in Fig. 2, the decoder can successfully decode information symbols $\{u_1, u_3\}$ after it receives $\{v_1, v_2, v_3, v_4\}$. However, it

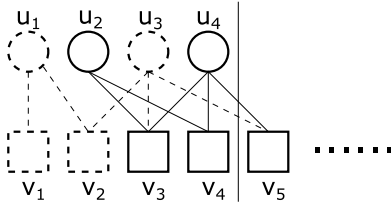


Fig. 3. LT decoding: Dashed circles indicate decoded information symbols. Dashed squares indicate coded symbols with zero degree. Dashed lines indicate the subtracted degree.

needs to collect one more coded symbol v_5 to successfully decode $\{u_2, u_4\}$.

An issue with the LT code is the error floor [36], [37]. The error floor means that the decoding failure rate does not drop sufficiently fast with more received coded symbols. This happens because the neighbors of coded symbols are uniformly chosen between $\{1, \dots, n\}$, and thus, there is a nonzero probability that an information symbol is not the neighbor of any received coded symbol, i.e., its edge is an empty set.

2) *Raptor Code* [35]: In order to address the error floor issue and to reduce the encoding/decoding complexity of the LT code, a raptor code first precodes the information symbols using a fixed rate outer code, such as LDPC, Reed–Solomon, or another linear code. The precoded symbols are called the *intermediate symbols*, which are then encoded into *coded* LT symbols. The raptor codes have very low-decoding failure probabilities, and thus they fit well with the stringent security requirement of blockchains. Moreover, the encoding and decoding complexity of raptor codes are $\mathcal{O}(k \log(1/\epsilon))$ [35], which is approximately a linear function of k . In what follows, we use raptor codes for our coded blockchains.

III. OVERVIEW OF PROPOSED RATELESS CODED BLOCKCHAIN

We first define the dynamic IoT blockchain network as follows. Time is divided into time epochs. We assume that the blockchain grows at a consistent rate of β blocks per time epoch. We further assume that in each time epoch t , l_t nodes leave and e_t nodes join the network, where l_t and e_t are Poisson distributed with means λ_l and λ_e , respectively. Moreover, we assume that IoT blockchain nodes have significantly lower storage capability than traditional blockchain nodes, e.g., servers and desktops. Let \mathcal{V}_t denote the set of nodes available in the network in the t th time epoch. Each node in the network can send “get address” message recursively to find all reachable nodes in the network to obtain \mathcal{V}_t [38]. Moreover, an address can be considered as valid only if it holds valid UTXOs to prevent Sybil attack. We next present the encoding and decoding procedures of the proposed rateless coded blockchain.

A. Encoding Procedure

We divide each block B^w into s symbols over \mathbb{F}_q and form groups as in Fig. 1. Thus, for each group we obtain a matrix

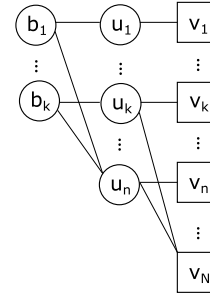


Fig. 4. Example of block coding graph using systematic raptor code.

in the form of (1). For each group we encode s rows of (1) into s code vectors using the same raptor code for each row. The number of blocks in each group varies depending on the network condition (detailed in Section VI). We use \mathcal{G}_m to denote the set of blocks in the m th group and $k_m = |\mathcal{G}_m|$. In general k_m is large if the number of active nodes in the network is large, and nodes do not actively leave the network. We encode the blocks in each group \mathcal{G}_m using a systematic raptor code [35] with an $[n_m, k_m]$ precode with a generator matrix \mathbf{G}_m . We assume that the *code rate* $r = k_m/n_m$ of the precode is the same for all groups and time epochs. The encoding and decoding procedures are the same for all groups, thus we sometimes may omit the subscript m to simplify the notation.

Since the same encoding and decoding is used for each row of (1), and therefore each row of (3), we will write $b_i, i = 1, \dots, k$, and $u_i, i = 1, \dots, n$, meaning any row of (1) and (3), respectively. Similarly for the matrix (9) presented below, we will write $v_i, i = 1, \dots, N$, meaning any row of (9). The information symbols $\{b_i\}$ are first encoded into intermediate symbols $\{u_i\}$ using (1)–(3). We call each column of (1), denoted by \mathbf{b}_i , an *original block*; and each column of (3), denoted by \mathbf{u}_i , an *intermediate block*. We assume that \mathbf{G}_m is in the systematic form, and therefore $\{\mathbf{u}_1, \dots, \mathbf{u}_k\} = \{\mathbf{b}_1, \dots, \mathbf{b}_k\}$.

The intermediate symbols of each row of (3) are then encoded into coded symbols using a systematic LT code with a degree distribution $\Omega(d)$. As a result we obtain the matrix

$$\begin{bmatrix} v_{1,1} & v_{2,1} & \dots & v_{k,1} & \dots & v_{n,1} & \dots & v_{N,1} \\ v_{1,2} & v_{2,2} & \dots & v_{k,2} & \dots & v_{n,2} & \dots & v_{N,2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ v_{1,s} & v_{2,s} & \dots & v_{k,s} & \dots & v_{n,s} & \dots & v_{N,s} \end{bmatrix}. \quad (9)$$

Here, N is the number of network nodes at the moment of encoding. Each column j of (9) is a *coded block* denoted by \mathbf{v}_j . We will use $\mathcal{E}(\mathbf{u}_i)$ to denote the set of edges for symbols $\{u_i\}$ and $\mathcal{N}(\mathbf{v}_i)$ to denote the set of neighbors for symbols $\{v_i\}$, respectively. We assume systematic encoding and therefore we have *systematic coded blocks* $\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ and *nonsystematic coded blocks* $\{\mathbf{v}_{n+1}, \dots, \mathbf{v}_N\}$. A coding graph from k original symbols $\{b_i\}$ to n intermediate symbols $\{u_i\}$ and then the N coded symbols $\{v_j\}$ is shown in Fig. 4. Each node stores only one coded block for each group. Note that, the indices of the coded block that a node stores for different groups may be different. For example, a node may store \mathbf{v}_a for the m th group and \mathbf{v}_b for the m' th group with $a \neq b$. However, to make our description simple, we assume that all

nodes are enumerated by integers and that node j stores \mathbf{v}_j^m for all groups $m = 1, \dots, M$, where M is the total number of groups. In the proposed rateless coded blockchain, we use a degree distribution $\Omega(d)$ with $\Omega(1) = 0$. An example will be considered in Section VII.

B. Decoding Procedure

When an original block \mathbf{b}_i from group m is needed by a node j , node j broadcasts a request to all nodes in the network. Then node i sends \mathbf{v}_i from group m (note that $\mathbf{v}_i = \mathbf{b}_i$) to node j . However, the blockchain network is dynamic and node i may leave the network or be disconnected. When this happens, node j can “repair” the needed block using the procedure that will be presented in Section V-B. Briefly, node j “repairs” the needed block using (7) by obtaining some other coded blocks from active nodes. If it fails, node j decodes all blocks in group m . To do this, the node j collects $(1 + \epsilon)k$ distinct coded blocks from other nodes, which are the columns of (9). Since the nonsystematic coded blocks $\{\mathbf{v}_{n+1}, \dots, \mathbf{v}_N\}$ have a random number of neighbors and the neighbors are randomly chosen, with a very high-probability arbitrary $(1 + \epsilon)k$ coded blocks are distinct. The decoder first runs the LT decoding as described in Section II-B1 to decode the intermediate blocks. It then runs a decoder of the precode to obtain the original blocks. Since each row of (1) is encoded into the corresponding row of (9) according to the same generator matrix of the precode and the same LT encoding procedure, the decoder can successfully decode all original blocks if it can decode the first row of (1).

