Escaping From Consensus: Instantly Redactable Blockchain Protocols in Permissionless Setting

Xinyu Li, Jing Xu, Lingyuan Yin, Yuan Lu, Qiang Tang, and Zhenfeng Zhang

Abstract—Blockchain technologies have drawn a lot of attentions, and its immutability is paramount to applications requiring persistent records. However, tremendous real-world incidents have exposed the harm of strict immutability, such as the illicit data stored on Bitcoin and the loss of millions of dollars in vulnerable smart contracts. Moreover, "Right to be Forgotten" has been imposed in new General Data Protection Regulation (GDPR) of European Union, which is incompatible with blockchain's immutability. Therefore, it is imperative to design efficient redactable blockchain in a controlled way. In this paper, we present a generic design of redactable blockchain protocols in the permissionless setting, applied to both proof-of-stake and proof-of-work blockchains. Our protocol can (1) maintain the same adversary bound requirement as the underlying blockchain, (2) support various network environments, (3) offer public verifiability for any redaction, and (4) achieve instant redaction, even only within one slot in the best case, which is desirable for redacting harmful data. Furthermore, we define the first ideal protocol of redactable blockchain and conduct security analysis following the language of universal composition. Finally, we develop a proof-of-concept implementation showing that the overhead remains minimal for both online and re-spawning nodes, which demonstrates the high efficiency of our design.

Index Terms—Blockchain, proof-of-stake, proof-of-work, redactable blockchain

1 Introduction

Blockchain has been gaining increasing popularity and acceptance by a wider community, which enables Internet peers to jointly maintain a ledger. One commonly mentioned feature of blockchain is immutability (or untamperability) in mass media, and immutability of blockchain is paramount to certain applications to ensure keeping persistent records. However, in many other applications, such strict immutability may not be desirable or even hinder a wider adoption for blockchain technology.

First, since everyone in the Internet is able to write to permissionless blockchain, some malicious users may abuse the ability to post arbitrary transaction messages [1]. It could be the case that the data stored on the ledger might be sensitive, harmful or illegal. For instance, Bitcoin blockchain has been reported to contain illicit contents like leaked private keys, materials that infringe on intellectual rights, and even child sexual abuse images [2]. It is clear that allowing those contents to be publicly available for everyone to access is unacceptable. They may affect the life of people forever, and hinder broader blockchain applications [3] in areas involving data such as government records [4] and social media [5].

On the other hand, as a full node, maintaining the whole ledger will also bear with the burden of maintaining those potentially illicit contents, thus the risk of being prosecuted for possessing and distributing illicit information increases. Concerning about above liability, honest nodes may opt-out as a full node, which in turn hurts the security of permissionless blockchain itself.

Indeed, with the adoption of the new European Union's General Data Protection Regulation (GDPR) [6] in May 2018, it is no longer compatible with current blockchains such as Bitcoin and Ethereum to record personal data [7]. In particular, GDPR imposes the "Right to be Forgotten" as a key Data Subject Right, i.e., the data subject shall have the right to require the controller to erase personal data concerning him/her. How to facilitate wider adoption of blockchain while complying with new regulations on personal data becomes a natural challenge.

Second, in certain systems, some flexibility is necessary to hedge with user mistakes or accidents to protect the system integrity. For example, in database, a rollback is the operation which returns the database to some previous state [8]. One other example is misdirected payment. According to statistics, around a quarter of people have

- *Xinyu Li is with the Department of Computer Science, University of Hong Kong, Pok Fu Lam, Hong Kong, and also with the State Key Laboratory of Cryptology, Beijing 100878, China. E-mail: xinyuli1920@gmail.com.*
- *Jing Xu, Yuan Lu, and Zhenfeng Zhang are with the Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China. E-mail: {xujing, luyuan, zhenfeng}@iscas.ac.cn.*
- *Lingyuan Yin is with the Institute of Industrial Internet and Internet of Things, China Academy of Information and Communications Technology, Beijing 100191, China. E-mail: lingyuan2018@iscas.ac.cn.*
- *Qiang Tang is with the School of Computer Science, The University of Sydney, Sydney, NSW 2006, Australia. E-mail: qiang.tang@sydney.edu.au.*

Manuscript received 5 December 2021; revised 31 July 2022; accepted 20 September 2022. Date of publication 10 October 2022; date of current version 1 September 2023.
The work of Xinyu Li was supported in part by the National Key R&D Program of China under Grant 2020YFB1005801, and in part by Innovation Technology Fund under Grant ITS/224/20FP. The work of Jing Xu was supported in part by the National Natural Science Foundation of China under Grant 62172396. The work of Yuan Lu was supported in part by the National Natural Science Foundation of China under Grant 62102404, and in part by Youth Innovation Promotion Association CAS. The work of Qiang Tang was supported in part by gifts from Ethereum Foundation, Stellar Foundation and Protocol Labs. The work of Zhenfeng Zhang was supported in part by the National Key R&D Program of China under Grant 2022YFB2701600.
(Corresponding author: Jing Xu.)
Digital Object Identifier no. 10.1109/TDSC.2022.3212601

accidentally paid the wrong person [9]. A voluntary code of conduct has been introduced by the Payments Council (part of U.K. finance) for building societies and banks when the misdirected payments appear. If a user who made the mistake notifies his bank fast enough, and provides clear evidence, "his bank will contact the receiving bank on his behalf to request the money isn't spent, so long as the recipient doesn't dispute the claim" [9]. In the centralized banking system, there may still exist options to reverse incorrect transactions, while if similar mistakes happen in decentralized cryptocurrencies, thing would become much more complicated even if it is ever feasible.

We would like to stress that though blockchain offers a more reliable trust model as no single entity can fully control the system, however, it by no means insists on a strict immutability as an inherent property that is derived from consensus.

In fact, when the notorious DAO vulnerability was exploited, 3,641,694 Ethers (worth of about 79 million US dollars) were stolen due to the flaws of Ethereum and DAO contract [10], the financial losses have to be resolved by patching the vulnerability and "rollback" via a hard fork (majority of the miners are suggested by the Ethereum developers to adopt a newer client and create a fork of the chain from a state before the vulnerable contract got deployed). Hard forks also happened before, e.g., for Bitcoin when upgrading its protocol [11]. Of course, hard forks are not desirable as they may split the community and are very costly to implement.

Following above discussions, there exists a strong need to redact content of blockchain in exceptional cases, as long as the redaction proposal is clearly examined and satisfies full transparency and accountability (not determined by any single entity, and sufficient confidence can be gained that at least some honest users have approved the proposal).

1.1 Related Work

There exist several works that start exploring feasible methods for redacting blockchain.

A straightforward approach is to initiate a hard fork, which essentially requires all community members to vote by action (whether to follow the new fork). Doing this sometimes brings the risk of dividing the community, e.g., Bitcoin has a dozen forks, each of which now forms its own community. Moreover, such a procedure is extremely costly and slow, which normally takes multiple months to finalize [12], and if the redaction needs to touch an ancient block, growing a longer fork may take even much longer.

Ateniese et al. [13] presented the concept of redactable blockchain in the permissioned setting. They use a chameleon hash function [14] to compute hash pointer, i.e., when redacting a block, a trusted party (e.g., the certificate authority) with access to the chameleon trapdoor key can efficiently compute a collision for the hash of the block. By this way, the block data can be modified while maintaining the chain consistency, and moreover a large consultancy company has commercially adopted that solution [15][16]. Later, in order to support controlled and fine-grained redaction of blockchain, Derler et al. [17] proposed a new primitive called policy-based chameleon hash (PCH), where arbitrary collisions for a given hash can be found by anyone with the trapdoor satisfying the policy.

Puddu et al. [18] also presented a redactable blockchain, called μ chain. In μ chain, the sender can encrypt all different versions of his/her transactions accompanied by a redaction policy, the unencrypted version is regarded as the valid transaction, and the keys for decryption are secretly split into shares for miners. When receiving a request for redacting a transaction, miners first check it according to redaction policy established by the sender, then compute the appropriate decryption key by executing a multi-party computation protocol, and finally decrypt the alternate version of the transaction as a new valid version.

Their solutions mainly focus on the permissioned setting, while in permissionless setting, there is no single trusted entity and users can join and leave the blockchain system at any moment, and thus their solutions [13][18] may suffer from scalability issues when secretly sharing the trapdoor/decryption key among miners by a multi-party computation protocol. In addition, the malicious users who establish redaction policy can escape redaction, or even break the stability of transactions by the influence among transactions [17][18]. Moreover, public accountability of redaction cannot be provided in their solutions, and users are not aware whether any redaction has happened.

Recently, Deuber et al. [19] gave the first construction of redactable blockchain protocol in the permissionless setting without additional trust assumption and heavy cryptographic tools. The construction relies on a consensus based voting, where any redaction can only be approved if enough votes for approving the redaction are collected. Each user can verify whether a redaction proposal is approved by checking the number of votes on the chain. Similarly, Thyagarajan et al. [20] proposed a generic protocol called Reparo on top of any blockchain to perform redactions, where the block structure remains unchanged by introducing external data structures to store block contents.

Their solutions are elegant, however, the voting period is very long, for example, 1024[1] consecutive blocks are required in their Bitcoin instantiation, which takes about 7 days to confirm and publish a redaction block. Nevertheless, in practice, it is inefficient to redact sensitive data after such a long time, and it is also difficult to ask newly joined users in the system maintain these redactions. In addition, the threshold of votes in their solutions relies on chain quality of underlying blockchain, concretely, if the threshold of votes approaches 1/2 (as in their Bitcoin instantiation), the chain quality also approaches 1/2. However, according to [21], the chain quality is close to $1-\frac{\rho}{1-\rho}$, where we denote by ρ the fraction of computational power the adversary controls, and thus redactable blockchains [19][20] actually tolerate $\rho < 1/3$ adversary.

Further, in the permissionless setting it seems unreasonable to have a trusted party holding certain trapdoor to modify the chain (like in the permissioned setting [13]). It follows that we have to choose a committee to jointly make the decision. Indeed, existing works [19][20] pick one committee member per block who can only make one vote. For

1. 1024 is suggested in [19][20] to guarantee honest majority of committee members with negligible violation probability.

this reason, the time needed for one redaction will be at least linear to $T \cdot t$, where T is the committee size, and t is the block generation time of the underlying blockchain. However, in order to ensure honest majority, the committee size has to be substantially large (e.g., at least 1024 in [19][20]), which in turn leads to a rather slow redaction.

Based on the above discussion we would like to study a central question in this paper:

Can we design a redactable blockchain in the permissionless setting such that

1) *the redaction can be completed quickly (i.e., within time $c \cdot t$ for a small constant c), and moreover*
2) *the redaction would not impose any additional restriction on the adversarial rate of the underlying blockchain*?

1.2 Our Contributions

In this work we answer the above question in the affirmative by introducing a new redaction mechanism. In particular, we design redactable blockchain protocols in the permissionless setting such that the redaction could be *instant*, which means that the redaction time is at most $c \cdot t$ for a small c. Ideally $c = 1$, and thus the redaction could be as fast as the underlying chain! Moreover, the selection of committee for voting does not rely on the chain quality any more, and thus the assumption of $1/3$ adversarial rate is avoided.

More specifically, the contributions of this work are summarized as follows.

A Brand-New Redaction Strategy. The core idea of this work is to decouple the voting stage from the underlying consensus layer. Observe that existing work emulates the Bitcoin design, viewing block generation as a random walk that eventually converges to the longest chain, thus directly binding the committee selection to the consensus (treating each block as a random draw of a peer) requires a long convergence time (large number of blocks). But in certain blockchain design (such as Algorand [22]), one may use each block to randomly draw a large number of committee members, then let the committee members to run BFT to determine next block.

Inspired by this simple observation, our strategy proceeds in two steps. First, instead of selecting just one committee member in each slot like in existing works, we directly use the underlying component relying on stake or computational power to select a large enough committee randomly among all parties, where we set the committee size to guarantee that a sufficient fraction of committee members are honest. Then the selected committee members would vote for one redaction request which would be approved if the votes exceed a threshold value. Intuitively, in our strategy both the committee selection process and voting period occur outside of the consensus layer (i.e., the block generation), which makes it possible to achieve instant redaction and $1/2$ adversary bound as the underlying blockchain.

Generic Construction of Blockchain With Instant Redaction. Based on the new redaction strategy, we propose a generic construction of blockchain with instant redaction. In particular, in the first phase for committee selection, the functionality of the committee election (resp. committee verification) is refined by the general functions Cmt (resp. $\mathsf{VerifyCmt}$). However, it is challenging to make Cmt and $\mathsf{VerifyCmt}$ suitable for different instantiations such as PoS and PoW. In our approach, whether a party being elected as the committee member is based on his voting period instead of his current slot, i.e., the first slot sl of his voting period as the input parameter of functions, which makes committee selection more generic.

Then in the second phase, each committee member would vote by signing on the hash of the candidate edited block and diffuse the vote (i.e., the signature as well as the proof of committee members) to the network. To avoid the impact of network delays and collect enough votes, we set the maximum time of collecting votes (a.k.a. voting period) to be w slots, which is independent of block generation time. The leader of current slot (during voting period) adds votes collected and corresponding succinct proofs to his block.

