The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example

Christopher Natoli
Data61-CSIRO
University of Sydney
christopher.natoli@sydney.edu.au

Vincent Gramoli
Data61-CSIRO
University of Sydney
vincent.gramoli@sydney.edu.au

***Abstract*—In this paper, we identify a new form of attack, called the Balance attack, against proof-of-work blockchain systems. The novelty of this attack consists of delaying network communications between multiple subgroups of nodes with balanced mining power. Our theoretical analysis captures the precise tradeoff between the network delay and the mining power of the attacker needed to double spend in Ethereum with high probability.**

We quantify our probabilistic analysis with statistics taken from the R3 consortium, and show that a single machine needs 20 minutes to attack the consortium. Finally, we run an Ethereum private chain in a distributed system with similar settings as R3 to demonstrate the feasibility of the approach, and discuss the application of the Balance attack to Bitcoin. Our results clearly confirm that main proof-of-work blockchain protocols can be badly suited for consortium blockchains.

Keywords: Ethereum; proof-of-work, GHOST, Chernoff bounds

I. Introduction

Blockchain systems are distributed implementations of a chain of blocks. Each node can issue a cryptographically signed transaction to transfer digital assets to another node or can create a new block of transactions, by solving a crypto-puzzle, and append this block to its current view of the chain. Due to the distributed nature of this task, multiple nodes may append distinct blocks at the same index of the chain before learning about the presence of other blocks, hence leading to a forked chain or a *tree*. For nodes to eventually agree on a unique state of the system, nodes apply a common strategy that selects a unique branch of blocks in this tree.

Bitcoin [23], one of the most popular blockchain systems, selects the longest branch. This strategy has however shown its limitation as it simply *wastes all blocks* not present in this branch [9], [27], [29], [15], [25]. If an attacker can solve crypto-puzzles fast enough to grow a local branch of the blockchain faster than the rest of the system, then it will eventually impose its own branch to all participants. In particular, by delaying the propagation of blocks in the system, one can increase the amount of wasted blocks and proportionally slow down the growth of the longest branch of the system. This delay presents a serious risk to the integrity of the blockchain, as the attacker does not even need a large fraction of the computational power to exceed the length of the chain, allowing her to *double spend* in new transactions the coins that she already spent in earlier transactions [28].

Ethereum [32] proposes another selection strategy that copes with this problem. Each node uses an algorithm, called GHOST, that starts from the first block, also called the *genesis block*, and iteratively selects the root of the heaviest subtree to construct the common branch. Even if nodes create many blocks at the same index of the blockchain, their computational power is not wasted but counted in the selection strategy [29]. In particular, the number of these "sibling" blocks increase the chance that their common ancestor block be selected in favor of another candidate block mined by the attacker. Although it clearly alleviates the Bitcoin limitation discussed above [9], [27], [15], [25] it remains unclear how long an attacker with a low mining power should delay messages to discard previous transactions in Ethereum.

In this paper, we answer this question by demonstrating theoretically and experimentally that an attacker can compensate a low mining power by delaying selected messages in Ethereum. To this end, we propose a simple attack, called the *Balance Attack*: an attacker transiently disrupts communications between subgroups of similar mining power. During this time, the attacker issues transactions in one subgroup, say the *transaction subgroup*, and mines blocks in another subgroup, say the *block subgroup*, up to the point where the tree of the block subgroup outweighs, with high probability, the tree of the transaction subgroup. The novelty of the Balance attack is to leverage the GHOST protocol that accounts for sibling or *uncle* blocks to select a chain of blocks. This strategy allows the attacker to mine a branch possibility in isolation of the rest of the network before merging its branch to one of the competing blockchain to influence the branch selection process.

We experimented a distributed system running Ethereum in similar settings as R3, a consortium of more than 70 world-wide financial institutions. In January, R3 consisted of eleven banks and successfully collaborated in deploying an Ethereum private chain to perform transactions.[1] Since then, R3 has grown and kept experimenting Ethereum[2] and other technologies while the concept of *consortium private*

[1] http://www.ibtimes.co.uk/r3-connects-11-banks-distributed-ledger-using-ethereum-microsoft-azure-1539044.