We would like to note that since we use an LT code, all nodes store distinct coded blocks with very high probability, even if the number of nodes N keeps growing. This reduces the chance that multiple nodes store the same coded block. Moreover, the LT encoding procedure is much simpler than the design of a $k \times N$ generator matrix need for usual (not rateless) linear codes, especially when N is large and not known in advance. When a new node joins the system, it only needs to collect on average $\mathbb{E}[\Omega(d)]$ systematic coded blocks to encode its own coded block to store for each group, see the details in Section V. This significantly reduces the communication overhead as compared with [30]. The code length k_m is calculated based on the network condition. If we expect that the network conditions are going to deteriorate (for example, we expect that many nodes may leave the network), then we can decode and further re-encode all previously encoded groups with small value k_m . All nodes in the network must have a consensus on the blocks included into group m and the generator matrix \mathbf{G}_m of the precode. To provide such consensus, we propose a novel *enhanced block* in Section IV that can be easily embedded into the current blockchain.

An overview of the proposed coded blockchain is shown in Fig. 5(a) and (b). In Fig. 5(a), data and headers of the blocks that form the m th group are shown, together with the m th enhanced block that stores coding parameters for group m . The m th enhanced block is always generated later than any blocks in the m th group. Details on how enhanced blocks are organized and how we determine the group size k_m are given

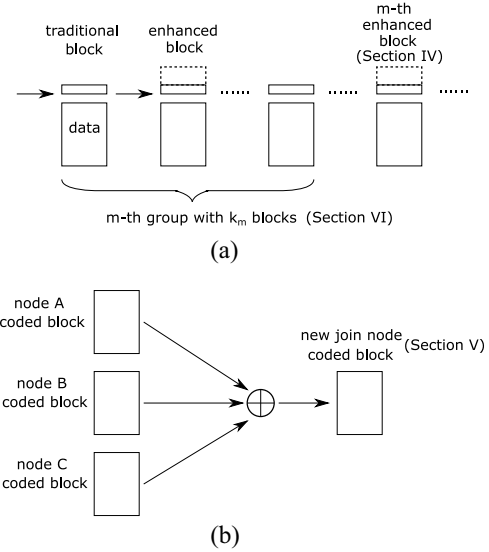


Fig. 5. Overview of the proposed rateless coded blockchain. (a) Rateless coded blockchain. (b) New joining node calculates coded block it needs to store.

in Sections IV and VI, respectively. When a new node joins the network in Fig. 5(b), it only needs to collect a small number of coded blocks from other nodes to calculate the coded block to store. Details of the new node joining procedure will be given in Section V.

Remark 1: The proposed encoding scheme is visibly different from the standard raptor code encoding, for instance presented in [35]. In the standard scenario one simply produces a semi-infinite sequence of parity symbols, since systematic (information) symbols are always available and never erased. In our case, however, systematic symbols may become unavailable if some systematic nodes leave the network. This results in significant changes of the encoding procedure, which takes into account possible absence of some systematic symbols (see Section V). This also results in that new (joining) nodes generate code symbols according to a different degree distribution, compared to the degree distribution used at the first instance of encoding a particular codeword (see Lemma 1). Up to the best of our knowledge raptor codes in such regimes have not been studied yet. Since our encoding and the effective erasure channel are substantially different from the standard ones, the standard analysis of the code performance, see [35], becomes inapplicable. For this reason we proposed a different approach for estimation of the code performance, see Section VI.

IV. ENHANCED BLOCK

In the existing coded blockchain system, see for example [10], the value of k is fixed for all groups. However, in our scheme, the group size varies according to the network condition and all nodes must have a consensus on coding parameters used for a particular group. Therefore, in this section, we present an enhanced block, which consists of a traditional block and some extra fields in the header to store the coding parameters. The block structure, mining and verification of the enhanced block is slightly different from traditional blocks.

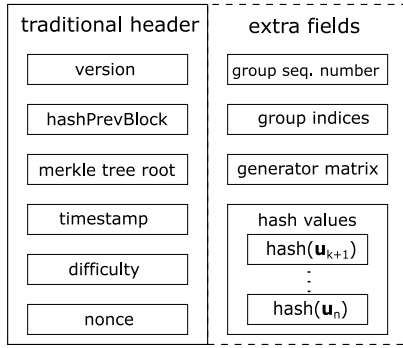


Fig. 6. Enhanced block header structure.

A. Enhanced Block Structure

The data of enhanced blocks is organized in the same way as in usual (not enhanced) blocks. However, the enhanced block header contains four additional fields compared with the header of a usual block, see Fig. 6. These new fields are as follows.

- 1) *Group Sequence Number*: This field is the sequence number of the enhanced block, which is independent of the block sequence number.
- 2) *Group Indices*: This field contains the block sequence numbers of the blocks to be encoded, i.e., $\mathcal{G}_m = \{w_1, \dots, w_k\}$. Note that $k_m = |\mathcal{G}_m|$ and $n_m = k_m/r$.
- 3) *Generator Matrix*: This field contains the generator matrix \mathbf{G}_m . It should be noted that this field can be omitted if the blockchain system uses a predefined generator matrix calculation algorithm. For example, if we use an LDPC code to encode the intermediate blocks, the code can be generated with progressive edge-growth (PEG) algorithm [39] and therefore it is enough to store values for k_m and n_m in the *group indices* field.
- 4) *Hash Values*: This field contains the hash values of the nonsystematic intermediate blocks $\{\mathbf{u}_{k+1}, \dots, \mathbf{u}_n\}$. When a new node joins the network, it needs systematic and sometimes nonsystematic intermediate blocks in order to generate its own coded block. The integrity of the systematic intermediate blocks, which are in fact the original blocks, can be verified via their Merkle tree roots in the corresponding block headers. The hash values field ensures that the new node can also validate the integrity of the nonsystematic intermediate blocks.

B. Mining

Recall that we employ the PoW protocol in which all nodes competitively “mine” new blocks. The “mining” procedure for the traditional blocks is the same as that in the existing blockchain. However, mining an enhanced block needs some more effort. Let M be the total number of “mined” enhanced blocks. All nodes in the network use the same algorithm to compute the value k_{M+1} , i.e., the size of the next group (see Section VI). Each node j also maintains a block pool \mathcal{P}_j , which contains confirmed, but not yet encoded blocks, see Fig. 7. A node j starts to mine the $(M+1)$ th enhanced block when $|\mathcal{P}_j| \geq k_{M+1}$. This includes the following steps.

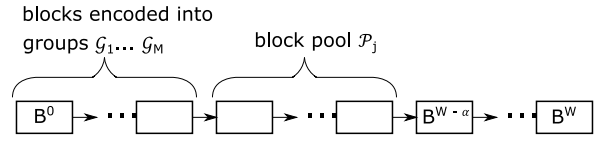


Fig. 7. Coded blockchain with block pool.