On a high level, any party can propose a candidate edited block B_j^* for B_j in the chain, and only committee members in the voting period can promptly process the edit request once receiving B_j^*, including voting for B_j^* and broadcasting their votes and corresponding proofs; the slot leader during the voting period adds these votes and proofs to its block data collected and proposes a new block; if votes are approved by the redaction policy (e.g., voting bound in the voting period), B_j is replaced by B_j^*.

Note that our redaction method can achieve instant redaction, if the underlying blockchain progresses fast, then redaction will also be fast. Moreover, for the new joined user, it is also fast to verify a redaction in the blockchain. Furthermore, our redactable protocol can tolerate an adversary with less than 50% computational power (or stake) as the underlying blockchain, which is optimal in the blockchain protocol. This also means our approach will not reduce the adversary bound requirements of all blockchain protocols. Our protocol can also provide accountability for redaction like [19][20], i.e., any edited block on the chain is publicly verifiable. In addition, multiple redactions per block can be performed throughout the execution of the protocol.

Simulation Based Security Analysis of Redactable Blockchain. Unlike most of existing works which only analyze the impact brought by the redaction operation, we give the first systematic and comprehensive analysis of the redactable blockchain as it is. To characterize the security properties of redactable blockchains more precisely and analyze them rigorously, we define for the first time the *ideal protocol* Π_{ideal} of a redactable blockchain in the simulation based paradigm. Our proof first considers an idealized functionality $\mathcal{F}_{tree}$ which keeps a record of the valid chains at any time and is invoked by Π_{ideal}. In $\mathcal{F}_{tree}$, we use $\mathcal{F}_{tree}.\mathsf{committee}$ query to obtain the committee members, and $\mathcal{F}_{tree}.\mathsf{redact}$ query to redact the blockchain under certain conditions. In fact, separating these two queries in our idealized functionality ensures generality and *instant* redaction of redactable protocol. Moreover, $\mathcal{F}_{tree}$ models the ability of voting period changing with w.

For the proof, we first show that Π_{ideal} indeed satisfies the redactable common prefix property defined in [19], and the usual chain quality and chain growth properties [23]. Essentially, the redactable common prefix property ensures that any edited block which violates original common prefix should satisfy the redaction policy $\mathcal{RP}$. However, different from the redaction policy in [19] considering the consecutive ℓ blocks as the redaction period (which is not suitable

TABLE 1
Comparison of Our Redaction Solution With Existing Works

	system-scale MPC	network compatibility[1]	adversary tolerance for PoW[2]	public verifiability	redaction time/slots[3]
Ateniese et al. [13]	required	yes	1/2	no	N/A
Puddu et al. [18]	required	yes	1/2	no	N/A
Derler et al. [17]	not required	yes	1/2	no	N/A
Deuber et al. [19]	not required	yes	1/3	yes	513
Thyagarajan et al. [20]	not required	yes	1/3	yes	513
Ours	not required	yes	1/2	yes	PoS: 1 PoW: ≤ 20

[1] *Network compatibility implies that the redaction solution does not impose any network assumption on the underlying blockchain.*
[2] *We only list the required adversary tolerance in PoW setting, while in PoS setting, all of adversary tolerance is 1/2 and thus omitted in the table.*
[3] *We evaluate the time one redaction can be completed in the best-case, where N/A is the abbreviation for the phrase "Not Applicable". In [19] and [20], the voting period is ℓ (instantiated to 1024 slots), and in the best-case more than one half of slots (i.e., 513 slots) are needed for the redaction. In our PoS construction, the redaction can be completed within just one slot if the underlying network is well enough. While in our PoW construction, the selection of committee members is completed in r slots, where r is instantiated to 20 in Section 5.2, thus in the best-case 20 slots are enough for one redaction. Note that for all solutions in the table, one completed redaction can only be stable on the chain after several new blocks have been generated, e.g., six blocks in Bitcoin.*

for *instant* redaction), our $\mathcal{RP}$ requires votes are embedded in at most w slots, where ℓ is the committee size and w is the number of slot in the voting period. Then we show that the real-world protocol (i.e., our redactable blockchain protocol) can securely emulate the ideal protocol, namely any attack against the real-world protocol also implies an valid attack against the ideal protocol Π_{ideal}.

Instantiations and Performance Evaluation. We demonstrate that our construction is generic by presenting concrete instantiations of the general functions Cmt and $\mathsf{VerifyCmt}$ on PoS and PoW (in principle, we may also instantiate via proof of space). Our instantiations can achieve the optimal $1/2$ adversary bound as the underlying blockchain and moreover support various network environments even semi-synchronous and asynchronous networks, and thus provide compatibility with the underlying blockchain.

In PoS instantiation, how to select a committee and set the voting bound to ensure that adversarial votes would never reach the bound is the main challenge. Our core idea is to select a committee with a fixed (expected) size T where the number of malicious members is guaranteed to be strictly less than $1/2.T$. Thus no matter how large the actual committee would be we can always set the voting bound to be $1/2.T$. Specifically, we leverage the hash function or verifiable random function (VRF) to sample sufficient number of committee members according to stake distribution as in [22]. Different from $1/3$ committee adversary tolerance in [22], we ensure the majority of committee members are honest by changing the constraint conditions on the expected committee size T.

While in PoW instantiations, we have to face more challenges. First, different from PoS, an adversary during the procedure of collecting votes still can continue to solve the computational puzzle, which leads to much computational power than honest users. Second, if an adversary in PoW withholds some blocks, and once these blocks are put to the chain, the adversary may have more advantage of computing the corresponding puzzles in advance. Finally, in semi-synchronous and even asynchronous networks, the actual number of committee members is impossible to be determined in advance, and thus it is hard to choose the voting bound. To resolve these *instant* redaction challenges in PoW blockchain, we propose a new approach to design redactable PoW blockchain compatible with various networks, and select committee members by finding solutions to a well-chosen easy puzzle (i.e., *bigger* difficulty parameter D), so that during regular mining procedure many easier puzzle solutions will be produced as a byproduct. In particular, according to "no long block withholding" lemma [21, Lemma 6.10], we increase the rounds of committee election to guarantee honest majority of committee members, even though the adversary has extra time advantage to find easier puzzle solutions. We also set the expected committee size satisfying two conditions: 1) a sufficient fraction of committee members are honest; and 2) malicious committee members cannot generate enough votes and complete the redaction of blockchain.

In addition, we give detailed analysis of each instantiation, and all of them satisfy the condition that committee members are chosen randomly and majority of the committee members are honest. The comparison of our construction with some related works is also shown in Table 1.

We also develop a proof-of-concept (PoC) implementation of our redaction approach, and conduct a series of experiments to evaluate the overhead after applying our redaction mechanism. The results show the high efficiency of our design. In particular, compared to the underlying blockchain (which simulates Cardano SL), the overhead incurred by redactions remains minimal for both online nodes and re-spawning nodes. For the online nodes, they only have to face a cheap and constant overhead (i.e., an extra latency of 0.8 second) to validate a newcoming block including a proof on redaction and then perform corresponding editing. For the re-spawning nodes, they can efficiently validate a redactable chain despite of many edited blocks. For example, when less than 6.25% blocks are edited, the time of validating a redactable chain is nearly same to that of validating an immutable chain. Remarkably, even if in the extremely pessimistic case that half blocks are edited, the performance of validating such a redacted chain remains acceptable (about 5X more than validating an unedited chain).

1.3 Outline

In Section 2 we recall the formulation of blockchain and the desired security goals. In Section 3 we give a generic construction of redactable blockchain and in Section 4 we give the simulation based security analysis. Section 5 presents two instantiations of the generic construction for both PoS and PoW. Section 6 elaborates the efficiency evaluation of redactable blockchain, and we conclude in Section 7.

2 Formal Abstraction of Blockchain

First of all we give the formal abstraction for blockchain protocols based on the approach of Garay et al. [23] and Pass et al. [21][24].

2.1 Protocol Execution Model

We assume a protocol specifies a set of instructions for the interactive Turing Machines (also called parties) to interact with each other. We denote by $\mathcal{Z}$ an environment that directs the execution of the protocol and can activate an honest or corrupt party. Honest parties would follow the protocol specifications and broadcast messages to each other. Messages broadcasted between honest parties cannot be modified by the adversary $\mathcal{A}$, however, can be *delayed* or *reordered* arbitrarily by $\mathcal{A}$ as long as he would deliver all messages eventually.

We follow the nice results on the foundation of blockchains [25][26] to assume a global clock, which can be seen as an equivalent notion of the height of the latest chain (or more specifically, the latest slot number in the blockchain). Notation-wise, by $Time$, we denote that a blockchain node invokes the global clock to get the current time. A protocol's execution proceeds in atomic time units. At the beginning of every time unit, honest parties receive inputs from an environment $\mathcal{Z}$; while at the end of every time unit, honest parties send outputs to $\mathcal{Z}$. $\mathcal{Z}$ can spawn, corrupt, and kill parties during the execution as follows.

- During the execution of the protocol, $\mathcal{Z}$ can *spawn* fresh parties that are honest or corrupt at any moment.
- $\mathcal{Z}$ can *corrupt* an honest party and in turn obtain its local state.
- $\mathcal{Z}$ can *kill* a party i which is honest or corrupt, or to say remove i from the protocol execution.

2.2 Blockchain Protocol

We recall basic definitions of blockchain [27]. The blockchain system consists of n parties $\mathcal{P}_1, \ldots, \mathcal{P}_n$ and each party $\mathcal{P}_i$ possesses a public/secret key pair (pk_i, sk_i). We assume without loss of generality all system users know the public keys $pk_1, \ldots, pk_n$. We split the protocol execution into time units called slots. A block in the blockchain is denoted by the form $B_j := (header_j, d_j)$, where $header_j = (sl_j, st_j, G(d_j), \pi_j)$ denotes the block header information, and d_j denotes the block data. In $header_j$, $sl_j \in \{sl_1, \ldots, sl_R\}$ is the slot number, st_j is the hash of the previous block header denoted by $H(header_{j-1})$, $G(d_j)$[2] denotes the state of the block data, and π_j contains some special header data for the block (e.g., in PoS, it's a signature on $(sl_j, st_j, G(d_j))$ computed under the secret key of slot leader generating the block, while in PoW, it is a nonce for the puzzle of PoW). Here H and G denote two collision-resistent hash functions.

A valid blockchain $chain$ is simply a sequence of blocks $B_0, \ldots, B_m$, where B_0 is called the genesis block containing auxiliary information and the list of parties identified by their respective public-keys. We use $\mathsf{Head}(chain)$ to denote the head of $chain$ (i.e., B_m). In a basic blockchain protocol, the users always update their current chain to the longest valid one they have obtained. We use the function $\mathsf{eligible}(\mathcal{P}_i, sl)$ to judge the leader election process at the slot sl, that is, if $\mathsf{eligible}(\mathcal{P}_i, sl) = 1$, then $\mathcal{P}_i$ is assigned to be an eligible leader and can create a block at sl and broadcast the updated $chain$, where the leader election can be achieved according to specific blockchain protocol.

2.3 Security Properties of Blockchain

We use $\mathsf{view} \leftarrow \mathsf{EXEC}^{\Pi}(\mathcal{A}, \mathcal{Z}, \lambda)$ to denote the trace of a randomly sampled execution of the blockchain protocol Π where λ is the security parameter, and $|\mathsf{view}|$ denote the number of time units in the protocol execution. Specifically, view contains the concatenation of all parties' view (i.e., all inputs/outputs, and messages sent/received by the parties in the execution). Denote by $\mathsf{chain}_i^t(\mathsf{view})$ the party i's output to $\mathcal{Z}$ at time unit t in view, where chain denotes an ideal blockchain where each block consists of transactions of the corresponding block of $chain$. The notation $\mathsf{chain}[i]$ denotes ith block of chain, $\mathsf{chain}[: l]$ denotes the prefix of chain consisting of the first l blocks, $\mathsf{chain}[l :]$ denotes the sequence of blocks at length that is not less than l, and $\mathsf{chain}[: -l]$ denotes the chain after removing the last l blocks.

We recall common security properties that blockchain protocols should satisfy following the approach of [24][28]. We refer the reader to the full version of this paper [29] for a more detailed definition.

Common Prefix. Informally speaking, considering chains of two honest parties at different time, the common prefix property requires that the shorter chain except for the last k_0 blocks is the prefix of the longer chain.

Definition 1. *(Common Prefix). For any two honest parties i and j, any $t \leq t'$ and any $k \geq k_0$, if the first $|\mathsf{chain}_i^t(\mathsf{view})| - k$ records of $\mathsf{chain}_i^t(\mathsf{view})$ are the prefix of $\mathsf{chain}_j^{t'}(\mathsf{view})$, then we say the blockchain satisfies the k_0-common prefix.*

Chain Quality. Informally speaking, the chain quality property requires that the ratio of adversarial blocks is bounded by $1 - \mu$.

Definition 2. *(Chain Quality). For any honest party i, any time t and any $k \geq k_0$, in the consecutive sequence of k blocks $\mathsf{chain}[j + 1..j + k] \subseteq \mathsf{chain}_i^t(\mathsf{view})$, if the ratio of honest blocks is at least μ, then we say the blockchain satisfies the (k_0, μ)-chain quality.*

Chain Growth. Informally speaking, the chain growth property requires that the chain grows in proportion to the time slots.