[2] http://www.coindesk.com/r3-ethereum-report-banks/.

chain gained traction for its ability to offer a blockchain system among multiple companies in a private and controlled environment. R3 has just released their own Corda framework. As opposed to a fully private chain scenario, the consortium private chain involves different institutions possibly competing among each other. As they can be located at different places around the world, they typically use Internet to communicate. We illustrate the Balance attack in the R3 testbed setting as of June 2016, by deploying our own private chain on 15 mining virtual machines in Emulab and configuring the network with ns-2.

While disrupting the communication between subgroups of a blockchain system may look difficult, there have been some attacks successfully delaying messages of Bitcoin in the past. In 2014, a BGP hijacker exploited access to an ISP to steal $83000 worth of bitcoins by positioning itself between Bitcoin pools and their miners [19]. Some known attacks against Bitcoin involved partitioning the communication graph at the network level [1] and at the application level [17]. At the network level, a study indicated the simplicity for autonomous systems to intercept a large amount of bitcoins and evaluated the impact of these network attacks on the Bitcoin protocol [1]. At the application level, some work showed that an attacker controlling 32 IP addresses can "eclipse" a Bitcoin node with 85% probability [17]. More generally, man-in-middle attacks can lead to similar results by relaying the traffic between two nodes through the attacker.

One can exploit the Balance attack to violate the persistence of the main branch, hence rewriting previously committed transactions, and allowing the attacker to double spend. As opposed to previous attacks against Bitcoin where the attacker has to expand the longest chain faster than correct miners to obtain this result [28], the novelty of our attack lies in the contribution of the attacker to one of the correct miner chain in order to outweigh another correct miner chain of Ethereum. We generalize our contribution to proof-of-work algorithms by proposing a simple model for proof-of-work blockchains and specifying Nakamoto's and GHOST consensus algorithmic differences. We also discuss how to adapt the Balance attack to violate the persistence of Bitcoin main branch. This adaptation requires to mine at the top of one of the correct chains rather than solo-mining a subchain but can lead to similar consequences. More precisely, we make the four following contributions:

1) We show that the GHOST consensus protocol can be vulnerable to a double spending attack without coalition and with high probability if a single attacker can delay communication between multiple communication subgraphs while owning 5% of the total mining power of the system.
2) We illustrate the problem in the context of the R3 consortium blockchain, as of June 2016, where we observed 50 nodes among which 15 were mining. We show that one of the nodes can execute a Balance attack by disrupting some communication channels less than 4 minutes.
3) We demonstrate a tradeoff between the mining power needed and the time selected communication channels have to be delayed to attack Ethereum. This suggests that combining network-level with application-level attacks increases the Ethereum vulnerability.
4) We generalize this result to Nakamoto's protocol and propose an adaptation of the Balance attack to double spend in Bitcoin if the attacker can contribute, even with a small power, by mining on top of some of the correct chains.

Section II defines the problem. In Section III, we present the algorithm to run the attack. In Section IV, we show how the analysis affects GHOST. In Section V, we simulate a Balance attack in the context of the R3 consortium network. In Section VI, we present our experiments run in an Ethereum private chain. In Section VII, we discuss the implications of the attack in existing blockchain systems. Section VIII presents the related work. And Section IX concludes. Appendix A includes the missing proofs for the general case.

II. PRELIMINARIES

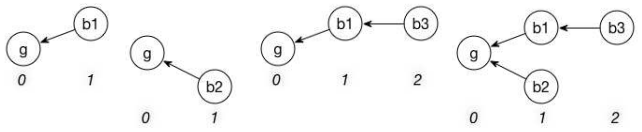
In this section we model a simple distributed system as a communication graph that implements a blockchain abstraction as a directed acyclic graph. We propose a high-level pseudocode representation of proof-of-work blockchain protocols in this model that allows us to illustrate an important difference between Bitcoin and Ethereum in the selection of a main branch with a persistent prefix.