- 1) The “miner” first chooses transactions to include into the enhanced block and calculates the Merkle tree root. It then fulfills the fields of version, hash of previous block, timestamp and difficulty. So this part is similar to mining a traditional block.
- 2) The miner forms the set $\mathcal{G}_{M+1} \subset \mathcal{P}_j$ with size $|\mathcal{G}_{M+1}| = k_{M+1}$.
- 3) The miner then forms an $k_{M+1} \times n_{M+1}$ generator matrix \mathbf{G}_{M+1} .
- 4) Next, the miner calculates the intermediate blocks $\{\mathbf{u}_1, \dots, \mathbf{u}_{n_{M+1}}\}$ using (2) and their hash values.
- 5) Finally, similar to mining a traditional block, the miner finds the nonce such that the hash value of the enhanced block header is less than the difficulty level.

After the above procedure, the miner produces an enhanced block with the header structure described in Section IV-A. We see that steps 2-4 are not present in the mining of a traditional block. However, the computational complexity of these steps is negligible compared with finding the nonce. Hence, the incentive for mining an enhanced block is the same as that for mining a traditional block.

C. Verification

When a node receives a new mined enhanced block with sequence number $M+1$, the node verifies this block. If the new enhanced block is valid, the node attaches it to its chain and terminates its own mining process of the $(M+1)$ th enhanced block. Otherwise, it continues its own mining process. In particular, the verification at node j' should include, but not limited to, the following steps.

- 1) The enhanced block is correctly formed, including block data and block header structure. This step can include the same verification process for traditional blocks, such as checking nonce and target, size of each field, chain to the previous block, etc.
- 2) The block pool size of the verifying node j' is larger than or equal to k_{M+1} , i.e.,

$$|\mathcal{P}_{j'}| \geq k_{M+1}. \quad (10)$$

- 3) All blocks in the encoding group are within the block pool, i.e.,

$$\mathcal{G}_{M+1} \subset \mathcal{P}_{j'}. \quad (11)$$

- 4) Calculating $\{\mathbf{u}_{k_{M+1}+1}, \dots, \mathbf{u}_{n_{M+1}}\}$ using (2) and \mathbf{G}_{M+1} and verifying their hash values.

We recall that when mining an enhanced block, a node needs slightly more resources, because it has to find k_{M+1} and \mathbf{G}_{M+1} . Though this extra resources are much smaller than resources needed for finding a nonce, still some nodes may continue mining traditional blocks instead of an enhanced block. To prevent this, we propose to use a punishment mechanism. For

example, nodes may follow the rule that if a node has a block pool size satisfying (10), then it accepts a new block if and only if this is an enhanced block.

D. Block Pool Update

After a node j mined or validated the new $(M + 1)$ th enhanced block, its block pool is updated as

$$\mathcal{P}_j \leftarrow \mathcal{P}_j \setminus \mathcal{G}_{M+1}. \quad (12)$$

However, it should be noted that the blocks from \mathcal{G}_{M+1} are not yet ready for encoding since the depth of the $(M + 1)$ th enhanced block is less than α , i.e., this enhanced block is not confirmed. It could happen that the blockchain splits into several branches, and that different candidate $(M + 1)$ th enhanced blocks are mined in more than one branch. In this case, node j will maintain pools \mathcal{P}_j^f for each branch f that contains a candidate $(M + 1)$ th enhanced block. As soon as one of these candidate enhanced blocks is confirmed, say in branch f^* , the node j assigns $\mathcal{P}_j = \mathcal{P}_j^{f^*}$ and discards the block pools in other branches. In this way the node keeps the pool of available blocks associated with the longest branch.

E. Decentralized Systematic Raptor Code Encoding

After the m th enhanced block is confirmed, all nodes start to encode the blocks in \mathcal{G}_m according to the procedure described in Section III-A, but in a distributive manner. We note that, because of network propagation delays and different processing speeds, at a given time moment t different nodes typically have different values of W . Let $\hat{B}(m)$ be the block sequence number of the m th enhanced block. Let us assume that any node j has W such that $W - \alpha = \hat{B}(m)$. Let us denote by

$$\mathcal{C}_j^m = \{i : \exists j', \mathcal{N}(\mathbf{v}_{j'}^m) = \{i\}\} \quad (13)$$

the set of intermediate blocks that are stored by some node at a given moment t . We describe the way how node j gets \mathcal{C}_j^m later in this section. Note that it is possible that $\mathcal{C}_j^m = \emptyset$. It is also possible that sets \mathcal{C}_j^m are different for different nodes. Let us also define

$$\mathcal{S}_j^m = \{1, \dots, n\} \setminus \mathcal{C}_j^m \quad (14)$$

the set of intermediate blocks that are not stored by any nodes.

As soon as $W - \alpha = \hat{B}(m)$, node j starts encoding its own coded block for the m th group as follows.

- 1) Node j first checks \mathcal{S}_j^m . If $\mathcal{S}_j^m = \emptyset$, then the node generates d_j from the generator degree distribution $\Omega(d)$, and a set $\mathcal{N}(\mathbf{v}_j^m)$, and computes \mathbf{v}_j^m according to (5). If $\mathcal{S}_j^m \neq \emptyset$, the node takes any $i_j \in \mathcal{S}_j^m$, assigns $\mathcal{N}(\mathbf{v}_j^m) = \{i_j\}$, and broadcasts the message “I store intermediate block $\mathbf{u}_{i_j}^m$ with a timestamp t_j ” across the network.
- 2) Upon receiving this message, each node, say node j' , updates its $\mathcal{C}_{j'}^m \leftarrow \mathcal{C}_{j'}^m \cup \{i\}$ and $\mathcal{S}_{j'}^m$. However, if node j receives $i_{j'} = i_j$ from node j' with timestamp $t_{j'} < t_j$, this means node j' decided to store $\mathbf{u}_{i_j}^m$ earlier than node j . In this case node j updates \mathcal{S}_j^m and \mathcal{C}_j^m , and starts the encoding process from scratch.

All network nodes follow the above procedure. As a result, this procedure ensures that each systematic coded block $\{\mathbf{v}_1^m, \dots, \mathbf{v}_n^m\} = \{\mathbf{u}_1^m, \dots, \mathbf{u}_n^m\}$ is stored at one and only one node. Moreover, this procedure also ensures that the degree distribution of the nonsystematic coded blocks $\{\mathbf{v}_{n+1}^m, \dots, \mathbf{v}_n^m\}$ follow the given degree distribution $\Omega(d)$. It is possible that some nodes storing the systematic coded block leave the network. Moreover, it is possible that malicious nodes pretend to have such systematic blocks, but cannot provide them to honest nodes. In the next section, we present a repair procedure to dynamically maintain the systematic property.

V. NETWORK MAINTENANCE ALGORITHM

In this section, we present our NMA. When a new node j joins the network, it first attempts to encode a new nonsystematic coded block by obtaining intermediate blocks from other nodes in the network. If it fails, i.e., one or more intermediate blocks are not stored by any node in the network, node j then tries to repair and store a missing intermediate block.