Definition 3. *(Chain Growth). For any two honest parties i and j, any time t and t_0, if $|\mathsf{chain}_j^{t+t_0}(\mathsf{view})| - |\mathsf{chain}_i^t(\mathsf{view})| \geq \tau \cdot t_0$, then we say the blockchain satisfies the τ-chain growth.*

3 Redacting Blockchain

In this section we propose a generic construction that converts a basic blockchain into redactable blockchain protocol. We also extend the redactable protocol to accommodate

2. In practice $G(d_j)$ means the Merkle root of the block data.

multiple redactions for each block in Appendix D, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TDSC.2022.3212601, and also the full version of this paper [29].

3.1 Overview of Redactable Blockchain Protocol

We construct our redactable blockchain protocol Γ by extending the basic blockchain protocol. We assume that the fraction of the computational power (or stake) held by honest users in the blockchain is h (a constant greater than $1/2$). We denote by w the needed slots for votes diffusion, where w can be selected based on specific environments to guarantee the votes can be received by all users after w slots with a greater probability. For every $sl \bmod w = 0$, we also use the slots between sl and $sl + w - 1$ to denote the voting period for the editing proposal.

In addition, we use $\mathsf{Cmt}(chain, sl, \mathcal{P}, para)$ to denote a function that examines whether $\mathcal{P}$ is the committee member in the voting period beginning from sl and outputs $(c, proof)$, where $para$ is an optional parameter in specific instantiations, c is the weight of $\mathcal{P}$ in the committee, $proof$ is committee member proof. Correspondingly, there is some application-specific function $\mathsf{VerifyCmt}(chain, sl, c, proof, para')$ to verify $(c, proof)$, where $para'$ is the public parameter related to specific applications. In the committee selected by Cmt, we set the fraction of the computational power (or stake) held by honest users is at least η ($\eta > 1/2$).

First, a redaction policy is introduced to determine whether an edit to the blockchain should be approved or not.

Definition 4. *(Redaction Policy $\mathcal{RP}$). We say that an edited block B^* at the slot sl satisfies the redaction policy, i.e., $\mathcal{RP}(chain, B^*, sl) = 1$, if the number of votes on B^* during a voting period is more than a threshold value,*[3] *where each block embedding votes is in $chain[: -k_0]$, and k_0 is the common prefix parameter.*

Next, in order to accommodate editable data, we extend the above block structure to be of the form $B := (header, d)$, where $header = (sl, st, G(d), ib, \pi)$ and the newly added item ib denotes the initial state of the block data. Specifically, if a blockchain $chain$ with $\mathsf{Head}(chain) = (header, d)$ is updated to a new longer blockchain $chain' = chain||B'$, the newly attached block $B' = (header', d')$ sets $header' = (sl,' st,' G(d'), ib,' \pi')$ with $st' = H(header)$ and $ib' = G(d')$. Notice that in order to maintain the link relationships between an edited block and its neighbouring blocks, inspired by the work [19] we introduce ib to represent the initial and unedited state of block, i.e., $ib = G(d_0)$ if original block data is d_0 in the edited block $B = (header, d)$, where $header = (sl, st, G(d), ib, \pi)$.

Generally, a blockchain $chain = (B_1, \ldots, B_m)$ can be redacted by the following steps, which are pictorially presented in Fig. 1.

1) *Proposing a Redaction.* If a user wants to create an edit proposal to block B_j in $chain$, he parses $B_j = (header_j, d_j)$ with $header_j = (sl_j, st_j, G(d_j), ib_j, \pi_j)$, replaces d_j with the new data d_j^*, and then broadcasts the candidate block $B_j^* = (header_j^*, d_j^*)$ to the network, where $header_j^* = (sl_j, st_j, G(d_j^*), ib_j, \pi_j)$, and d_j^* is the empty data if the user wants to remove all data from B_j.
2) *Updating the Editing Pool.* Upon receiving B_j^* from the network, every party $\mathcal{P}_i$ first validates whether B_j^* is a valid candidate editing block, and stores it in his own editing pool $\mathcal{EP}$ if it is. Notice that each candidate editing block in the pool $\mathcal{EP}$ has a period of validity t_p. At the beginning of each new slot sl, every party $\mathcal{P}_i$ tries to update his own editing pool $\mathcal{EP}$. Specifically, for every candidate editing block B_j^* in $\mathcal{EP}$: (i) $\mathcal{P}_i$ checks whether B_j^* has expired or not, and if it is, $\mathcal{P}_i$ removes B_j^* from $\mathcal{EP}$; (ii) $\mathcal{P}_i$ computes $\mathcal{RP}(chain, B_j^*, sl_j)$, and if it outputs 1, $\mathcal{P}_i$ removes B_j^* from $\mathcal{EP}$.
3) *Voting for Candidate Editing Blocks.* For each candidate editing block B_j^* in $\mathcal{EP}$, $\mathcal{P}_i$ checks whether he has voting right in the current voting period, which is determined by $\mathsf{Cmt}(chain, \lfloor sl'/w \rfloor * w, \mathcal{P}_i, para)$, where sl' is the current slot, and $\lfloor sl'/w \rfloor * w$ denotes the first slot in the current voting period. If it outputs $(c, proof)$ and $c \neq 0$, $\mathcal{P}_i$ broadcasts $(c, proof)$ and the signature sig on $H(B_j^*)$ as his votes.
4) *Proposing New Blocks.* The slot leader of sl' creates a block and broadcasts $chain$ in exactly the same manner as the basic blockchain, if his editing pool is empty. Otherwise, for the candidate block B_j^* in the editing pool, the leader tries to collect and validate the votes on B_j^* in the voting period by using subprotocol $\mathsf{collectVote}$ (Fig. 3). If $\mathsf{collectVote}$ returns $\mathsf{vote-proof}$ at slot sl', the leader of sl' adds $\mathsf{vote-proof}$ to his block data, creates a new block and broadcasts $chain$.
5) *Editing a Block.* For each B_j^* in the editing pool $\mathcal{EP}$, the users check whether $\mathcal{RP}(chain, B_j^*, sl_j) = 1$. If yes, they replace $chain[j]$ with B_j^* and remove B_j^* from $\mathcal{EP}$.

3. The threshold value would be set according to different committee selection methods such that it is more than the maximum number of votes the adversary can produce.

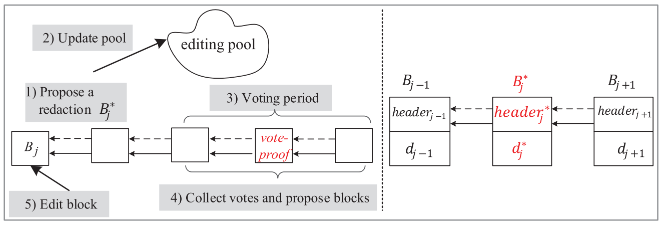

Fig. 1. Overview of our redactable blockchain protocol.

In the right sub-figure of Fig. 1, B_j is modified into B_j^*, and we now show the link relationship between neighbouring blocks. One block is linked to its neighbouring block by two links — old link and new link, which are denoted by the solid arrow and dashed arrow correspondingly as shown in the figure. Without loss of generality we assume B_{j-1} has not been modified yet, then the old link between B_{j-1} and B_j^* still holds, that is, $st_j = H(header_{j-1})$. While the case for the new link relationship between B_j^* and B_{j+1} is different due to the fact that $st_{j+1} = H(header_j)$ however $st_{j+1} \neq H(header_j^*)$, then we can turn to check the old link

$st_{j+1} = H(sl_j, st_j, ib_j, ib_j, \pi_j)$. We would give more details in Section 3.2.

Redactable blockchain protocol offers public verifiability. Concretely, to validate a redactable chain, users can check all blocks and the link relation between neighbouring blocks as in the immutable blockchain protocol. Once a "broken" link between blocks is found, users check whether the link is still valid for the original state, and whether the redaction policy $\mathcal{RP}$ is satisfied. By this way, the redaction operation of blockchain can be verified. For example, in the blockchain $chain = (B_1, \ldots, B_m)$, if $st_j \neq H(header_{j-1})$ for $header_{j-1} = (sl_{j-1}, st_{j-1}, G(d_{j-1}), ib_{j-1}, \pi_{j-1})$, $chain$ is valid only under the condition of $st_j = H(sl_{j-1}, st_{j-1}, ib_{j-1}, ib_{j-1}, \pi_{j-1})$ and $\mathcal{RP}(chain, B_{j-1}, sl_{j-1}) = 1$.

For presentation simplicity, we extend the structure of block headers in the underlying blockchains like in [19], but it is straightforward to perform engineering optimizations to maintain the same block structure between the old and the new nodes. The idea behind the optimization could be simple [20]: i) the upgraded blockchain node maintains two separate storages for the original blockchain and the modifications respectively, so the blockchain's upgrade does not have to change the structure of block headers at the end of new nodes; ii) all modification requests and approvals are sent to the blockchain by rephrasing existing script opcodes, for example, through being attached to OP _ RETURN in Bitcoin-like script (e.g., Cardano's settlement layer). In addition, we do not consider the redaction about the payment information just like in [19], which can be achieved by additionally updating the UTXO as discussed in [20].

3.2 Redactable Blockchain Protocol

Before our protocol is described, we first define how to determine the validity of the blocks, blockchains and candidate editing blocks. Roughly speaking, we need to ensure that for an edited block, its original state before editing still can be accessible for verification.

Valid Blocks. To validate a block B, the validateBlock algorithm (Algorithm 1) first checks the validity of data included in B according to the system rules. It then checks the validity of the leader by eligible function. Finally, it verifies the signature π (on $(sl, st, G(d), ib)$ or on (sl, st, ib, ib)) with the public key pk of the leader or verifies the nonce π for the puzzle of PoW. In particular, for an edited block, the signature π is on the "old" state (sl, st, ib, ib). We say that B is a valid block iff validateBlock(B) outputs 1.

Algorithm 1. Block Validation Algorithm validateBlock(B)

```
1: Parse $B = (header, d)$, where $header = (sl, st, G(d), ib, \pi)$;
2: Validate data $d$, **if** invalid **return** 0;
3: Validate the leader, **if** invalid **return** 0;
4: Validate data $\pi$, **if** invalid **return** 0;
5: **else return** 1.
```

Valid Blockchains. To validate a blockchain $chain$, the validateChain algorithm (Algorithm 2) first checks the validity of every block B_j, and then checks its relationship to the previous block B_{j-1}, which has two cases depending on whether B_{j-1} is an edited block. If B_{j-1} has been redacted (i.e., $st_j \neq H(header_{j-1})$), its check additionally depends on whether the redaction policy $\mathcal{RP}$ has been satisfied. We say $chain$ is valid iff validateChain$(chain)$ outputs 1.

Algorithm 2. Chain Validation Algorithm validateChain $(chain)$

```
1: Parse $chain = (B_1, \ldots, B_m)$, parse $B_j = (header_j, d_j)$ where
   $header_j = (sl_j, st_j, G(d_j), ib_j, \pi_j)$, and set $j = m$;
2: **while** $j \geq 2$ **do**
3:   **if** validateBlock$(B_j) = 0$, **return** 0;
4:   **else if** $st_j = H(header_{j-1})$, **then** $j = j - 1$;
5:   **else if** $st_j = H(sl_{j-1}, st_{j-1}, ib_{j-1}, ib_{j-1}, \pi_{j-1}) \wedge$
6:       $\mathcal{RP}(chain, B_{j-1}, sl_{j-1}) = 1$, **then** $j = j - 1$;
7:   **else return** 0.
8: **end while**
9: **If** $j = 1$ **return** validateBlock$(B_1)$.
```

Valid Candidate Editing Blocks. To validate a candidate editing block B_j^* for the jth block of blockchain $chain$, the validateCand algorithm (Algorithm 3) first checks the validity of B_j^*. It then checks the link relationship with B_{j-1} and B_{j+1}, where the link with B_{j+1} is "old," i.e., $st_{j+1} = H(sl_j, st_j, ib_j, ib_j, \pi_j)$. We say B_j^* is a valid candidate editing block iff validateCand$(chain, B_j^*)$ outputs 1.

Algorithm 3. Candidate Block Validation Algorithm validateCand$(\mathcal{C}, B_j^*)$

```
1: Parse $B_j^* = (header_j, d_j^*)$, where $header_j = (sl_j, st_j, G(d_j^*),$
   $ib_j, \pi_j)$;
2: **if** validateBlock$(B_j^*)$ = 0 **then return** 0;
3: Parse $B_{j-1} = (header_{j-1}, d_{j-1})$,
4:     where $header_{j-1} = (sl_{j-1}, st_{j-1}, G(d_{j-1}), ib_{j-1}, \pi_{j-1})$;
5: Parse $B_{j+1} = (header_{j+1}, d_{j+1})$,
6:     where $header_{j+1} = (sl_{j+1}, st_{j+1}, G(d_{j+1}), ib_{j+1}, \pi_{j+1})$;
7: **if** $st_j = H(sl_{j-1}, st_{j-1}, ib_{j-1}, ib_{j-1}, \pi_{j-1})$
8:     and $st_{j+1} = H(sl_j, st_j, ib_j, ib_j, \pi_j)$, **then return** 1;
9: **else return** 0.
```

We now present redactable blockchain protocol Γ in Fig. 2, where collectVote is used to collect the votes.