A. A simple distributed model for blockchains

We consider a communication graph $G = \langle V, E \rangle$ with nodes V connected to each other through fixed communication links E. Nodes are part of a blockchain system $S \in \{\mathsf{bitcoin}, \mathsf{ethereum}\}$ and can act as clients by issuing transactions to the system and/or servers by *mining*, the action of trying to combine transactions into a block. For the sake of simplicity, we consider that each node possesses a single account and that a *transaction* issued by node p_i is a transfer of digital assets or *coins* from the account of the source node p_i to the account of a destination node $p_j \neq p_i$. Each transaction is uniquely identified and broadcast to all nodes in a best-effort manner. We assume that a node re-issuing the same transfer multiple times creates as many distinct transactions.

Nodes that mine are called *miners*. We refer to the computational power of a miner as its *mining power* and we denote the total mining power t as the sum of the mining powers of all miners in V. Each miner tries to group a set T of transactions it heard about into a block $b \supseteq T$ as long as transactions of T do not conflict and that the account balances remain non-negative. For the sake of simplicity in the presentation, the graph G is static meaning that no nodes can join and leave the system, however, nodes may fail as described in Section II-A2.

1) Miner must solve a crypto-puzzle to create a new block: Miners provably solve a hashcash crypto-puzzle [3] before creating a new block. Given a global threshold and the block of largest index the miner knows, the miner repeatedly selects



(a) view ℓ_1 (b) view ℓ_2 (c) view ℓ_3 (d) global state $\ell_0 = \ell_1 \cup \ell_2 \cup \ell_3$

Fig. 1: The global state ℓ_0 of a blockchain results from the union of the distributed local views ℓ_1, ℓ_2 and ℓ_3 of the blockchain

a nonce and applies a pseudo-random function to this block and the selected nonce until it obtains a result lower than the threshold. Upon success the miner creates a block that contains the successful nounce as a proof-of-work as well as the hash of the previous block, hence fixing the index of the block, and broadcasts the block. As there is no known strategy to solve the crypto-puzzle, the miners simply keep testing whether randomly chosen numbers solve the crypto-puzzle. The mining power is thus expressed in the number of hashes the miner can test per second, or H/s for short. The *difficulty* of this crypto-puzzle, defined by the threshold, limits the rate at which new blocks can be generated by the network. In the remainder, we refer to d as the difficulty of this crypto-puzzle.

2) The failure model: We assume the presence of an *adversary* (or attacker) that can control nodes that together own a relatively small fraction $\rho < 0.5$ of the total mining power of the system. The nodes controlled by the adversary are called *malicious* and may not follow the protocol specification, however, they cannot impersonate other nodes while issuing transactions.[3] A node that is not malicious is *correct*. We also assume that the adversary can transiently disrupt communications on a selected subset of edges E_0 of the communication graph G.

3) The blockchain abstraction: Let the *blockchain* be a directed acyclic graph (DAG) $\ell = \langle B, P \rangle$ such that blocks of B point to each other with pointers P (pointers are recorded in a block as a hash of the previous block) and a special block $g \in B$, called the *genesis block*, does not point to any block.

Algorithm 1 Blockchain construction at node p_i

1: $\ell_i = \langle B_i, P_i \rangle$, the local blockchain at node p_i is a directed acyclic
2: graph of blocks B_i and pointers P_i

3: receive-blocks$(\langle B_j, P_j \rangle)_i$: ▷ *upon reception of blocks*
4: $B_i \leftarrow B_i \cup B_j$ ▷ *update vertices of blockchain*
5: $P_i \leftarrow P_i \cup P_j$ ▷ *update edges of blockchain*

Algorithm 1 describes the progressive construction of the blockchain at a particular node p_i upon reception of blocks from other nodes by simply aggregating the newly received blocks to the known blocks (lines 3–5). As every added block contains a hash to a previous block that eventually leads back to the genesis block, each block is associated with a fixed index. By convention we consider the genesis block at index 0, and the blocks at k hops away from the genesis block as the blocks at index k. As an example, consider the simple blockchain $\ell_1 = \langle B_1, P_1 \rangle$ depicted in Figure 1(a) where $B_1 = \{g, b_1\}$ and $P_1 = \{\langle b_1, g \rangle\}$. The genesis block g has index 0 and the block b_1 has index 1.