A. Encoding Nonsystematic Coded Block

Let \mathcal{M} be the set of enhanced blocks such that all groups of blocks $\mathcal{G}_m \forall m \in \mathcal{M}$ are encoded. When a new node j joins the network, it first copies the original uncoded blocks from other nodes. It then calculates the coded block \mathbf{v}_j^m to store for each $m \in \mathcal{M}$. In particular, for each group $m \in \mathcal{M}$, the node j generates a degree d_j^m from $\Omega(d)$ and forms $\mathcal{N}(\mathbf{v}_j^m)$. It then broadcasts across the network a request for blocks with indices from $\mathcal{N}(\mathbf{v}_j^m)$. Upon receiving this request, a node j' will send to node j an index i if $\mathcal{N}(\mathbf{v}_{j'}^m) = \{i\}$ for any $i \in \mathcal{N}(\mathbf{v}_j^m)$, to inform node j that the intermediate block \mathbf{u}_i^m . Node j then assigns $\phi(\mathbf{u}_i^m) = 1$ to indicate the availability of \mathbf{u}_i^m , otherwise $\phi(\mathbf{u}_i^m) = 0$. Hence, for each group $m \in \mathcal{M}$, node j is able to construct a set \mathcal{R}_j^m of missing intermediate blocks

$$\mathcal{R}_j^m = \{i : \phi(\mathbf{u}_i^m) = 0, i \in \mathcal{N}(\mathbf{v}_j^m)\}. \quad (15)$$

If $\mathcal{R}_j^m = \emptyset$, then node j can obtain all blocks from $\mathcal{N}(\mathbf{v}_j^m)$ from other nodes and then it calculates and stores the coded block \mathbf{v}_j^m according to (5). Otherwise, if $\mathcal{R}_j^m \neq \emptyset$ due to nodes storing the systematic coded blocks leaving the network or having bad network connection, node j will try to repair a block in \mathcal{R}_j^m . It starts by trying to repair one block from \mathcal{R}_j^m . During the process of repairing, the set \mathcal{R}_j^m can be expanded with other missing intermediate blocks, as it is described in the next Section.

B. Intermediate Block Repair

Node j chooses random $i \in \mathcal{R}_j^m$ and tries to repair \mathbf{u}_i^m using an edge coded block $\mathbf{v}_{j'}^m$, where $j' \in \mathcal{E}(\mathbf{u}_i^m)$, and $\mathbf{v}_{j'}^m$'s other neighboring intermediate blocks $\mathcal{N}(\mathbf{v}_{j'}^m) \setminus \{i\}$ similar to (7), i.e.,

$$\mathbf{u}_i^m = \mathbf{v}_{j'}^m \oplus \sum_{h \in \mathcal{N}(\mathbf{v}_{j'}^m) \setminus \{i\}} \mathbf{u}_h^m, \text{ for any } j' \in \mathcal{E}(\mathbf{u}_i^m). \quad (16)$$

However, the set of edges $\mathcal{E}(\mathbf{u}_i^m)$ and the set of neighbors $\mathcal{N}(\mathbf{v}_{j'}^m)$ for any $j' \in \mathcal{E}(\mathbf{u}_i^m)$ are not known by node j . For this

on simulation results in the Bitcoin blockchain network (see Section VII-C).

VI. DETERMINING GROUP SIZE k_m

Recall that k_m is the number of blocks in the m th group. When a miner is mining the m th enhanced block, see Section IV-B, it needs to determine k_m to ensure the decoding failure probability of this group is less than a target failure probability ζ for all future γ time epochs. To do this, the miner first obtains the current number of nodes $|\mathcal{V}_t|$ at current time epoch t_m . It then calculates k_m using a function of $|\mathcal{V}_t|$, ζ and γ . Details of finding such a function will be discussed in this section. Note that, the time epoch t_m is the current time and is not by chosen or adjusted.

As will be explained later, our goal is to choose k_m as large as possible, but so that after γ time epochs the original blocks from \mathcal{G}_m can be restored with a decoding failure probability less than ζ . A reliable system typically requires the failure probability be less than 10^{-9} [40]. In our proposed rateless coded blockchain with a set of \mathcal{M} encoded groups, each node stores only $|\mathcal{M}|$ coded blocks and the blocks that have not been encoded yet. The extra storage for the enhanced block headers, i.e., the hash values of the nonsystematic intermediate blocks, is negligible.¹ Hence, we define the *storage reduction coefficient* as follows.

Definition 1: The storage reduction coefficient R_s is defined as the ratio of the space needed by an individual node in the proposed rateless coded blockchain over such space in a replicated blockchain, i.e.,

$$R_s = \frac{W - \sum_{m \in \mathcal{M}} k_m + |\mathcal{M}|}{W}. \quad (23)$$

The total number of encoded blocks is $\sum_{m \in \mathcal{M}} k_m$. Hence, the larger are k_m 's, the smaller is $|\mathcal{M}|$, and therefore the smaller is the storage reduction coefficient. Thus, we would like k_m 's to be large. On the other hand, if k_m is too large and some nodes leave the network, we may not be able to recover (decode) some groups. To find a good tradeoff, we define the decoding failure probability as follows.

Definition 2: Given the degree distribution $\Omega(d)$, the rate of nodes leaving and joining the network λ_l and λ_e , respectively, and initial number of nodes N , the decoding failure probability $f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma)$ is the probability that a node fails to decode a group of blocks after γ time epochs since the group encoding.

Let $p(\mathbf{G}, \Omega^*(d), \epsilon)$ be the probability that the raptor code fails to decode at least one information symbol with precode matrix \mathbf{G} , coded symbol degree distribution $\Omega^*(d)$ and overhead ϵ . Let us assume that $p(\mathbf{G}, \Omega^*(d), \epsilon)$ is known to us, for example it can be derived using an analysis similar to that in [35], or it can be obtained via simulations. Then we have the following result.

Lemma 2: The decoding failure probability is given by (26).

¹For example, when a group has $k = 10000$ blocks and $r = 0.8$, there are 2500 hash values to store in the enhanced block header and needs 0.076 MB, which is negligible as compared with more than 9.76-GB space saving when all blocks are 1 Mb.

Proof: It is not difficult to see that

$$f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma) = \int_0^\infty p(\mathbf{G}, \Omega^*(d), \epsilon) \Pr(N + \Delta_\gamma = (1 + \epsilon)k) d\epsilon \quad (24)$$

where Δ_γ is the sum of two Poisson processes that follows a Skellam distribution [41], i.e.,

$$\Pr(\Delta_\gamma = s) = e^{-\gamma(\lambda_l + \lambda_e)} \left(\frac{\lambda_l}{\lambda_e}\right)^{\frac{s}{2}} \sum_{X=0}^\infty \frac{1}{X!(X+s)!} \left(\gamma\sqrt{\lambda_l\lambda_e}\right)^{2X+s}. \quad (25)$$

Hence, by substituting (25) into (24), we obtain

$$f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma) = \int_0^\infty p(\mathbf{G}, \Omega^*(d), \epsilon) e^{-\gamma(\lambda_l + \lambda_e)} \left(\frac{\lambda_l}{\lambda_e}\right)^{\frac{(1+\epsilon)k-N}{2}} \times \sum_{X=0}^\infty \frac{1}{X!(X+(1+\epsilon)k-N)!} \left(\gamma\sqrt{\lambda_l\lambda_e}\right)^{2X+(1+\epsilon)k-N} d\epsilon. \quad (26)$$

As we explain below, for finding an appropriate value of k_m we use the function $f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma)$, which can be obtained in several possible ways. One way is to use analysis similar to the one presented in [35] for first obtaining values $p(\mathbf{G}, \Omega^*(d), \epsilon)$ and next using Lemma 2. Another way is to obtain $f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma)$ via simulations, which requires some efforts since obtaining small values of $f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma)$ may take too long simulation time. Several methods for resolving this problem have been proposed by the coding theory community, see for example [42] and references therein. The main goal of our work is not coding theory, however, but design of new blockchain. For this reason, in this work, we simply assume that $f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma)$ is available to us. For our numerical examples considered in the next Section, we generate $f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma)$ by simulating it up to 10^{-4} and extrapolating it further for smaller values. For example, when $\lambda_l = 12$, $\lambda_e = 4$, $N = 3000$, $\gamma = 100$, and $\Omega(d)$ follows the generator degree distribution in Section VII, the decoding failure probability is shown in Fig. 9.