Collecting Votes. The subroutine collectVote (Fig. 3) collects and validates the votes from the slot sl (where $sl \bmod w = 0$) to the slot $sl + w - 1$. The collected votes are stored in $msgs$ buffer. The algorithm first checks whether the number of votes on $H(B_j^*)$ is enough by $\mathcal{RP}(chain, B_j^*, sl_j)$, and stops collecting if it is. Otherwise, it begins to validate the vote. Specifically, it first verifies the signature on $H(B_j^*)$ under the public key of the voter, and then confirms the voting right and the voting number c of the voter determined by VerifyCmt$(chain, sl, c, proof, para')$.4 Then the algorithm generates an aggregate signature $asig_j$ on all these valid vote signatures SIG, aggregates corresponding proofs $PROOF$, and returns them, where aggregate signature can reduce the communication complexity and storage overhead for blockchains.

Remark 1. (How to set the voting period w.) Observe that in a synchronous network, messages are delivered within a

4. In this paper, we assume the identifier of the public key would be sent to receivers associated with the signature, such that the corresponding public key can be located for verification.

```
Redactable Blockchain Protocol $\Gamma$ (of Node $\mathcal{P}$)
/ * Initialization * /
Upon receiving init() from $\mathcal{Z}$, $\mathcal{P}$ is activated to initialize as follows:
  let $(pk_p, sk_p) := \mathsf{Gen}(1^\lambda)$
  let $txpool$ be an empty FIFO buffer
  let $chain := B_0$, where $B_0$ is the genesis block
  let $\mathcal{EP}$ be an empty set (to store editing candidates)
  let $\mathcal{VEP}$ be an empty set (to store proof for voted editings)
  let $vote\_msgs$ be an empty FIFO buffer (to store votes)
/ * Receiving a longer chain * /
Upon receiving $chain'$ for the first time, the (online) $\mathcal{P}$ proceeds as:
  if $|chain'| > |chain|$ and validateChain$(chain') = 1$;
    let $chain := chain'$ and broadcast $chain$
/ * Receiving transactions * /
Upon receiving transactions$(d')$ from $\mathcal{Z}$ (or other nodes) for the first time, the (online) $\mathcal{P}$ proceeds as:
  let $txpool.enqueue(d')$ and broadcast $d'$
/ * Receiving candidate blocks for editing * /
Upon receiving edit$(B_j^*)$ from $\mathcal{Z}$ (or other nodes) for the first time, the (online) $\mathcal{P}$ proceeds as:
  let $\mathcal{EP} := \mathcal{EP} \cup \{B_j^*\}$, if validateCand$(chain, B_j^*) = 1$
/ * Receiving vote information * /
Upon receiving vote$(c_i, proof_i, pk_i, H(B_j^*), sig_j)$ for the first time, the (online) $\mathcal{P}$ proceeds as:
  let $vote\_msgs.enqueue((c_i, proof_i, pk_i, H(B_j^*), sig_j))$
/ * When collectVote subroutine returns * /
Upon receiving vote-proof$(v)$ from collectVote$(sl, \dots)$ through the subroutine tape, the (online) $\mathcal{P}$ proceeds as:
  let $\mathcal{VEP} := \mathcal{VEP} \cup v$, where $v$ is in form of $(H(B_j^*), asig_j, PROOF)$

/ * Main procedure * /
for each slot $sl' \in \{1, 2, \dots\}$, the (online) $\mathcal{P}$ proceeds as:
  for each $B_j^*$ in $\mathcal{EP}$:
    if $B_j^*$ is expired, let $\mathcal{EP} := \mathcal{EP} \setminus \{B_j^*\}$
    if $\mathcal{RP}(chain, B_j^*, sl_j) = 1$, let $chain[j] := B_j^*$, $\mathcal{EP} := \mathcal{EP} \setminus \{B_j^*\}$
  if $\mathcal{EP} \neq \emptyset$:
    let $sl := \lfloor sl'/w \rfloor * w$
    activate collectVote$(sl, vote\_msgs, \dots)$ subroutine
    let $(c, proof) := \mathsf{Cmt}(chain, sl, \mathcal{P}, para)$
    if $c$ is non-zero:
      for each $B_j^*$ in $\mathcal{EP}$, broadcast vote$(c, proof, pk_{\mathcal{P}}, H(B_j^*), sig_j)$, where $sig_j = \mathsf{Sign}(sk_{\mathcal{P}}; H(B_j^*))$
  if eligible$(\mathcal{P}, sl') = 1$:
    let $d' := txpool.dequeue() \cup \mathcal{VEP}$
    let $(header, d) := \mathsf{Head}(chain)$
    let $header' := (sl', st', G(d'), ib', \pi')$, where $st' := H(header)$ and $\pi'$ is the output of $\mathcal{P}$ (the signature or the nonce)
    let $chain := chain \| (header', d')$
    let $\mathcal{VEP} := \emptyset$
    broadcast $chain$
  output chain=extract$(chain)$ to $\mathcal{Z}$. Recall that chain denotes an ideal blockchain where each block consists of transactions of the corresponding block of $chain$ (see Section 2.3).
```

Fig. 2. Redactable blockchain protocol Γ.

```
subroutine collectVote$(chain, sl, msgs, w, T, \eta)$ invoked by $\mathcal{P}$
//$msgs$ is a FIFO buffer receiving votes from the network
//$sl$ is the number of the first slot in this $w$-slot voting period
let $SIG$ be a dictionary of hash-set pairs;
let $PROOF$ be a dictionary of hash-set pairs;
Upon $Time^1 \geq sl + w$:
  halt
Upon $msgs$ not empty:
  assert $sl \leq Time < sl + w$
  for each $Time$
    for each $(c, proof, pk, H(B_j^*), sig_j) \leftarrow msgs.dequeue()$
      if $\mathcal{RP}(chain, B_j^*, sl_j) = 1$ continue;
      if $SIG[B_j^*]$ and $PROOF[B_j^*]$ not initialized yet
        let $SIG[B_j^*] := \emptyset$, $PROOF[B_j^*] := \emptyset$;
      if $sig_j$ on $H(B_j^*)$ cannot be validated by $pk$ continue;
      if VerifyCmt$(chain, sl, c, proof, para') = 0$ continue;
      $SIG[B_j^*] := SIG[B_j^*] \cup \{sig_j\}$;
      $PROOF[H(B_j^*)] := PROOF[H(B_j^*)] \cup \{proof\}$;
    compute aggregate signature $asig_j$ on $H(B_j^*)$ from $SIG[B_j^*]$
    send vote-proof$(H(B_j^*), asig_j, PROOF[H(B_j^*)])$ to $\mathcal{P}$
    let $SIG[B_j^*] := \emptyset$ and $PROOF[H(B_j^*)] := \emptyset$
$^1Time$ represents the latest slot number (see Section 2.1)
```

Fig. 3. Collecting votes.

maximum network delay of Δ and we can initially set $w = \Delta$. While in semi-synchronous or asynchronous network, we can not obtain such Δ. We can first make a rough estimate of the network delay Δ and set $w = \Delta$ initially, and if there are not enough votes for a candidate editing block during the current voting period due to network delay, then the block will be voted again in the next voting period, where we set $w = 2\Delta$. The time window will increase exponentially with slot until the candidate editing block expires. By this way, it is very likely that a candidate editing block will be approved eventually unless message delays grow faster than the time window indefinitely, which is unlikely in a real system.

Remark 2. (About the fork problem.) Similar to existing works for redactable blockchain, our solution cannot support soft-fork for all cases, and hard-fork may be unavoidable if the redaction would lead to the inconsistency of validity verification of blocks among different nodes. Specifically, if the redaction alters the state of blocks, e.g, modifying UTXOs in Bitcoin or the account balance in Ethereum, then there would exist one transaction that can be considered to be valid to some nodes but invalid to others, in which case hard-fork may be unavoidable. For other cases like adding node to empty contract [20] or deleting some illegal non-transaction data [19], soft-fork is possible. Also note that, it is the redaction operation itself rather than the specific technique of existing works which leads to potential fork.

4 Security Analysis

In this section, we analyze the security of redactable blockchain protocol Γ as depicted in Fig. 2. The security properties of redactable blockchain are same as that of basic blockchain, except for the common prefix property.

Redactable Common Prefix. We observe that our protocol Γ inherently does not satisfy the original definition of common prefix due to the (possible) edit operation. In detail, consider the case where the party $\mathcal{P}_1$ is honest at time slot sl_1 and the party $\mathcal{P}_2$ is honest at time slot sl_2 in view, such that $sl_1 < sl_2$. For a candidate block B_j^* to replace the original B_j, whose votes are published at slot sl such that $sl_1 < sl < sl_2$, the edit request has not been proposed in $\mathsf{chain}_{\mathcal{P}_1}^{sl_1}(\mathsf{view})$ but may have taken effect in $\mathsf{chain}_{\mathcal{P}_2}^{sl_2}(\mathsf{view})$. As a result, the original B_j remains unchanged in $\mathsf{chain}^{sl_1}_{\mathcal{P}_1}(\mathsf{view})$ while it is replaced with the candidate B^*_j in $\mathsf{chain}^{sl_2}_{\mathcal{P}_2}(\mathsf{view})$. Therefore, the security requirement in Definition 1 is violated.

The main reason lies in the fact that the original definition of common prefix does not account for edits in the chain, while any edit may break the common prefix property. To address this issue, we adopt the extended definition called redactable common prefix [19] and consider the effect of each edit operation, which is suitable for redactable blockchains. Roughly speaking, the property of redactable common prefix states that if the common prefix property is violated, it must be the case that there exist edited blocks satisfying the redaction policy $\mathcal{RP}$.

Definition 5. *(Redactable Common Prefix [19]). For any two honest parties $\mathcal{P}_i$ and $\mathcal{P}_{i'}$, any $t \leq t'$ and any $k \geq k_0$, we say the blockchain satisfies k_0-redactable common prefix if one of the following conditions is satisfied.*

1) *the first $|\mathsf{chain}^t_{\mathcal{P}_i}(\mathsf{view})| - k$ records of $\mathsf{chain}^t_{\mathcal{P}_i}(\mathsf{view})$ are the prefix of $\mathsf{chain}^{t'}_{\mathcal{P}_{i'}}(\mathsf{view})$, or*
2) *for each B^*_j in the first $|\mathsf{chain}^t_{\mathcal{P}_i}(\mathsf{view})| - k$ records of $\mathsf{chain}^{t'}_{\mathcal{P}_{i'}}(\mathsf{view})$ but not in the first $|\mathsf{chain}^t_{\mathcal{P}_i}(\mathsf{view})| - k$ records of $\mathsf{chain}^t_{\mathcal{P}_i}(\mathsf{view})$, it must be the case that $\mathcal{RP}(chain, B^*_j, t_j) = 1$ where $t_j < t < t'$.*

Essentially, Γ behaves just like the underlying immutable blockchain protocol in Appendix B, available in the online supplemental material (see also the full version [29]) if there is no edit in the chain, and otherwise each edit must be approved by the redaction policy $\mathcal{RP}$. Therefore, we prove Γ can guarantee the same or variant version of properties as the underlying immutable blockchain under the redaction policy $\mathcal{RP}$.

Theorem 1. (Security of Γ). *Assume that the signature scheme* SIG *is EUF-CMA secure, the aggregate signature scheme* ASIG *is unforgeable, the hash function H is collision-resistant, the function* Cmt *ensures the fraction of honest users (in terms of computational power or stake) in the committee is at least η, and the underlying immutable blockchain protocol in Appendix B, available in the online supplemental material, satisfies k_0-common prefix, (k_0, μ)-chain quality, and τ-chain growth. Then, redactable blockchain protocol Γ satisfies the k_0-redactable common prefix, (k_0, μ)-chain quality, and τ-chain growth.*

Proof roadmap. We first consider an ideal-world protocol Π_{ideal} having access to an ideal functionality $\mathcal{F}_{tree}$, and prove that Π_{ideal} satisfies redactable common prefix, chain quality, and chain growth in Section 4.1. Then we prove the ideal-world protocol Π_{ideal} can be securely emulated by the real-world protocol Γ in Section 4.2.

4.1 Security of Ideal Protocol Π_{ideal}

We first define an ideal functionality $\mathcal{F}_{tree}$ (Fig. 4) and analyze an ideal-world protocol Π_{ideal} (Fig. 5) parameterized with $\mathcal{F}_{tree}$.