4) Forks as disagreements on the blocks at a given index: As depicted by views ℓ_1, ℓ_2 and ℓ_3 in Figures 1(a), 1(b) and 1(c), respectively, nodes may have a different views of the current state of the blockchain. In particular, it is possible for two miners p_1 and p_2 to mine almost simultaneously two different blocks, say b_1 and b_2. If neither block b_1 nor b_2 was propagated early enough to nodes p_2 and p_1, respectively, then both blocks would point to the same previous block g as depicted in Figures 1(a) and 1(b). Because network delays are not predictable, a third node p_3 may receive the block b_1 and mine a new block without hearing about b_2. The three nodes p_1, p_2 and p_3 thus end up having three different local views of the same blockchain, denoted $\ell_1 = \langle B_1, P_1 \rangle$, $\ell_2 = \langle B_2, P_2 \rangle$ and $\ell_3 = \langle B_3, P_3 \rangle$.

We refer to the *global blockchain* as the directed acyclic graph $\ell_0 = \langle B_0, P_0 \rangle$ representing the union of these local blockchain views, denoted by $\ell_1 \cup \ell_2 \cup \ell_3$ for short, as depicted in Figure 1, and more formally defined as follows:

$$\begin{cases} B_0 &= \cup_{\forall i} B_i, \\ P_0 &= \cup_{\forall i} P_i. \end{cases}$$

The point where distinct blocks of the global blockchain DAG have the same predecessor block is called a *fork*. As an example Figure 1(d) depicts a fork with two branches pointing to the same block: g in this example.

In the remainder of this paper, we refer to the DAG as a *tree* rooted in g with upward pointers, where children blocks point to their parent block.

5) Main branch in Bitcoin and Ethereum: To resolve the forks and define a deterministic state agreed upon by all nodes, a blockchain system must select a *main branch*, as a unique sequence of blocks, based on the tree. Building upon the generic construction (Alg. 1), we present two selections: Nakamoto's consensus protocol (Alg. 2) present in Bitcoin [23] and the GHOST consensus protocol (Alg. 3) present in Ethereum [32].

a) Nakamoto's consensus algorithm: The difficulty of the crypto-puzzles used in Bitcoin produces a block every 10 minutes in expectation. The advantage of this long period, is that it is relatively rare for the blockchain to fork because blocks are rarely mined during the time others are propagated to the rest of the nodes.

Algorithm 2 depicts the Bitcoin-specific pseudocode that includes Nakamoto's consensus protocol to decide on a particular block at index i (lines 8–18) and the choice of parameter m (line 6) explained later in Section II-B. When a fork occurs, Nakamoto's protocol resolves it by selecting the deepest branch as the main branch (lines 8–15) by iteratively selecting the root of the deepest subtree (line 11). When process p_i is

[3]This is typically ensured through public key crypto-systems.

Algorithm 2 Nakamoto's consensus protocol at node p_i

6: $m = 5$, the number of blocks to be appended after the block containing
7: tx, for tx to be committed in Bitcoin

8: get-main-branch()$_i$: ▷ *select the longest branch*
9: $b \leftarrow$ genesis-block(B_i) ▷ *start from the blockchain root*
10: **while** $b.children \neq \emptyset$ **do** ▷ *prune shortest branches*
11: $block \leftarrow \text{argmax}_{c \in b.children}\{\text{depth}(c)\}$ ▷ *root of deepest subtree*
12: $B \leftarrow B \cup \{block\}$ ▷ *update vertices of main branch*
13: $P \leftarrow P \cup \{\langle block, b\rangle\}$ ▷ *update edges of main branch*
14: $b \leftarrow block$ ▷ *move to next block*
15: **return** $\langle B, P\rangle$ ▷ *returning the Bitcoin main branch*