Recall that our goal is to determine k_m at time epoch t_m when the number of nodes in the network is $|\mathcal{V}_{t_m}|$, so that the decoding failure probability after γ time epoch when network changes to $|\mathcal{V}_{t_m+\gamma}|$ as a result of nodes leaving and joining the network, is no higher than ζ . It should be noted that $f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma)$ becomes a function of (k/N) when $N \rightarrow \infty$. For finite N , the probability $f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma)$ increases as N decreases with a fixed ratio of (k/N) , see simulation results in Fig. 10(b). It should be also noted that the blocks in group \mathcal{G}_m will be encoded after the m th enhanced block is confirmed. Recall that β is the number of blocks generated in each time interval, which is a constant on average, and α is the required depth for a block to be confirmed. Therefore, we calculate k_m by table lookup according to the following:

$$f\left(k_m, |\mathcal{V}_{t_m}|; \Omega(d), \lambda_l, \lambda_e, \gamma + \frac{\alpha}{\beta}\right) = \zeta \quad (27)$$

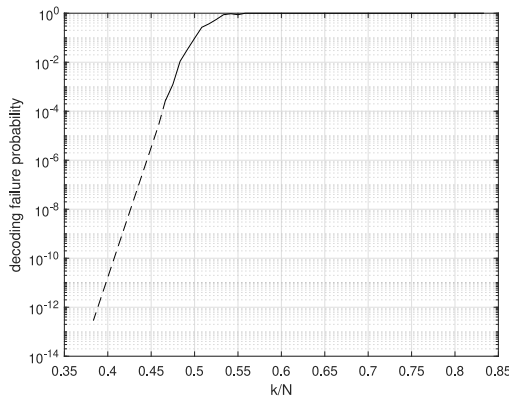


Fig. 9. Decoding failure probability of $f(k, 3000; \Omega(d), 12, 4, 100)$. Solid line indicates the failure probability from simulation and dashed line indicates the predicted failure probability.

where (α/β) is the number of time epochs needed for the m th enhanced block to be confirmed, and ζ is the target failure probability.

If at a moment $t' \geq t_m + \gamma$ we have that $|\mathcal{V}_{t'}| < |\mathcal{V}_{t_m}|$, then we cannot guarantee that at time $t' + \gamma$ we will have decoding failure probability smaller than ζ . In this case each node j puts the blocks in \mathcal{G}_m back to the pool \mathcal{P}_j , and proceeds further in the standard way with one exception—if node j mines the next enhanced block, it assigns to it the sequence number m , instead of $M + 1$. This new m th enhanced block overwrites the old one and its mining and verification processes are the same as those for a new mined enhanced block. Thus, if more than one enhanced blocks have the same sequence number, only the latest one is valid. If malicious nodes deliberately “remin” an enhanced block with sequence number m^* that not need to be “remined,” all honest nodes will not accept this enhanced block since the blocks \mathcal{G}_{m^*} are not in their block pools. The new joining node runs the NMA algorithm in the backward direction—from the latest enhanced block in the longest blockchain branch toward to the genesis block. If the new node bumps to an enhanced block with a sequence number, say m , that it already met earlier in this backward process, then the new node simply ignores this enhanced block.

In a situation where malicious nodes exist. The altered coded block sent from malicious nodes can be detected and/or corrected via the error correction feature, also see discussion in [9]. The number of tolerable malicious nodes can be considered as node leave the network, since their coded block are unavailable for decoding. Note that this article provides an upper bound of the storage reduction when no malicious nodes occur. By considering malicious nodes, one can simply reduce the number of available nodes $|\mathcal{V}|$ in the network when calculating (26).

It should be noted that our scheme increases communication overhead when an enhanced block miner needs to estimate the number of nodes in the network. In order to obtain the number of nodes, we can employ the “ping” and “pong” mechanism used in the existing blockchains for checking whether a node is alive [43]. We can only count the nodes that recently broadcast

honest messages, such as valid blocks or transactions, to avoid fake connections. Each node can broadcast an alive message every 24 h, which should be enough since in the modern blockchains the number of nodes typically varies quite slowly. For instance, in the Bitcoin network, the average number of joining and leaving nodes per day are 42.18 and 43.16, respectively, see Section VII-C. Hence, the percentage-wise the increased communication overhead for estimating network size is much smaller compared to the typical network load.²

VII. SIMULATION RESULTS

Our simulations are conducted using MATLAB 2020b on a laptop with an Intel Core i7 eight-core CPU @ 2.2 GHz. In our simulations, we implemented the proposed rateless coded blockchain using the Reed–Solomon code as the precode. The generator matrix of the Reed–Solomon code is from MATLAB 2020b Communication Toolbox. The generator degree distribution $\Omega(d)$ is as follows. Let $S = c \ln(k/\delta) \sqrt{k}$, where c and δ are constants, and define

$$\tau(d) = \begin{cases} \frac{S}{ik}, & \text{for } d = 1, \dots, \frac{k}{S} - 1 \\ \frac{S \ln(S/\delta)}{k}, & \text{for } d = \frac{k}{S} \\ 0, & \text{for } d = \frac{k}{S} + 1, \dots, k \end{cases} \quad (28)$$

$$\rho(d) = \begin{cases} \frac{1}{k}, & \text{for } d = 1 \\ \frac{1}{d(d-1)}, & \text{for } d = 2, \dots, k. \end{cases} \quad (29)$$

In [29] the following degree distribution is proposed for obtaining LT codes:

$$\mu(d) = \frac{\tau(d) + \rho(d)}{\sum_{j=1}^k (\tau(j) + \rho(j))}. \quad (30)$$

In our simulations, we set $c = 0.1$ and $\delta = 0.5$, which are known to lead to good and stable performance [36]. As discussed in Section III-A, a new node should use a degree distribution with $\Omega(1) = 0$. For this reason we slightly modify $\mu(d)$ in (30) and set

$$\Omega(d) = \begin{cases} 0, & \text{for } d = 1 \\ \mu(d) + \frac{\mu(1)}{k-1}, & \text{for } d = 2, \dots, k. \end{cases} \quad (31)$$

We first compare the LT and raptor codes in the dynamic network, and show the decoding failure probabilities $f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma)$ for several network scenarios. Next, we evaluate the proposed rateless coded blockchain in a highly dynamic blockchain network where the number of nodes leaving is much higher than that for joining. Finally, we show the performance of the proposed scheme in the real-world Bitcoin network. Note that the performance of encoding/decoding complexity of the raptor code can be found in [35]. Moreover, this article focuses on the dynamic blockchain network, i.e., nodes joining and leaving. We do not consider the network topology nor how nodes are connected via wired or wireless links. Therefore, we omit the effect of propagation delay.

²A typical ping and pong message have 32 byte, which increases network communication overhead $32 \times N^2/24$ bytes per hour. A Bitcoin block has 10^6 bytes and is generated every 10 min, which results in a typical network load of $10^6 \times N \times 6$ bytes per hour. Hence, the increased communication overhead is 0.22% when $N = 10000$.