We use the ideal functionality $\mathcal{F}_{tree}$ to keep a record of the extracted blockchain chain (see Section 2.3) up to now which is denoted by tree. Initially, only the blockchain genesis corresponding to the genesis block is contained in the set tree. $\mathcal{F}_{tree}$ decides whether a party $\mathcal{P}$ is the elected leader for every time step t with probability $\phi(s, p)$ or the committee member with probability $\phi(s, p')$, where ϕ is a general function whose output is proportional to the stake (or the computational power) s of $\mathcal{P}$, and the parameter p (or p', resp.) provides the randomness. An adversary $\mathcal{A}$ can know which party is elected as the leader (or voting committee member, resp.) in time t using the $\mathcal{F}_{tree}$.leader (or $\mathcal{F}_{tree}$.committee, resp.) query. Further, honest and corrupted parties can extend known chains with new block by calling $\mathcal{F}_{tree}$.extend, if they are elected as leaders for specific time steps. Specifically, honest parties always extend chains in the current time, while corrupted parties are allowed to extend a malicious chain in a past time step t' as long as t' complies with the strictly increasing rule. In addition, the voting committee member can call $\mathcal{F}_{tree}$.redact to redact the blockchain, if the votes during one voting period are more than the number of corrupted committee members. Finally,

```
$\mathcal{F}_{tree}(p, p')$
Upon receiving init(): tree := genesis, time(genesis) := 0
Upon receiving leader$(\mathcal{P}, t)$ from $\mathcal{A}$ or internally:
  let $s$ be the stake (or computational power) of $\mathcal{P}$ at time $t$
  if leader$(\mathcal{P}, t)$ has not been assigned,
  set and return leader$(\mathcal{P}, t) = \begin{cases}1 & \text{with probability } \phi(s,p)\\ 0 & \text{otherwise}\end{cases}$
Upon receiving extend(chain, B) from honest party $\mathcal{P}$:
  denote by $t$ the present time
  if leader$(\mathcal{P}, t) = 1$, chain||B $\notin$ tree and chain $\in$ tree
  extend chain to chain||B in tree, set time(chain||B) := $t$
  return "succ"
Upon receiving extend(chain, B, $t'$) from corrupted party $\mathcal{P}^*$:
  denote by $t$ the present time
  if leader$(\mathcal{P}^*, t) = 1$, chain||B $\notin$ tree and chain $\in$ tree, and
  time(chain) $< t' < t$
  extend chain to chain||B in tree, set time(chain||B) := $t'$
  return "succ"
Upon receiving committee$(\mathcal{P}, t)$ from $\mathcal{A}$ or internally:
  let $s$ be the stake of $\mathcal{P}$ at time $\lfloor t/w \rfloor * w$
     or the computational power of $\mathcal{P}$ at time $t$
 if committee$(\mathcal{P}, t)$ has not been assigned,
  return committee$(\mathcal{P}, t) = \begin{cases}1 & \text{with probability } \phi(s,p')\\ 0 & \text{otherwise}\end{cases}$
Upon receiving redact(chain, $i$, $B^*$) from $\xi$ distinct parties $\mathcal{P}_j$:
  assert chain $\in$ tree and committee$(\mathcal{P}_j, t_j) = 1$ for every $\mathcal{P}_j$
  assert all of $\lfloor t_j/w \rfloor$ are equal
  assert $\xi$ is more than the number of corrupted parties $\mathcal{P}_j$
     with committee$(\mathcal{P}_j, t_j) = 1$
  redact chain[$i$] := $B^*$ and return "succ"
Upon receiving verify(chain) from $\mathcal{P}$:
  return 1 if chain $\in$ tree, otherwise return 0
```

Fig. 4. Ideal functionality $\mathcal{F}_{tree}$.

```
Ideal Protocol $\Pi_{\mathsf{ideal}}$
Upon receiving init(): chain := genesis
Upon receiving chain':
if |chain'| > |chain| and $\mathcal{F}_{tree}$.verify(chain') = 1
  chain := chain' and broadcast chain
for every slot:
for the input B (or B*) from $\mathcal{Z}$:
–if $\mathcal{F}_{tree}$.extend(chain, B) outputs "succ",
extend chain to chain||B and broadcast chain
–if $\mathcal{F}_{tree}$.redact(chain, i, B*) outputs "succ",
let chain[i] := B* and broadcast chain
–output chain to $\mathcal{Z}$
```

Fig. 5. Ideal protocol Π_{ideal}.

$\mathcal{F}_{tree}$ records each valid chain, and parties can check if any chain they received is valid by calling $\mathcal{F}_{tree}.\mathsf{verify}$.

Theorem 2. (Security of Π_{ideal}). *If the underlying immutable ideal protocol in Appendix C, available in the online supplemental material, satisfies k_0-common prefix, (k_0, μ)-chain quality, and τ-chain growth, then Π_{ideal} satisfies the k_0-redactable common prefix, (k_0, μ)-chain quality, and τ-chain growth.*

Proof. Note that if there is no edit in chain, then Π_{ideal} behaves exactly like the underlying immutable ideal protocol in Appendix C, available in the online supplemental material, (see also the full version [29]), and thus k_0-common prefix, (k_0, μ)-chain quality, and τ-chain growth can be preserved directly. Thus we mainly prove the security of Π_{ideal} with any edit satisfying the redaction policy $\mathcal{RP}$.

Redactable Common Prefix. Assume that there exists B_j^* in first $|\mathsf{chain}^t_{\mathcal{P}_i}(\mathsf{view})| - k_0$ of $\mathsf{chain}^{t'}_{\mathcal{P}_{i'}}(\mathsf{view})$ but not in first $|\mathsf{chain}^t_{\mathcal{P}_i}(\mathsf{view})| - k_0$ records of $\mathsf{chain}^t_{\mathcal{P}_i}(\mathsf{view})$, where $t \leq t'$, and a party $\mathcal{P}_i$ is honest at t and a party $\mathcal{P}_{i'}$ is honest at t' in view, which means B_j is redacted with B_j^* in $\mathsf{chain}^{t'}_{\mathcal{P}_{i'}}(\mathsf{view})$ but not in $\mathsf{chain}^t_{\mathcal{P}_i}(\mathsf{view})$. Then it must be the case that the party $\mathcal{P}_{i'}$ receives enough votes (more than the number of corrupt committee members) for B_j^* according to the ideal protocol specification. Therefore, the redaction policy $\mathcal{RP}$ is satisfied, and we conclude Π_{ideal} satisfies the k_0-redactable common prefix.

Chain Quality. If an honest block B_j is replaced with a malicious candidate block B_j^* (e.g., containing harmful data), the adversary $\mathcal{A}$ can increase the fraction of adversarial blocks in chain and finally break the chain quality property. However, according to the ideal protocol specification, an edited block can only be adopted when the votes are more than the number of adversarial committee members. Since only those adversarial committee members would vote for the malicious block B_j^*, chain cannot be redacted. Therefore, we conclude Π_{ideal} satisfies the (k_0, μ)-chain quality.

Chain Growth. Note that any edit operation would not alter the length of chain, since it is not possible to remove any blocks from chain according to the ideal protocol specification. Moreover, the new block issue process in current time slot is not influenced by votes for any edit request. No matter whether a party $\mathcal{P}$ has received enough votes, $\mathcal{P}$ always extends chain at time slot t as long as $\mathsf{leader}(\mathcal{P}, t) = 1$. Therefore, we conclude Π_{ideal} satisfies the τ-chain growth. □

4.2 Real-World Emulates Ideal-World

We next show that the real-world protocol Γ as depicted in Fig. 2 emulates the ideal-world protocol Π_{ideal}.

Theorem 3. (Γ emulates Π_{ideal}). *For any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ of the real-world protocol Γ, there exists a PPT adversary (also called the simulator) $\mathcal{S}$ of the ideal protocol Π_{ideal}, such that for any PPT environment $\mathcal{Z}$, for any $\lambda \in \mathbb{N}$, we have*

$$\mathsf{view}(EXEC^{\Pi_{ideal}}(\mathcal{S}, \mathcal{Z}, \lambda)) \overset{c}{\equiv} \mathsf{view}(EXEC^{\Gamma}(\mathcal{A}, \mathcal{Z}, \lambda)),$$

where $\overset{c}{\equiv}$ denotes computational indistinguishability.

Proof. The proof process can be shown by a standard simulation argument. Specifically, for any adversary $\mathcal{A}$ in the real world, we can construct a simulator $\mathcal{S}$ in the ideal world such that no p.p.t. environment $\mathcal{Z}$ can distinguish an ideal execution with the simulator $\mathcal{S}$ and Π_{ideal} from a real execution with the adversary $\mathcal{A}$ and Γ under the security assumption of the underlying primitives including the digital signature scheme, aggregate signature scheme and verifiable random function. We defer the (security) definitions of the corresponding primitives in Appendix A, available in the online supplemental material.

Consider a PPT adversary $\mathcal{A}$ in the real-world protocol Γ. The simulator $\mathcal{S}$ in the ideal protocol Π_{ideal} can be constructed as follows:

1) At the beginning of the protocol execution, $\mathcal{S}$ generates public/secret key pair $(pk_{\mathcal{P}}, sk_{\mathcal{P}})$ for each honest party $\mathcal{P}$, and stores the party $\mathcal{P}$ and public key $pk_{\mathcal{P}}$ mapping.
2) For the leader selection process, we consider two common cases.
   - The leader selection function $\mathsf{eligible}$ is first modeled as the random oracle $H(\cdot)$ like in [24][28]. Whenever $\mathcal{A}$ sends a hash query $H(\mathcal{P}, t)$, $\mathcal{S}$ would return the same answer as before if $\mathcal{A}$ has made the same query before. Otherwise, $\mathcal{S}$ checks whether the identifier $\mathcal{P}$ corresponds to some public key. If yes, $\mathcal{S}$ calls $b \leftarrow \mathcal{F}_{tree}.\mathsf{leader}(\mathcal{P}, t)$, and returns b. Otherwise, $\mathcal{S}$ randomly samples a string of the length $|H(\cdot)|$ and returns it to $\mathcal{A}$.
   - Second, the random oracle is replaced with normal function such as the keyed $\mathsf{PRF}_k(\cdot)$. In this case, $\mathsf{PRF}_k(\cdot)$ is used by both $\mathcal{S}$ and $\mathcal{A}$. The simulation process is almost the same to that of the above random oracle case, except that $\mathcal{S}$ would just send the key k to $\mathcal{A}$ as soon as he obtains k from $\mathcal{F}_{tree}$ and moreover not have to simulate queries against $\mathsf{PRF}_k(\cdot)$ for $\mathcal{A}$ any more.
3) For each honest party $\mathcal{P}_i$, $\mathcal{S}$ keeps a record of the $chain$ in the real-world. Whenever $\mathcal{A}$ sends $chain$ to an honest party $\mathcal{P}_i$, $\mathcal{S}$ checks the validity of $chain$ by running the check in the real-world (i.e., $\mathsf{validateChain}(.)$). If the check passes and moreover $chain$ is longer compared with the current chain owned by $\mathcal{P}_i$, $chain$ would be updated by $\mathcal{S}$ as the new chain in the real-world for $\mathcal{P}_i$.
4) Whenever receiving an extracted chain chain from an honest party $\mathcal{P}$, $\mathcal{S}$ fetches the current $chain$ in the real-world owned by for $\mathcal{P}$.
   - If the editing pool $\mathcal{EP}$ is empty, a new $chain'$ in the real-world would be computed by $\mathcal{S}$ as follows. Specifically, let sl be the current slot, and if $\mathsf{eligible}(\mathcal{P}, sl) = 1$, then $\mathcal{S}$ sets $B := (header,' d')$ with $header' = (sl, st,' G(d'), ib,' \pi')$ such that $st' = H(header)$ and π' is the output of $\mathcal{P}$ (the signature for $\mathsf{Head}(chain) = (header, d)$ or the nonce). Finally, $\mathcal{S}$ sets $chain' := chain \| B$ and sends $chain'$ to $\mathcal{A}$.
   - If the editing pool $\mathcal{EP}$ is not empty (e.g., one candidate edited block B_j^* for B_j is included in $\mathcal{EP}$), $\mathcal{S}$ starts to collect the votes for B_j^* and simulates

the vote process using the real-world algorithm. Specifically, for any party $\mathcal{P}_i$ who sends the candidate B_j^* to $\mathcal{S}$ in sl, if $\mathsf{Cmt}(chain, \lfloor sl/w \rfloor * w, \mathcal{P}_i, para)$ returns $(c_i, proof_i)$, $\mathcal{S}$ votes for B_j^* in the name of $\mathcal{P}_i$ by computing $v_i = \mathsf{Sign}\ (sk_i, H(B_j^*))$, and then sends $(c_i, proof_i, v_i)$ to $\mathcal{A}$. If $\mathcal{S}$ receives votes for B_j^*, $\mathcal{S}$ computes $(asig, PROOF)$ for B_j^* by the aggregation of v_i and $(c_i, proof_i)$. If $\mathsf{eligible}(\mathcal{P}, sl') = 1$, $\mathcal{S}$ sets $d' := d' \| asig \| PROOF$ and $B := (header,' d')$ with $header' = \{sl,' st,' G(d'), ib,' \pi'\}$, such that $st' = H(header)$ and π' is the output of $\mathcal{P}$ (the signature for $\mathsf{Head}(chain) = (header, d)$ or the nonce). Finally, $\mathcal{S}$ sets $chain' := chain \| B$ and sends $chain'$ to $\mathcal{A}$.