16: depth(b)$_i$: ▷ *depth of tree rooted in b*
17: **if** $b.children = \emptyset$ **then return** 1 ▷ *stop at leaves*
18: **else return** $1 + \max_{c \in b.children}$ depth(c) ▷ *recurse at children*

Algorithm 3 The GHOST consensus protocol at node p_i

6: $m = 11$, the number of blocks to be appended after the block containing
7: tx, for tx to be committed in Ethereum (since Homestead v1.3.5)

8: get-main-branch()$_i$: ▷ *select the branch with the most nodes*
9: $b \leftarrow$ genesis-block(B_i) ▷ *start from the blockchain root*
10: **while** $b.children \neq \emptyset$ **do** ▷ *prune lightest branches*
11: $block \leftarrow \text{argmax}_{c \in b.children}\{\text{num-desc}(c)\}$ ▷ *root of heaviest tree*
12: $B \leftarrow B \cup \{block\}$ ▷ *update vertices of main branch*
13: $P \leftarrow P \cup \{\langle block, b\rangle\}$ ▷ *update edges of main branch*
14: $b \leftarrow block$ ▷ *move to next block*
15: **return** $\langle B, P\rangle$. ▷ *returning the Ethereum main branch*

16: num-desc(b)$_i$: ▷ *number of nodes in tree rooted in b*
17: **if** $b.children = \emptyset$ **then return** 1 ▷ *stop at leaves*
18: **else return** $1 + \sum_{c \in b.children}$ num-desc(c) ▷ *recurse at children*

done with this pruning, the resulting branch becomes the main branch $\langle B_i, P_i\rangle$ as observed by the local process p_i. Note that the pseudocode for checking whether a block is decided and a transaction committed based on this parameter m is common to Bitcoin and Ethereum, it is thus deferred to Alg. 4.

6) The GHOST *consensus algorithm:* As opposed to the Bitcoin protocol, Ethereum generates one block every 12–15 seconds. While it improves the throughput (transactions per second) it also favors transient forks as miners are more likely to propose new blocks without having heard about the latest mined blocks yet. To avoid wasting large mining efforts while resolving forks, Ethereum uses the GHOST (Greedy Heaviest Observed Subtree) consensus algorithm that accounts for the, so called *uncles*, blocks of discarded branches. In contrast with Nakamoto's protocol, the GHOST protocol iteratively selects, as the successor block, the root of the subtree that contains the largest number of nodes (cf. Algorithm 3).

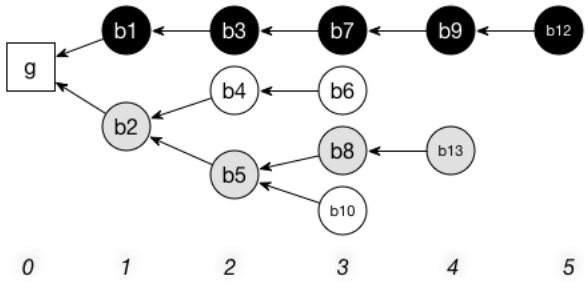


Fig. 2: Nakamoto's consensus protocol at the heart of Bitcoin selects the main branch as the deepest branch (in black) whereas the GHOST consensus protocol at the heart of Ethereum follows the heaviest subtree (in grey)

The main difference between Nakamoto's consensus protocol and GHOST is depicted in Figure 2, where the black blocks represent the main branch selected by Nakamoto's consensus protocol and the grey blocks represent the main branch selected by GHOST.