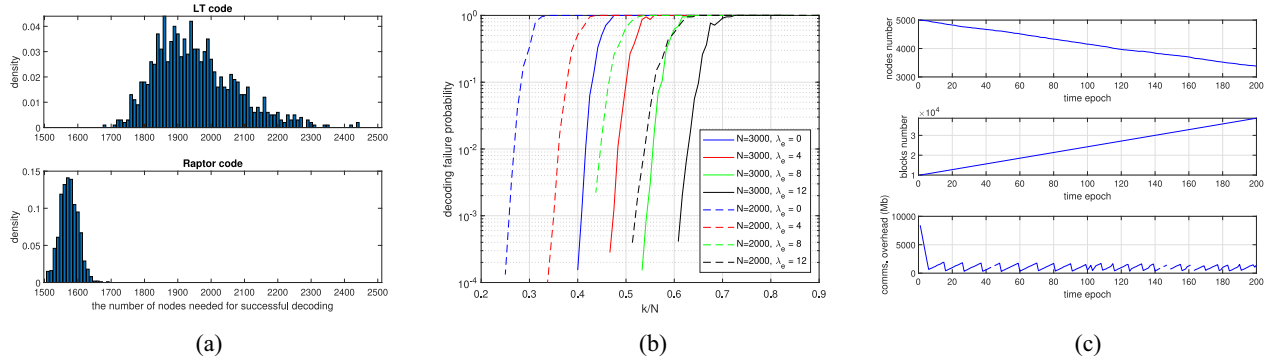


Fig. 10. (a) Performance comparison of LT and Raptor codes in dynamic blockchain networks. (b) Decoding failure probability when $\gamma = 100$, $\lambda_l = 12$, $\lambda_e = \{0, 4, 8, 12\}$. (c) Number of nodes, number of blocks, and communication overhead (Mb) of the new joining node with time epoch growth.

A. Code Performances

We first study the minimum number of nodes needed for successful decoding by using the LT and raptor codes, respectively. We set a fixed length blockchain with only one group with $k = 1000$, the network initially has $N = 3000$ nodes, and $\lambda_l = 50$ and $\lambda_e = 40$ nodes per time epoch. We set the code rate of the precode as $r = 0.8$. The network is dynamic using the NMA algorithm. We generated 1000 blockchains and ran them until a new node decoding fails. We record the numbers of nodes needed in each of these networks for the latest successful decoding before the failure occur, and show their densities in Fig. 10(a). We see that the raptor code significantly outperforms the LT code since it requires smaller number of nodes for successful decoding. We also see that sometimes the LT code needs more than 2400 nodes for decoding, which means that sometimes it needs very large, $\epsilon = 1.4$, decoding overhead. This is due to the error floor issue present in LT codes [36], [37].

We next show the decoding failure probability $f(k, N; \Omega(d), \lambda_l, \lambda_e, \gamma)$ in Fig. 10(b). We fix $\lambda_l = 12$, $\gamma = 100$, and take $\lambda_e = \{0, 4, 8, 12\}$ and $N = \{2000, 3000\}$. We keep the code rate of the precode as $r = 0.8$. Note that when $\lambda_e = 0$, decoding blocks in the dynamic network is equivalent to decoding through a binary erasure channel (BEC) since nodes (symbols) leave the network, i.e., are erased, with uniform probability, and no repairing occurs. From the result, we can see that BEC is the worst scenario in the sense that it leads to the minimum value of k for a given decoding failure probability. This opens the possibility of obtaining $f(\cdot)$ by using known methods, see for example [35], for analysis of raptor codes in BEC. This possibility will be explored in future works. The results also show that $f(\cdot)$ increases as N decreases.

B. Rapidly Reducing Network

It is instructive to consider a rapidly reducing network. We set $\lambda_l = 12$, $\lambda_e = 4$, $N = 5000$, $\gamma = 98$, $\beta = 144$, $\alpha = 244$, and target decoding failure probability $\zeta = 10^{-12}$. We assume that initially there are 5000 nodes and 10000 un-encoded blocks in the blockchain when implementing the proposed rateless coded blockchain approach. We assume that

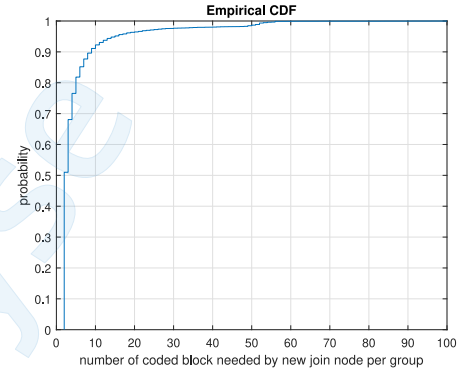


Fig. 11. CDF of the number of coded blocks that a new joining node needs to collect from other nodes in order to generate its parity or intermediate block for a given group.

all blocks have a constant bit-size of 1 Mb. In order to clearly demonstrate the group size change, we assume that a maximum of 1 new enhanced block can be generated at each time epoch. The network is run through 200 time epochs.

Fig. 10(c) shows the number of network nodes and number of blockchain blocks at a given time epoch, and the communication overhead needed by a new node for generating new parity check blocks or repairing intermediate blocks for previously encoded groups. The communication overhead is measured in the total number of bits that a new joining node needs. The communication overhead of the traditional blockchain is the total bit-size of all blocks and it increases with the blockchain length. In contrast, the communication overhead of the rateless coded blockchain is less than 800 Mb when the total blockchain bit-size exceeds 38 000 Mb. The communication overhead alternatively increases and decreases because the blocks are consistently generated, and they are encoded only when the involved enhanced block is confirmed. It should be noted that the communication overhead increases with the number of encoded groups $|\mathcal{M}|$, and thus with the size W of the blockchain. However, since $|\mathcal{M}|$ grows very slowly, the increment is not noticeable during the presented 200 time epochs.

In this experiment, 26 enhanced blocks are mined. In particular, the third to 13th enhanced blocks are mined twice and the first to second enhanced blocks are mined thrice. The

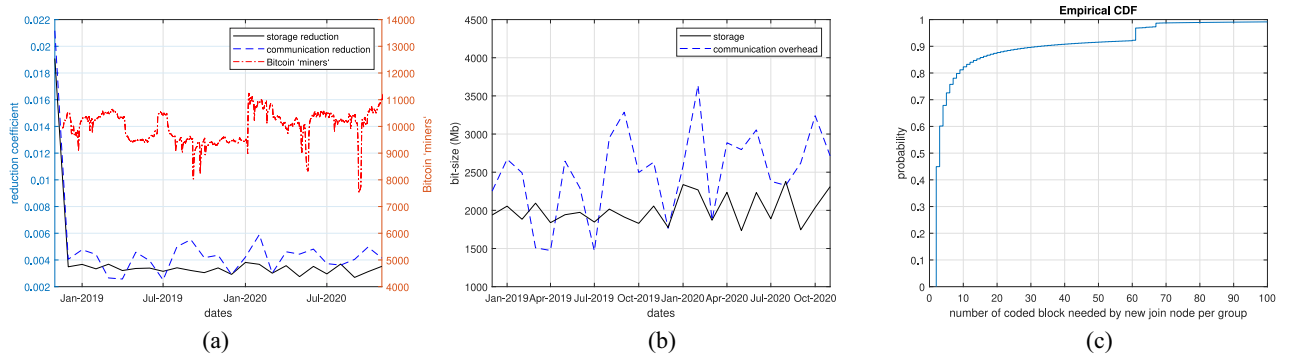


Fig. 12. (a) Storage and communication reduction coefficients in real Bitcoin blockchain. (b) Storage and communication overhead bit-sizes in real Bitcoin blockchain. (c) CDF of the number of coded blocks that a new joining node needs in real Bitcoin blockchain.