5) Whenever an honest party $\mathcal{P}$ receives a message $chain$ from $\mathcal{A}$, $\mathcal{S}$ intercepts the message and checks the validity of $chain$ by executing the real-world protocol's checks (i.e., $\mathsf{validateChain}(.)$). If the checks do not pass, $\mathcal{S}$ ignores the message. Otherwise,
   - For the candidate edited block B_j^*, $\mathcal{S}$ abort outputting vote-failure if $\mathcal{RP}(chain, B_j^*, sl) = 1$ for some slot sl however $\mathcal{S}$ has never received enough votes for B_j^*.
   - Else, let $\mathsf{chain} := \mathsf{extract}(chain)$, and let l be the largest value such that $\mathcal{F}_{tree}.\mathsf{verify}(\mathsf{chain}[:l]) = 1$. If any block in $chain[l+1:]$ has been signed in the name of an honest party $\mathcal{P}$, $\mathcal{S}$ aborts wieh sig-failure as the output. Otherwise, for each $l' \in [l+1, |\mathsf{chain}|]$, $\mathcal{S}$ calls $\mathcal{F}_{tree}.\mathsf{extend}(\mathsf{chain}[:l'-1], \mathsf{chain}[l'], t')$ acting as a corrupted stakeholder $\mathcal{P}^*$, where $t' = Time$. Then $\mathcal{S}$ forwards $chain$ to $\mathcal{P}$.

Lemma 4.1. *If the signature scheme* SIG *is EUF-CMA secure and the hash function H is collision-resistant, the probability that the above simulation would abort with* sig-failure *is negligible.*

Proof. Note that the adversary $\mathcal{A}$ cannot produce a malicious block $\widetilde{B_j^*}$ such that $H(\widetilde{B_j^*}) = H(B_j^*)$ for the candidate edited block B_j^*, since the hash function H is collision-resistant. Then, if sig-failure ever happens, the adversary $\mathcal{A}$ must have generated or to say forged a valid signature on a different message that $\mathcal{S}$ never signed. Thus, we can immediately construct a reduction that breaks the EUF-CMA security of the underlying signature scheme SIG. Specifically, $\mathcal{S}$ simulates for $\mathcal{A}$ the protocol executing just as the above specification, and guesses a random party $\mathcal{P}_i$ whose signature security is broken. $\mathcal{S}$ generates the public/secret key pair for all other parties and produces the corresponding signatures. $\mathcal{S}$ also calls the signing oracle to generate signatures for $\mathcal{P}_i$. Eventually, if $\mathcal{A}$ outputs a valid signature σ and σ has never been previously output by the signing oracle, σ can be used as a forgery and EUF-CMA security of SIG is broken. □

Lemma 4.2. *If the aggregate signature scheme* ASIG *is unforgeable and the function* Cmt *ensures the fraction (in terms of computational power or stake) of honest users in the committee is at least η, the probability that the above simulation would abort with* vote-failure *is negligible.*

Proof. If vote-failure ever happens, the adversary $\mathcal{S}$ must have forged an aggregate signature $asig$ on the individual messages in the name of the ξ parties, among which there is at least one honest stakeholder. Then we can construct a reduction that breaks the security of the underlying aggregate signature scheme ASIG. Specifically, $\mathcal{S}$ simulates the protocol executing for $\mathcal{A}$ as the above specification, and guesses a random party $\mathcal{P}_i$ as the honest party among the ξ parties. We denote by (pk^*, sk^*) the public/secret key pair of $\mathcal{P}_i$. $\mathcal{S}$ generates the public/secret key pair for all other parties and produces the corresponding signatures. $\mathcal{S}$ also calls the signing oracle $\mathsf{Sign}(sk^*, .)$ to generate any signature for $\mathcal{P}_i$ as specified in the security experiment. Eventually, if $\mathcal{A}$ outputs a valid aggregate signature $asig$ on the message set $M = \{m^*, m_1, \ldots, m_{n-1}\}$ under the public key set $\{pk^*, pk_1, \ldots, pk_{n-1}\}$ and has never queried the signing oracle $\mathsf{Sign}(sk^*, .)$ on m^*, where $n = \xi$, then $asig$ can be used as a forgery and the security of ASIG is broken. □

If all of the above failure events never happen, we can conclude that the simulated execution of $\mathcal{S}$ and the real-world execution are indistinguishable in the view of $\mathcal{Z}$. We thus complete the proof of theorem. □

5 Instantiation

Following the generic construction, we now present two concrete instantiations of redactable PoS blockchain and PoW blockchain.

5.1 Redactable Proof-of-Stake Blockchain

In proof-of-stake blockchain, we assume S is total stakes in the system, T is the expected number of stakes in committee for voting, and the fraction of stakes held by honest users in the committee is at least η. The committe members are selected only at the first slot sl of each voting period between sl and $sl + w - 1$, and w can be set based on specific network environment to guarantee the votes received by all users after w slots with a greater probability.

Checking Committee Members Cmt. The function Cmt (Algorithm 4) checks whether a party $\mathcal{P}_i$ (with secret key sk_i and stake s_i) is the committee member at the slot sl and outputs $(c, proof)$. Inspired by the idea of Algorand [22], Cmt uses VRFs to randomly select voters in a private and non-interactive way[5]. Specifically, $\mathcal{P}_i$ computes $(hash, \pi) \leftarrow VRF_{sk_i}(seed \| sl)$ with his own secret key sk_i, where $sl \bmod w = 0$, $seed$ is identical to that in the underlying proof-of-stake blockchain, and the pseudo-random $hash$ determines how many votes of $\mathcal{P}_i$ are selected. In order to select voters in proportion to their stakes, we regard each unit of stakes as a different "sub-user". For example, $\mathcal{P}_i$ with stakes s_i owns s_i units, each unit is selected with probability $p = \frac{T}{S}$, and the probability that q out of the s_i sub-users are selected follows the binomial distribution $B(q; s_i, p) = C(s_i, q)p^q(1-p)^{s_i - q}$, where $C(s_i, q) = \frac{s_i!}{q!(s_i - q)!}$ and $\Sigma_{q=0}^{s_i} B(q; s_i, p) = 1$. To determine how many sub-users of s_i in $\mathcal{P}_i$ are selected, the algorithm divides the interval [0,1) into consecutive intervals of the form $I^c = [\Sigma_{q=0}^{c} B(q; s_i, p), \Sigma_{q=0}^{c+1} B(q; s_i, p))$ for $c \in$

5. In a similar way, hash function can also be used to select committee members in a public way [28], which is secure against static adversary.

$\{0, 1, \ldots, s_{i-1}\}$. If $\frac{hash}{2^{hashlen}}$ falls in the interval I^c, it means that c sub-users (i.e., c votes) of $\mathcal{P}_i$ are selected, where $hashlen$ is the bit-length of $hash$.

Algorithm 4. Checking Committee Members $\mathsf{Cmt}(chain, sl, sk_i, s_i, seed, \mathcal{P}_i, T, S)$

```
1: $(hash, \pi) := VRF_{sk_i}(seed \| sl)$;
2: $p := \frac{T}{S}$; $c := 0$;
3: while $\frac{hash}{2^{hashlen}} \notin [\Sigma_{q=0}^{c} B(q; s_i, p), \Sigma_{q=0}^{c+1} B(q; s_i, p))$ do
4:     $c := c + 1$.
5: end while
6: $proof := (hash, \pi)$;
7: return $(c, proof)$.
```

Verifying Committee Members VerifyCmt. The function VerifyCmt (Algorithm 5) verifies $\mathcal{P}_i$ (with public key pk_i) is the committee member with the weight c using $proof$ (i.e., $(hash, \pi)$). Specifically, it first verifies $proof$ by $\mathsf{VerifyVRF}_{pk_i}(hash, \pi, seed \| sl)$, and then verifies $\frac{hash}{2^{hashlen}}$ falls in the interval I^c.

Algorithm 5. Verifying Committee Members $\mathsf{VerifyCmt}$ $(chain, pk_i, sl, s_i, seed, c, proof, T, S)$

```
1: $(hash, \pi) := proof$;
2: if $\mathsf{VerifyVRF}_{pk_i}(hash, \pi, seed \| sl) = 0$, then return 0;
3: $p := \frac{T}{S}$; $\chi := 0$;
4: while $\frac{hash}{2^{hashlen}} \notin [\Sigma_{q=0}^{\chi} B(q; s_i, p), \Sigma_{q=0}^{\chi+1} B(q; s_i, p))$ do
5:     $\chi := \chi + 1$.
6: end while
7: if $\chi = c$, then return 1;
8: else return 0.
```

Parameter Selection. As mentioned earlier, we consider each unit of stakes as a different "sub-user," for example, if user U_i with s_i stakes owns s_i units, then U_i is regarded as s_i different "sub-users". We assume the total stakes S in the system is arbitrarily large. When a redaction is proposed, a committee for voting will be selected from all sub-users. The expected size of committee, T, is fixed, and thus the probability ρ_s of a sub-user to be selected is $\frac{T}{S}$. Then the probability that exactly K sub-users are sampled is

$$\binom{S}{K}\rho_s^K(1-\rho_s)^{S-K} = \frac{S!}{K!(S-K)!}\left(\frac{T}{S}\right)^K\left(1-\frac{T}{S}\right)^{(S-K)}$$
$$= \frac{S\cdots(S-K+1)}{S^K}\frac{T^K}{K!}\left(1-\frac{T}{S}\right)^{(S-K)}$$

If K is fixed, we have
$\lim_{S\to\infty}\frac{S\cdots(S-K+1)}{S^K} = 1$
and
$\lim_{S\to\infty}(1-\frac{T}{S})^{(S-K)} = \lim_{S\to\infty}\frac{(1-\frac{T}{S})^S}{(1-\frac{T}{S})^K} = \frac{e^{-T}}{1} = e^{-T}$

Then the probability of sampling exactly K sub-user approaches

$$\frac{T^K}{K!}e^{-T} \quad (1)$$

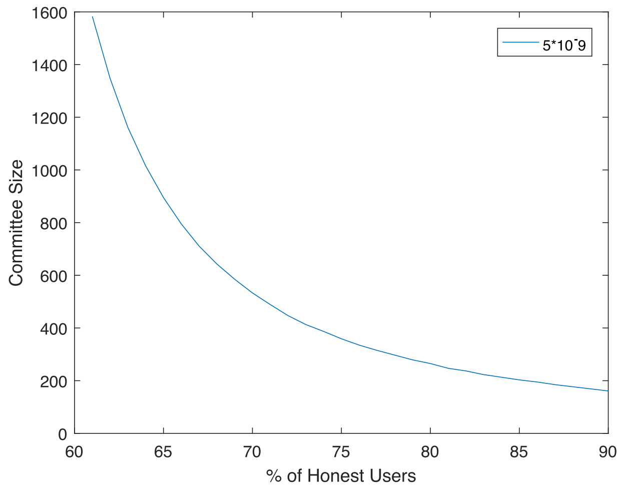

Fig. 6. The x-axis specifies h, the stakes fraction of honest users. The y-axis specifies T, the committee size.

Denote by $\#good$ and $\#bad$ the number of honest and malicious committee members respectively. If we set the majority of commmitee members are honest (i.e., $\eta > 1/2$), the following conditions should be satisfied.

(1): $\#good \geq 1/2 \cdot T$. The condition is violated when the number of honest committee members is $< 1/2 \cdot T$. From (1), the probability that we have exactly K honest committee members is $\frac{(h\cdot T)^K}{K!}e^{-h\cdot T}$, where honest stakes ratio in the system is h ($h > 1/2$). Thus, the probability of violating the condition is given by the formula

$$\sum_{K=0}^{1/2\cdot T-1}\frac{(hT)^K}{K!}e^{-hT}.$$

(2): $\#bad < 1/2 \cdot T$. As above, the probability that we have exactly L malicious committee members is $\frac{((1-h)\cdot T)^L}{L!}e^{-(1-h)\cdot T}$. Thus, the probability that satisfying the condition is given by the formula

$$\sum_{L=0}^{1/2\cdot T-1}\frac{((1-h)T)^L}{L!}e^{-(1-h)T}.$$

F is a parameter which marks a negligible probability for failure of either condition, and our experience sets $F = 5\times10^{-9}$. Our goal is to compute the minimum value of T, and ensure the probability that condition (1) or (2) doses not hold is at most F. If we find some T that satisfies both conditions with probability $1-F$, then it is also true for any larger value of T. Based on the above observation, in order to find the optimal T, we first assign an arbitrary large value (e.g., 10^4) to T, and then check whether both conditions are satisfied. If both conditions hold, we decrease T and check whether both conditions are still satisfied. We continue the above process until finding the minimal T that ensures both conditions are satisfied. In this way, we can get Fig. 6, plotting the expected committee size T satisfying both conditions, as a function of h, with a probability of violation of 5×10^{-9}. A similar approach to compute the threshold of committee size can be referred to [22].

In the implementation of our system, we assume the fraction of honest stakes is 0.65,[6] and thus we select $T = 1000$ according to Fig. 6. A valid editing block is approved only when it obtains more than $1/2 \cdot T$ votes, that is, the threshold value in Definition 4 is equal to $1/2 \cdot T = 500$.