B. Decided blocks and committed transactions

A blockchain system S must define when the block at an index is agreed upon. To this end, it has to define a point in its execution where a prefix of the main branch can be "reasonably" considered as persistent.[4] More precisely, there must exist a parameter m provided by S for an application to consider a block as *decided* and its transactions as *committed*. This parameter is typically $m_{bitcoin} = 5$ in Bitcoin (Alg. 2, line 6) and $m_{ethereum} = 11$ in Ethereum (Alg. 3, line 6).

Definition 1 (Transaction commit)**.** *Let $\ell_i = \langle B_i, P_i\rangle$ be the blockchain view at node p_i in system S. For a transaction tx to be* locally committed *at p_i, the conjunction of the following properties must hold in p_i's view ℓ_i:*

1) *Transaction tx has to be in a block $b_0 \in B_i$ of the main branch of system S. Formally, $tx \in b_0 \wedge b_0 \in B'_i : c_i = \langle B'_i, P'_i\rangle =$ get-main-branch()$_i$.*
2) *There should be a subsequence of m blocks $b_1, ..., b_m$ appended after block b. Formally, $\exists b_1, ..., b_m \in B_i : \langle b_1, b_0\rangle, \langle b_2, b_1\rangle, ..., \langle b_m, b_{m-1}\rangle \in P_i$. (In short, we say that b_0 is* decided*.)*

A transaction tx is committed *if there exists a node p_i such that tx is* locally committed*.*

Property (1) is needed because nodes eventually agree on the main branch that defines the current state of accounts in the system—blocks that are not part of the main branch are ignored. Property (2) is necessary to guarantee that the blocks and transactions currently in the main branch will persist and remain in the main branch. Before these additional blocks are created, nodes may not have reached consensus regarding the unique blocks b at index j in the chain. This is illustrated by the fork of Figure 1 where nodes consider, respectively, the pointer $\langle b_1, g\rangle$ and the pointer $\langle b_2, g\rangle$ in their local blockchain view. By waiting for m blocks were m is given by the blockchain system, the system guarantees with a reasonably high probability that nodes will agree on the same block b.

[4]In theory, there cannot be consensus on a block at a partiular index [13], hence preventing persistence, however, applications have successfully used Ethereum to transfer digital assets based on parameter $m_{ethereum} = 11$ [24].

Algorithm 4 Checking transaction commit at node p_i

19: is-committed$(tx)_i$: ▷ *check whether transaction is committed*
20: $\langle B'_i, P'_i \rangle \leftarrow$ get-main-branch() ▷ *pick main branch with Alg. 2 or 3*
21: **if** $\exists b_0 \in B'_i : tx \in b_0 \wedge \exists b_1, ..., b_m \in B_i :$ ▷ *tx in main branch*
22: $\langle b_1, b_0 \rangle, \langle b_2, b_1 \rangle ..., \langle b_m, b_{m-1} \rangle \in P_i$ **then** ▷ *enough blocks*
23: **return** true
24: **else return** false

For example, consider a fictive blockchain system with $m_{fictive} = 2$ that selects the heaviest branch (Alg. 3, lines 8–15) as its main branch. If the blockchain state was the one depicted in Figure 2, then blocks b_2 and b_5 would be decided and all their transactions would be committed. This is because they are both part of the main branch and they are followed by at least 2 blocks, b_8 and b_{13}. (Note that we omit the genesis block as it is always considered decided but does not include any transaction.)

III. The Balance Attack

In this section, we present the Balance attack, a novel form of attacks that affect proof-of-work blockchains, especially Ethereum. Its novelty lies in identifying subgroups of miners of equivalent mining power and delaying messages between them rather than entering a race to mine blocks faster than others.

The balance attack demonstrates a fundamental limitation of main proof-of-work systems in that they are block oblivious.