TABLE I
ENHANCED BLOCK GENERATION AND k_m VALUES

seq.	1	2	3 ~ 13	14 ~ 26
1st "mined"	1	2	3 ~ 95	102 ~ 198
k_m	1910	1906	1904 ~ 1613	1593 ~ 1287
2nd "mined"	100	101	102 ~ 194	-
k_m	1600	1595	1593 ~ 1301	-
3rd "mined"	199	200	-	-
k_m	1284	1279	-	-

reason is that the number of nodes keeps decreasing, thus, the blocks in these groups need to be regrouped and re-encoded to ensure the decoding failure probability meets the requirement. We show the time epochs when these blocks are mined and their k_m values in Table I. From Table I, we see that the enhanced blocks are mined at a near constant interval of 12 time epochs after the initial stage at which there are a large pool of available blocks. Table I also shows that the enhanced blocks are regenerated or remined immediately after γ time epochs and their values of k_m decreases with the time epoch. This is because the number of nodes in the network is rapidly decreasing.

Fig. 11 shows the CDF of the number of coded blocks, which can be systematic or nonsystematic ones, that a new joining node needs to collect from other nodes in order to generate its own parity or intermediate block for a given group. We can see that with more than 90% probability, the new joining node only needs to collect ten blocks. This is significantly lower than other coded blockchains proposed in [9], [10], and [30]. In these works a new node needs to collect more than k_m blocks for group G_m , and as we saw k_m is typically much larger than 10.

It should be noted that this section simulates an extreme scenario where nodes consistently and rapidly leaving the network. In this case, existing nodes need to re-encode to ensure the blockchain is decodable, thus, increase the overall communication overhead. However, in practice, a typical blockchain network, such as Bitcoin, has a relative static number of nodes, e.g., the number of nodes in Bitcoin network is around 10 000 for many years, see in Section VII-C. Moreover, in practice, we can employ some simple strategies to reduce the frequency of re-encoding. For instance, we can introduce

an coefficient $r < 1$ in (27) as $f(k_m, r|\mathcal{V}_{t_m}; \cdot) = \zeta$. Then remaining an enhanced block will only occur when $|\mathcal{V}_t| < r|\mathcal{V}_{t_m}|$. In Bitcoin network, we can set $r = 0.7$, which means "re-encoding" a group only occurs when the number of nodes is reduced by 30%. As far as we know, this has not happened in Bitcoin history since 2015 [28], and is not expected in future.

C. Performance in Bitcoin Network

We evaluate our rateless coded blockchain using the real-world Bitcoin data obtained in [38] from 18 November 2018 to 13 November 2020. We assume that our approach was implemented into the Bitcoin blockchain on 18 November 2018. The initial and the latest blockchain lengths are 551 685 and 656 805 blocks, respectively. We assume that each time epoch is one day, i.e., 24 h, hence we have $\beta = 144$, since one block is generated per 10 min on average [44]. We then assume that all blocks are fully loaded with bit-size of 1 Mb. From [38] we obtain that nodes are leaving and joining the network as Poisson processes with $\lambda_l = 42.18$ and $\lambda_e = 43.16$, respectively, and that the average number of nodes is 10 000. We set $\alpha = 144$ [45], $\zeta = 10^{-12}$ and $\gamma = 98$ (roughly three months). We omit the bit-size of block headers (latest about 50 Mb), which is negligible as compared with the total block data. We define the *communication reduction coefficient* as the ratio of the communication overheads of the proposed rateless coded blockchain and the traditional blockchain.

We show the month average storage reduction coefficient defined in (23) and the communication reduction coefficient in Fig. 12(a). We see that both storage and communication reduction coefficients shrink to around 0.4% and remain constants after December 2018. This is because during the initial stage of the implementation, there are a very large number of original blocks that should be encoded into the coded blocks. Thus, the storage and communication reduction coefficients are both high at the beginning.

In Fig. 12(b), we show the bit-size in Mb of the average storage at each node and the average communication overhead for each new joining node over a month. Recall that for the traditional replicated blockchain, both storage and communication overheads increase from 540 to 640 Gb. So one can see the dramatic reduction by using the rateless coded blockchain. Even though the blockchain size has increased by

100 Gb from December 2018 to November 2020, the average storage and communication overheads have increased by only 400 and 700 Mb, respectively. The trends of storage and communication overheads in Fig. 12(b) are similar to those in Fig. 12(a) because the Bitcoin blockchain length increases at a constant rate of 144 blocks per day.

Fig. 12(c) shows the CDF of the number of coded blocks, either systematic or nonsystematic ones, that a new node collects. With very high probability, i.e., 99%, the new joining node only needs to obtain 70 coded blocks from other nodes per group, while on average there are $10\,000 \times 0.337 = 3370$ blocks in each group. The number of blocks collected by a new node is slightly higher than that in Fig. 11 in Section VII-B. This is because there are more nodes in the Bitcoin network—10 000 as opposed to 5000 assumed in Section VII-B. Hence, the size of the groups and the expected generator degree in the Bitcoin network are both higher than those in Section VII-B. Although it is hard to observe in Fig. 12(c), we found that the probability that a new node has to decode a group \mathcal{G}_m , rather than directly encode or repair, is less than 6.3×10^{-5} . The decoding has relatively large complexity, so it is preferable to keep this probability low.

In summary, if all Bitcoin blockchain nodes store the original blocks that are needed for verifying new transactions (around 5 GB [5]) and encode all other old blocks using the proposed rateless coded blockchain, then each node needs a total storage space of around 7 GB. In this way, all old blocks are recoverable rather than simply deleted. In addition, when a new Bitcoin node joins the network, it only needs to download 8 GB of data. These values are significantly lower than those of the current Bitcoin, which needs to download and store more than 300 Gb (600 Gb if all blocks are fully loaded).

VIII. CONCLUSION

We have proposed a rateless coded blockchain to reduce the node storage requirement and the communication overhead for new joining nodes in practical dynamic IoT blockchain networks. It adjusts the coding parameters according to the network conditions to guarantee that all encoded blocks can be decoded whenever needed with very high probabilities. We have also presented novel enhanced blocks, which are embedded into the blockchain, to store the coding parameters, so that these parameters are immutable and can be shared among all nodes via the integrated and distributive features of the blockchain. Extensive simulations have been conducted using both synthetic data and real-world Bitcoin data. Results show that both the storage requirement at each node and the communication overhead of each new joining node are reduced by 99.6% as compared with the traditional uncoded blockchain. A potential future work is to determine coding parameters of raptor code, such as precode rate and degree distribution, to have a lower decoding failure probability in the context of coded blockchain. Another future work is to build an IoT blockchain system with elaborate design that implements the proposed scheme.