Fraction of Honest Users. According to Theorem 1, we only need to prove the fraction (in terms of stakes) of honest users in the committee is at least η. If $\mathcal{A}$ can "presciently" ensure which user would become the member of the voting committee, he can adaptively corrupt and impersonate this user, such that the fraction of honest users in the committee is less than η. However, according to the uniqueness property of the underlying VRF, the adversary has only a negligible probability $1/2^{hashlen}$ to win. In detail, the function value $hash$ of VRF is random and unpredictable, the adversary without the secret key can only predict whether an honest user is chosen as the committee member with a negligible probability $1/2^{hashlen}$. In addition, $\mathcal{A}$ is allowed to corrupt the known committee members only after the corresponding w slots, which would not bring any non-negligible advantage since the committee would be reselected in the next voting period.

5.2 Redactable Proof-of-Work Blockchain

We also give an instantiation for PoW that is compatible with various networks. To get sufficient numbers of committee members according to computational power distribution and ensure honest majority in the committee, we just need to collect sufficient PoW puzzle solutions. This can be easily realized by creating a "virtual selection" procedure using PoW with a bigger difficulty parameter D.

However, the adversary may be able to find "virtual puzzle solutions" in advance by the withholding attack. Specifically, if the adversary is lucky to produce a longer chain before sl that is likely to be the longest valid chain of slot sl, it temporarily withholds the chain and starts to find "virtual puzzle solutions". Then at slot sl, the adversary releases its chain and solutions, thus he has more time to find solutions. To thwart this attack, we elect the committee in r consecutive slots such that the majority of committee is honest even under the withholding attack. Like in the PoS instantiation, we use the network related parameter w to ensure all users would receive the votes with large probability, where $w \geq r$.

Checking Committee Members Cmt. In the function Cmt (Algorithm 6), if $\mathcal{P}$ can find some "virtual puzzle solutions" for PoW with difficulty parameter D between sl and $sl + r - 1$, $\mathcal{P}$ is elected as the committee and the weight c of $\mathcal{P}$ in the committee is the number of puzzle solutions. The committee member proof $proof$ includes the corresponding puzzle solutions.

Verifying Committee Members VerifyCmt. The function VerifyCmt (Algorithm 7) verifies whether $\mathcal{P}$ with the public key pk is the committee member by computing hash with the puzzle solutions, which is similar to Algorithm 6.

6. Recall that our protocol can tolerate $1/2$ adversary bound in both PoS and PoW instantiations, and larger adversary rate would imply larger committee size.

Algorithm 6. Checking Committee Members Cmt$(chain, sl, pk, D, \mathcal{P}, r)$

```
1: $c := 0$;
2: $proof := \emptyset$;
3: $Time := sl$;
4: while $Time \leq sl + r - 1$ do
5:     Parse $chain = (B_1, \ldots, B_m)$;
6:     Parse $B_{Time} = (Time, pk, st, G(d), ib, \pi, d)$;
7:     if $\mathcal{P}$ finds $nonce$ such that
       $H(Time, pk, st, G(d), nonce) < D$,
8:     then $c := c + 1, proof := proof \cup$
       $(Time, pk, st, G(d), nonce)$;
9: end while
10: return $(c, proof)$.
```

Algorithm 7. Verifying Committee Members VerifyCmt $(chain, pk, sl, D, c, proof, r)$

```
1: Parse $chain = (B_1, \ldots, B_m)$, where $B_i = (header_i, d_i)$,
   $i \in [1..m]$;
2: if the number of set member in $proof$ is not $c$ then return 0;
3: for every proof in $proof$ do
4:   if $Time \geq sl + r$ or $Time < sl$, then return 0;
5:   if $H(Time, pk, st, G(d), nonce) \geq D$ or $st \neq$
     $H(header_{Time-1})$, then return 0;
6: end for
7: return 1.
```

Parameter Selection. We assume the adversary is able to find "virtual puzzle solutions" at most t slots earlier than honest nodes and we elect the committee in r slots. Suppose that $h = \frac{1}{2} + \epsilon$ fraction of nodes in the underlying blockchain are honest, where $\epsilon \in (0, \frac{1}{2})$. Let $\alpha = \frac{D}{2^\ell} hn$ and $\beta = \frac{D}{2^\ell}(1-h)n$ denote the expected number of "virtual puzzle solutions" found by honest nodes and corrupt nodes in each slot respectively, where ℓ is the output length of the hash function $H(\cdot)$ and n is the total number of nodes.

We denote the maximum number of "virtual puzzle solutions" found by the adversary from the slot $sl - t$ to $sl + r - 1$ by N_A, and the minimum number of "virtual puzzle solutions" found by honest nodes from the slot sl to $sl + r - 1$ by N_H, respectively. Due to the Chernoff bound [30], for any $\delta > 0$, except with a negligible probability $p_1 = \exp(-\frac{\delta \cdot \min\{\delta, 1\} \cdot \beta(t+r)}{3})$, it holds that $N_A \leq (1+\delta)\beta(t+r)$. Similarly, for any $\delta \in (0,1)$, except with a negligible probability $p_2 = \exp(-\frac{\delta^2 \alpha r}{2})$, it holds that $N_H \geq (1-\delta)\alpha r$. If we set the majority of committee members are honest (i.e., $\eta > 1/2$), then we need to guarantee $N_H > N_A$ and thus the following condition should be satisfied

$$(1+\delta)\beta(t+r) < (1-\delta)\alpha r.$$

Therefore, we have $r > \frac{t}{\frac{(1-\delta)h}{(1+\delta)(1-h)} - 1}$.

According to "no long block withholding" lemma [21, Lemma 6.10], we set t to be the longest number of slots that the adversary can withhold a block B. Consider the case that k_0 new blocks are mined in the longest valid chain when the adversary withholds some blocks, where k_0 is the common prefix parameter. According to the common prefix

TABLE 2
Preliminary Tests of Votes and Proofs on Redaction

Vote on redaction candidate	Time to generate vote	$\sim$ 9 ms
	Time to validate vote	$\sim$ 1 ms
	Size of each vote	$\sim$ 0.2 KB
Proof on approved redaction	Time to validate proof	$\sim$ 560 ms
	Size of each proof	$\sim$ 109 KB

property, these withholding blocks will never appear in the chains of honest nodes. Therefore, t should be less than the minimum time the longest valid chain increases by at least k_0 blocks. According to the chain growth property [21, Theorem 4.1], $t \approx k_0/\alpha'$, where $\alpha' = \frac{D'}{2^\ell}hn$ and D' is the difficulty parameter for the underlying PoW blockchain such that at least one party can find a puzzle solution at each slot (i.e., $\frac{D'}{2^\ell}n = 1$).

For instance, let $k_0 = 6$ as in Bitcoin, $h = 0.65$ and $\delta = 0.1$, then we have $r > 1.93t$ and without loss of generality we set $r = 2t$. Then we can compute $t = 10$ and $r = 20$. Further, if we set $p_1 = exp(-13)$ and $p_2 = exp(-25)$, then $D = \frac{5000}{hr}D' \approx 385D'$. An editing block would be approved only when it obtains more than $(1+\delta)\beta(t+r) = (1-h)(1+\delta)\frac{5000}{hr}(t+r) \approx 4443$ votes, which are distributed among $r = 20$ slots, that is, the threshold value in Definition 4 is equal to $(1+\delta)\beta(t+r) \approx 4443$.

Fraction of Honest Users. To prove the security of the redactable PoW blockchain as claimed in Theorem 1, we need to ensure the fraction of solutions found by honest users in the committee is at least η ($\eta > 1/2$), and the argument is similar to that for PoS in Section 5.1. Specifically, the known committee members in redactable PoW blockchain protocol can only be corrupted by the adversary $\mathcal{A}$ after the corresponding voting period ends, which ensures honest majority during the voting period, moreover, it would not bring any non-negligible advantage even though the adversary would corrupt the known committee members after the current voting period, since a new committee would be selected in the next voting period.

6 Implementation and Evaluation

To demonstrate the feasibility of our approach, we choose redactable proof-of-stake blockchain just as an example and develop a proof-of-concept (PoC) implementation that simulates Cardano Settlement Layer (Cardano SL) [31]. We conduct extensive experiments on it, and reveal this non-optimized PoC implementation is already efficient. In particular, we showcase, even if in some extremely pessimistic cases (having tremendous redactions), the overhead of our approach remains acceptable (relative to an immutable chain).

6.1 Setup

Execution Environment. We write in standard C language (C11 version) to implement a proof-of-stake chain that simulates Cardano SL (i.e., generating a valid local Cardano replica without executing consensus). The chain supports a subset of Cardano SL's Bitcoin-style scripts, thus allowing to record basic ledger operations such as transacting coins and so on. Furthermore, we build our redaction protocol in it, thus enabling each block to include a special redaction transaction to solicit votes on editing earlier blocks. All tests runs on a personal computer with Ubuntu 16.04 (64bits) system, and equipped with a 2.20 GHz Intel Core i5-5200 U CPU and 8 GB main memory.

Cryptographic Building Blocks. Our PoC implementation adopts ECDSA over secp256k1 for all digital signatures in both editing votes and block proposals, which is a widely adopted approach by PoC tests in the blockchain community [32]. For VRF, we adopt a generic approach due to deterministic "ECDSA" in the random oracle model [33]. We import the VRF's concrete instantiation over secp256k1 in C language from [34].

Other Parameters. We set $h = 0.65$, namely, the adversary might control up to 35% of stakes in the system, which corresponds to the committee with expected size $T = 1000$. Moreover, when implementing Ouroboros Praos [27] (for simulating Cardano SL), we only consider one epoch, thus omitting the dynamic change of stakes. We might fix the block size in experiments. For example, we can specify that each block contains up to 10 transactions, which is enough to capture the number of transactions in nowadays Cardano. In addition, we also assume that each redaction request of editing a block only aims to modify a single transaction.

6.2 Experiments and Measurements

Then we conduct extensive experiments in the above PoC "sandbox" to tell the small overhead of our redaction protocol relative to an immutable chain through various performance metrics.

Votes and Proofs on Redaction. As shown in Table 2, we begin with some preliminary experiments to understand (i) the generating time, the validating time, and the size of each vote on redaction as well as (ii) the validating time and the size of each proof on approved redaction. In general, these votes and proofs incur little computational burden and are also small in size, which at least flatters the necessary conditions of efficient redactions.

Proposing/Receiving New Blocks With Redaction Proof. To evaluate how redactions would impact the performance of consensus, we consider two key metrics in the *online* nodes' critical path: (i) the latency of producing new blocks with redaction and (ii) the latency of appending new blocks with redaction to the local replica.

First, we consider the latency of producing blocks with redaction proof(s) and without redaction proof(s), respectively. For both cases, we test 500 blocks (with fixed size up to 10 transactions), and do not realize any statistic differences. Nevertheless, this is not surprising, because we

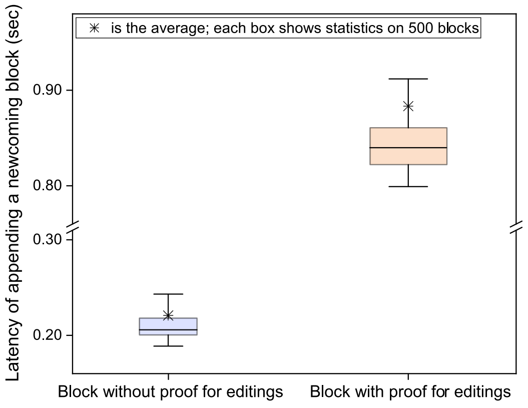

Fig. 7. The latency of appending a newcoming block (without or with proof on redaction) to the local replica.

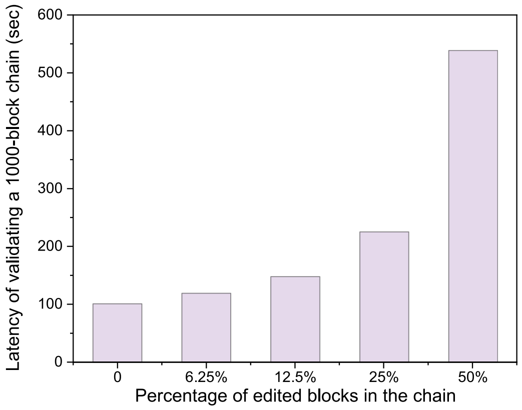

Fig. 8. The latency of validating 1000-block redactable chains (respect to various percentages of editings).

explicitly decouple the generation of blocks and the voting on redaction, so the generation of blocks in the two cases would execute the exactly same code.

Second, we measure the time spent on appending newly received blocks to the local storage, for the cases with redaction proof(s) and without redaction proof(s) respectively. As illustrated in Fig. 7, we compare appending a block with a redaction proof to the benchmark case of appending a block without any redaction proof. For each case, we conduct extensive tests to get statistics on 500 blocks (at distinct slots but with fixed block size up to 10 transactions) and visualize the statistics. It reveals that the extra overhead (incurred by validating redaction proof and editing earlier block) is small and nearly constantly. In particular, compared to the immutable case, the node only needs an extra time of 0.7 s to (i) validate a redaction proof and (ii) edit an earlier block accordingly.

Validating a Chain Consisting of Edited Blocks. Then, we conduct a series of experiments to measure the extra cost of validating an entire chain with edited blocks. Comparing to validating the immutable chain, validating an edited chain further requires to fetch and validate the proof on redaction for each edited block (besides validating block headers). This could be another critical metric to reflect how efficient our scheme is regarding *re-spawning* nodes.

To this end, we evaluate the time needed to validate a redactable chain, with respect to the varying portion of edited blocks. In the experiments, we generate redactable chains consisting of 1000 blocks and each block contains 10 transactions, and measure the time to validate them. As shown in Fig. 8, the latency of validating chains is almost increasing linearly in the number of redactions, especially when the percentage of edited blocks is small or moderately large (e.g., smaller than 25%). For example, when the percentage of edited blocks is 6.25% and 12.5%, the *extra* latency to verify the chain is about 10 seconds and 30 seconds, respectively. Even if in the extremely pessimistic case (i.e., 50% blocks are edited), the cost is still acceptable (i.e., about 5x the immutable case).

Evaluation of Other Factors. Here we mainly evaluate the extra cost for blockchain after applying our redaction mechanism like in [19]. Note that, some other factors like the network latency and node failure may also affect the blockhain consensus, however, they would not make immediate impression on the value of extra cost brought by one redaction operation and thus the above results still hold. According to our additional test, those factors would be bound to affect the needed time to complete one redaction, which can be imagined since the redaction process would be delayed. Specifically, recall that in the above implementation $T = 1000$ and the threshold value for voting is 500, and we try to set a certain fraction of nodes in the selected committee to be off-line during the evaluation, e.g, the number of nodes in the committee who are honest and moreover on-line is less than 500, then the votes for the current redaction request would not exceed the threshold value (i.e., 500), and as a result the redaction request would be delayed and voted again in the next voting period according to our design.

6.3 More Discussions

For other h. In the above instantiations for both PoS and PoW, we select the honest fraction of nodes $h = 0.65$ which is close to the ratio in many practical BFT blockchains. We want to argue that when h is close to $1/2$ our solution is still practical. For example, we select $h = 0.58$ in the above evaluation, we have the committee size $T = 3100$, and according to our evaluation: (1) for the preliminary tests of votes and proofs on redaction, the results in Table 2 remains unchanged except that the proof size increases to about 180 KB; in addition, the latency evaluation results of (2) appending newly received blocks and (3) validating an entire chain with edited blocks still hold as shown in Figs. 7 and 8 correspondingly, the reason behind which is that the verifier only needs to verify an aggregate signature to verify one redaction. In conclusion, our solution is still practical for h close to $1/2$.

Minimal Impact on Consensus. When proposing and receiving (new) blocks with proofs on redaction, there is only small overhead in our design. That means it places little burden on the *online* blockchain nodes, and more importantly, it causes minimal overhead to the critical path of consensus. In particular, when proposing new blocks with redaction, there is no extra cost to slow down the consensus; while receiving new blocks with redaction, the extra latency is as small as 0.8 s.

Efficiency for Re-Spawning Nodes. When some nodes are re-spawning, they have to bootstrap to sync up to the current longest chain. Our extensive experiments reveal it would be feasible for the re-spawning node to download and then verify the entire chain despite of a few editable blocks. Especially, in the normal cases that edited blocks are rare (e.g., less than 6.25%), the extra cost incurred by redaction is overwhelmed by the original cost of validating chain headers and transactions.

Instant Redaction (Close to Actual Network Delay). Our design dedicates to decouple voting from consensus: all votes are diffused across the network via the underlying gossip network; once the votes are successfully diffused, any honest block proposer can include a proof on redaction in its block, which would be confirmed immediately after the block becomes stable. This typically costs only a couple of minutes in Cardano. In contrast, prior art [19] lets the node proposing a block to embed its own vote in the block, resulting in a latency liner to a large security parameter. For example, [19] requires about 1024 consecutive blocks to collect votes, which means about 6 hours in Cardano and 7 days in Bitcoin. To sum up, our construction achieves significant improvement by greatly reducing the latency of confirming redactions.

Possible Storage Optimizations. Different from the immutable blockchain, our redaction protocol has to store the collected votes on each redaction, which is the most significant storage overhead relative to an immutable blockchain. Currently, our PoC implementation requires about 110 KB to store the votes for each redaction. We remark that various optimizations can be explored to further reduce the storage overhead. For example, we can use pairing-based multi-signature scheme [35] to aggregate signatures of votes instead of trivially concatenating secp256k1 ECDSA, which can reduce the size of votes to only about 60 KB.

7 Conclusion

It is crucial and even legally required to design redactable blockchain protocols with instant redaction. We propose a new redaction strategy to decouple the voting stage from the consensus layer. Based on the new strategy, we present a generic approach to construct redactable blockchain protocols with instant redaction, where redactable blockchain inherits the same security assumption from the underlying blockchain. Our protocol can tolerate the optimal $1/2$ adversary as the underlying blockchain, and supports various network environments. Our protocol can also offer accountability for redaction, where any edited block in the chain is publicly verifiable. In addition, multiple redactions per block can be performed throughout the execution of the protocol. We also define the first ideal functionality of redactable blockchain following the language of universal composition, and prove the security of our construction. Moreover, we present concrete instantiations of redactable PoS and PoW blockchains. Finally, we develop a PoC implementation of our PoS instantiation, and the experimental results demonstrate the high efficiency of our design. Our work makes a step forward in understanding of redactable blockchain protocols.

References

[1] M. R., H. J., and H. M., “A quantitative analysis of the impact of arbitrary blockchain content on bitcoin,” in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2018, pp. 420–438.

[2] “Interpol cyber research identifies malware threat to virtual currencies,” *Interpol*, 2015. [Online]. Available: https://www.tinyurl.com/y9wfekr6

[3] “Banking is only the beginning: Big industries blockchain could transform,” 2020. [Online]. Available: https://medium.com/the-capital/banking-is-only-the-beginning-big-industries-blockchain-could-transform-358b218a3fe3

[4] “Governments may be big backers of the blockchain,” 2017. [Online]. Available: https://www.goo.gl/uEjckp

[5] “Akasha,” [Online]. Available: https://akasha.world

[6] “The eu general data protection regulation,” 2016. [Online]. Available: https://gdpr-info.eu/

[7] O. K. Ibanez, Luis-Daniel, and E. Simperl, “On blockchains and the general data protection regulation,” 2018. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

[8] M. Isard and M. Abadi, “Falkirk wheel: Rollback recovery for dataflow systems,” 2015, *arXiv:1503.08877*. [Online]. Available: https://arxiv.org/abs/1503.08877

[9] “Sent money to the wrong account? how to get money back after a misdirected payment,” 2021. [Online]. Available: https://www.lovemoney.com/news/91297/sent-money-to-the-wrong-account-get-money-back-after-misdirected-payment

[10] C. Jentzsch, Decentralized autonomous organization to automate governance, 2017. [Online]. Available: https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/187/2017/07/WhitePaper-1.pdf

[11] “All about the bitcoin cash hard fork,” 2022. [Online]. Available: https://www.investopedia.com/news/all-about-bitcoin-cash-hard-fork

[12] “The hard fork: What’s about to happen to ethereum and the dao,” 2016. [Online]. Available: https://www.coindesk.com/hard-fork-ethereum-dao

[13] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, “Redactable blockchain - or - rewriting history in bitcoin and friends,” in *Proc. IEEE Eur. Symp. Secur. Privacy*, 2017, pp. 111–126.

[14] J. Camenisch, D. Derler, S. Krenn, H. C. Pohls, K. Samelin, and D. Slamanig, “Chameleon-hashes with ephemeral trapdoors,” in *Proc. Int. Workshop Public Key Cryptogr.*, 2017, pp. 152–182.

[15] “Downside of bitcoin: A ledger that can’t be corrected,” *New York Times*, 2016. [Online]. Available: https://tinyurl.com/ydxjlf9es

[16] G. Ateniese, M. T. Chiaramonte, D. Treat, B. Magri, and D. Venturi, “Rewritable blockchain,” US Patent 9,967,096, 2018.

[17] D. Derler, K. Samelin, D. Slamanig, and C. Striecks, “Fine-grained and controlled rewriting in blockchains: Chameleon-hashing gone attribute-based,” in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2019, pp. 211–225.

[18] I. Puddu, A. Dmitrienko, and S. Capkun, “μ chain: How to forget without hard forks,” *Cryptol. ePrint Arch.*, 2017. [Online]. Available: https://eprint.iacr.org/2017/106

[19] D. Deuber, B. Magriy, S. Aravinda, and T. Krishnan, “Redactable blockchain in the permissionless setting,” in *Proc. IEEE Symp. Secur. Privacy*, 2019, pp. 124–138.

[20] S. A. K. Thyagarajan, A. Bhat, B. Magri, D. Tschudi, and A. Kate, “Reparo: Publicly verifiable layer to repair blockchains,” in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2021, pp. 37–56.

[21] R. Pass, L. Seeman, and A. Shelat, “Analysis of the blockchain protocol in asynchronous networks,” in *Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2017, pp. 643–673.

[22] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, “Algorand: Scaling byzantine agreements for cryptocurrencies,” in *Proc. ACM Symp. Operating Syst. Princ.*, 2017, pp. 51–68.

[23] J. Garay, A. Kiayias, and N. Leonardos, “The bitcoin backbone protocol: Analysis and applications,” in *Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2015, pp. 281–310.

[24] R. Pass and E. Shi, “The Sleepy Model of Consensus,” in *Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2017, pp. 380–409.

[25] A. Kiayias, H.-S. Zhou, and V. Zikas, “Fair and robust multi-party computation using a global transaction ledger,” in *Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2016, pp. 705–734.

[26] A. E. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in *Proc. IEEE Symp. Secur. Privacy*, 2016, pp. 839–858.

[27] B. David, P. Gazi, A. Kiayias, and A. Russell, “Ouroboros Praos: An Adaptively-Secure, Semi-Synchronous Proof-of-Stake Blockchain,” in *Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2018, pp. 66–98.

[28] P. Daian, R. Pass, and E. Shi, "Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2019, pp. 23–41.

[29] X. Li, J. Xu, L. Yin, Y. Lu, Q. Tang, and Z. Zhang, "Escaping from consensus: Instantly redactable blockchain protocols in permissionless setting," *Cryptol. ePrint Arch.*, 2021. [Online]. Available: https://eprint.iacr.org/2021/223

[30] H. Chernoff, "A measure of the asymptotic efficiency for tests of a hypothesis based on the sum of observations," *Ann. Math. Statist.*, vol. 23, pp. 493–509, 1952.

[31] " Cardano," [Online]. Available: https://cardano.org/

[32] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "Hotstuff: Bft consensus in the lens of blockchain," 2018, *arXiv: 1803.05069*. [Online]. Available: https://arxiv.org/abs/1803.05069

[33] D. Papadopoulos et al., "Making nsec5 practical for dnssec," *Cryptol. ePrint Arch.*, 2017. [Online]. Available: https://eprint.iacr.org/2017/099

[34] "libsecp256k1-vrf," [Online]. Available: https://github.com/aergoio/secp256k1-vrf

[35] D. Boneh, M. Drijvers, and G. Neven, "Compact multi-signatures for smaller blockchains," in *Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2018, pp. 435–464.

[36] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM J. Comput.*, vol. 17, pp. 281–308, 1988.

[37] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2003, pp. 416–432.

[38] S. Micali, M. Rabin, and S. Vadhan, "Verifiable random functions," in *Proc. IEEE Symp. Found. Comput. Sci.*, 1999, pp. 120–130.

[39] Y. Dodis and A. Yampolskiy, "A verifiable random function with short proofs and keys," in *Proc. Int. Workshop Public Key Cryptogr.*, 2005, pp. 416–431.

Xinyu Li received the PhD degree in computer science and technology from Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences-&University of Chinese Academy of Sciences, Beijing, China, in September 2020. He is currently a postdoctoral fellow with the Department of Computer Science, the University of Hong Kong, Hong Kong. His major research interests include applied cryptography, provable security, authenticated key exchange protocol and blockchain security.

Jing Xu received the PhD degree in computer theory from the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, in June 2002. She is currently a research professor with Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences. Her research interests include applied cryptography and security protocol. She is a senior member of Chinese Association for Cryptologic Research.

Lingyuan Yin received the bachelor's degree in computer science and engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2016. She is currently working toward the PhD degree in software engineering with Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing, and the University of Chinese Academy of Sciences, Beijing. Her current research interests include applied and theoretical cryptography and blockchain technology.

Yuan Lu received the PhD degree in computer science from the New Jersey Institute of Technology, in August 2020. He is currently an associate research professor with Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences. His research interests include blockchain's consensus, decentralized applications, and the design and analysis of cryptograhpic protocols.

Qiang Tang received the PhD degree from the University of Connecticut, in 2015. He is currently a senior lecturer with the University of Sydney. Before joining the USYD, he was an assistant professor with the New Jersey Institute of Technology, and also a director of JACOBI Blockchain Lab and postdoc with Cornell. His research interests broadly lies in applied and theoretical cryptography and blockchain technology, and his work mostly appeared at top venues of security/crypto/distributed computing. He is a recipient of MIT Technical Review 35 Chinese Innovators under 35, 2019, a Google Faculty Award and more.

Zhenfeng Zhang received the PhD degree from the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, in 2001. He is currently a research professor and director with Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences. His main research interests include applied cryptography, security protocol and trusted computing. He is a senior member of the Chinese Association for Cryptologic Research.