REFERENCES

- [1] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
- [2] G. O. Karame and E. Androulaki, *Bitcoin and Blockchain Security*. Norwood, MA, USA: Artech House, 2016.
- [3] X. Fan, B. Niu, and Z. Liu, "Scalable blockchain storage systems: Research progress and models," *Computing*, vol. 104, no. 6, pp. 1497–1524, 2022.
- [4] "Bitcoin blockchain size." Blockchain. 2023. [Online]. Available: <https://www.blockchain.com/charts/blocks-size>
- [5] "Bitcoin core." 2023. [Online]. Available: <https://bitcoincore.org/>
- [6] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020.
- [7] S. Das, A. Kolluri, P. Saxena, and H. Yu, "On the security of blockchain consensus protocols," in *Proc. Int. Conf. Inf. Syst. Security*, 2018, pp. 465–480.
- [8] M. Dai, S. Zhang, H. Wang, and S. Jin, "A low storage room requirement framework for distributed ledger in blockchain," *IEEE Access*, vol. 6, pp. 22970–22975, 2018.
- [9] D. Perard, J. Lacan, Y. Bachy, and J. Detchart, "Erasure code-based low storage blockchain node," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2018, pp. 1622–1627.
- [10] H. Wu, A. Ashikhmin, X. Wang, C. Li, S. Yang, and L. Zhang, "Distributed error correction coding scheme for low storage blockchain systems," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7054–7071, Aug. 2020.
- [11] R. K. Raman and L. R. Varshney, "Coding for scalable blockchains via dynamic distributed storage," *IEEE/ACM Trans. Netw.*, vol. 29, no. 6, pp. 2588–2601, Dec. 2021.
- [12] C. Yang, X. Wang, and A. Ashikhmin, "Storage and communication tradeoff for wireless coded blockchains," *IEEE Syst. J.*, vol. 16, no. 2, pp. 2911–2922, Jun. 2022.
- [13] M. Cebe, B. Kaplan, and K. Akkaya, "A network coding based information spreading approach for permissioned blockchain in IoT settings," in *Proc. ACM Mobiquitous*, 2018, pp. 470–475.
- [14] N. Chawla, H. W. Behrens, D. Tapp, D. Boscovic, and K. S. Candan, "Velocity: Scalability improvements in block propagation through rateless erasure coding," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, Seoul, South Korea, 2019, pp. 447–454.
- [15] M. Braun, A. Wiesmaier, N. Alnahawi, and J. Beibler, "On message-based consensus and network coding," in *Proc. 12th Int. Conf. Netw. Future (NoF)*, Coimbra, Portugal, 2021, pp. 1–9.
- [16] L. Zhang, T. Wang, and S. C. Liew, "Speeding up block propagation in Bitcoin network: Uncoded and coded designs," *Comput. Netw.*, vol. 206, Apr. 2022, Art. no. 108791.
- [17] M. Al-Bassam, A. Sonnino, and V. Buterin, "Fraud and data availability proofs: Maximising light client security and scaling blockchains with dishonest majorities," 2018, *arXiv:1809.09044*.
- [18] P. Santini, G. Rifaiani, M. Battaglioni, F. Chiaraluce, and M. Baldi, "Optimization of a Reed-Solomon code-based protocol against blockchain data availability attacks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Seoul, South Korea, 2022, pp. 31–36.
- [19] M. Yu, S. Sahraei, S. Li, S. Avestimehr, S. Kannan, and P. Viswanath, "Coded Merkle tree: Solving data availability attacks in blockchains," in *Proc. Int. Conf. Financ. Cryptogr. Data Security*, 2020, pp. 114–134.
- [20] D. Mitra, L. Tauz, and L. Dolecek, "Overcoming data availability attacks in blockchain systems: Short code-length LDPC code design for coded Merkle tree," *IEEE Trans. Commun.*, vol. 70, no. 9, pp. 5742–5759, Sep. 2022.
- [21] D. Mitra, L. Tauz, and L. Dolecek, "Polar coded Merkle tree: Improved detection of data availability attacks in blockchain systems," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Espoo, Finland, 2022, pp. 2583–2588.
- [22] S. Li, M. Yu, C.-S. Yang, A. S. Avestimehr, S. Kannan, and P. Viswanath, "PolyShard: Coded sharding achieves linearly scaling efficiency and security simultaneously," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 249–261, 2020.

- [23] B. Sasidharan and E. Viterbo, "Private data access in blockchain systems employing coded sharding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2021, pp. 2684–2689.
- [24] D. S. Gadiraju, V. Lalitha, and V. Aggarwal, "Secure regenerating codes for reducing storage and bootstrap costs in sharded blockchains," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, 2020, pp. 229–236.
- [25] S. B. Wicker and V. K. Bhargava, *Reed–Solomon Codes and Their Applications*. Piscataway, NJ, USA: Wiley-IEEE Press, 1994.
- [26] R. Gallager, "Low-density parity-check codes," *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, 1962.
- [27] P. Trifonov, "Efficient design and decoding of polar codes," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3221–3227, Nov. 2012.
- [28] "Bitcoin nodes number since 2015." 2023. [Online]. Available: <https://coin.dance/nodes>
- [29] M. Luby, "LT codes," in *Proc. 43rd Symp. Found. Comput. Sci.*, 2002, pp. 271–280.
- [30] S. Kadhe, J. Chung, and K. Ramchandran, "SeF: A secure fountain architecture for slashing storage costs in blockchains," 2019, *arXiv:1906.12140*.
- [31] L. Quan and Q. Huang, "Transparent coded blockchain," in *Proc. 15th Int. Conf. Emerg. Netw. Exp. Technol.*, New York, NY, USA, 2019, pp. 12–13.
- [32] R. Pal, "Fountain coding for bootstrapping of the blockchain," in *Proc. IEEE Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bengaluru, India, 2020, pp. 1–5.
- [33] Q. Huang, L. Quan, and S. Zhang, "Downsampling and transparent coding for blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2139–2149, Jul./Aug. 2022.
- [34] A. Tiwari and V. Lalitha, "Secure raptor encoder and decoder for low storage blockchain," in *Proc. IEEE Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bengaluru, India, Jan. 2021, pp. 161–165.
- [35] A. Shokrollahi, "Raptor codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2551–2567, Jun. 2006.
- [36] D. J. MacKay, "Fountain codes," *IEE Proc. Commun.*, vol. 152, no. 6, pp. 1062–1068, 2005.
- [37] I. Hussain, M. Xiao, and L. K. Rasmussen, "Error floor analysis of LT codes over the additive white gaussian noise channel," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, 2011, pp. 1–5.
- [38] "Bitcoin nodes number," 2023. [Online]. Available: <https://bitnodes.io/dashboard/?days=730>
- [39] X.-Y. Hu, E. Eleftheriou, and D.-M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.
- [40] X. Li, M. C. Huang, K. Shen, and L. Chu, "A realistic evaluation of memory hardware errors and software system susceptibility," in *Proc. USENIX Annu. Tech. Conf.*, Boston, MA, USA, 2010, pp. 75–88.
- [41] D. Karlis and I. Ntzoufras, "Bayesian analysis of the differences of count data," *Stat. Med.*, vol. 25, no. 11, pp. 1885–1905, 2006.
- [42] T. Richardson, "Error floors of LDPC codes," in *Proc. 41st Annu. Allerton Conf. Commun. Control Comput.*, 2003, pp. 1426–1435.
- [43] "Bitcoin P2P network." 2023. [Online]. Available: https://developer.bitcoin.org/reference/p2p_networking.html
- [44] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin, Las Vegas, NV, USA, White Paper, 2008.
- [45] "Bitcoin Wiki." 2023. [Online]. Available: <https://en.bitcoin.it/wiki/>