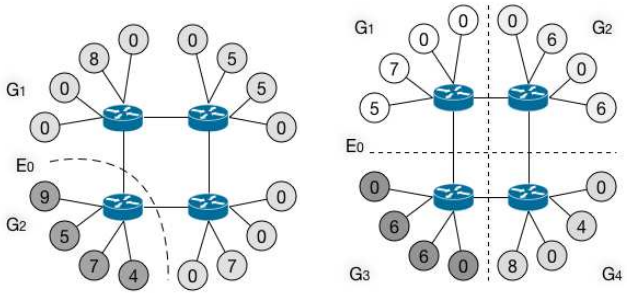
Definition 2 (Block Obliviousness)**.** *A blockchain system is* block oblivious *if an attacker can:*

1) *make the recipient of a transaction tx observe that tx is committed and*
2) *later remove the transaction tx from the main branch,*

with a probability $1 - \varepsilon$, where ε is a small constant.

The balance attack is simple: after the attacker introduces a delay between correct subgroups of equivalent mining power, it simply issues transactions in one subgroup. The attacker then mines sufficiently many blocks in another subgroup to ensure with high probability that the subtree of another subgroup outweighs the transaction subgroup's. Even though the transactions are committed, the attacker can rewrite with high probability the blocks that contain these transactions by outweighing the subtree containing this transaction.

Note that one could benefit from delaying messages only between the merchant and the rest of the network by applying the eclipse attack [17] to Ethereum. Eclipsing one node of Bitcoin appeared, however, sufficiently difficult: it requires to restart the node's protocol in order to control all the logical neighbors the node will eventually try to connect to. While a Bitcoin node typically connects to 8 logical neighbors, an Ethereum node typically connects to 25 nodes, making the problem even harder. Another option would be to isolate a subgroup of smaller mining power than another subgroup, however, it would make the attack only possible if the recipients of the transactions are located in the subgroup of smaller mining power. Although possible this would limit the generality of the attack, because the attacker would be constrained on the transactions it can override.



(a) Example of the selection of edges E_0 delayed between $k = 2$ subgraphs of 25 units of mining power each

(b) Example of the selection of edges E_0 delayed between $k = 4$ subgraphs of 12 units of mining power each

Fig. 3: Two decompositions of communication graphs into subgraphs by an attacker where E_0 represents the cut of communication edges linking the subgraphs

Note that the Balance Attack inherently violates the persistence of the main branch prefix and is enough for the attacker to double spend. The attacker has simply to identify the subgroup that contains merchants and create transactions to buy goods from these merchants. After that, it can issue the transactions to this subgroup while propagating its mined blocks to at least one of the other subgroups. Once the merchant shipped goods, the attacker stops delaying messages. Based on the high probability that the tree seen by the merchant is outweighed by another subtree, the attacker could reissue another transaction transferring the exact same coin again.

A. Executing a Balance Attack

For the sake of simplicity, let us fix $k = 2$ and postpone the general analysis for any $k \geq 2$ to Appendix A. We consider subgraphs $G_1 = \langle V_1, E_1 \rangle$ and $G_2 = \langle V_2, E_2 \rangle$ of the communication graph $G = \langle V, E \rangle$ so that each subgraph has half of the mining power of the system as depicted in Figure 3(a) whereas Figure 3(a) illustrates the variant when $k = 4$. Let $E_0 = E \setminus (E_1 \cup E_2)$ be the set of edges that connects nodes of V_1 to nodes of V_2 in the original graph G. Let τ be the communication delay introduced by the attacker on the edges of E_0.

As indicated in Algorithm 5, the attacker can introduce a sufficiently long delay τ during which the miners of G_1 mine in isolation of the miners of G_2 (line 13). As a consequence, different transactions get committed in different series of blocks on the two blockchains locally viewed by the subgraphs G_1 and G_2. Let b_2 be a block present only in the blockchain viewed by G_2 but absent from the blockchain viewed by G_1. In the meantime, the attacker issues transactions spending coins C in G_1 (line 14) and mines a blockchain starting from the

Algorithm 5 The Balance Attack initiated by attacker p_i

1: **State:**
2: $G = \langle V, E \rangle$, the communication graph
3: pow, a mapping from of a node in V to its mining power in $\mathbb{R}$
4: $\ell_i = \langle B_i, P_i \rangle$, the local blockchain at node p_i is a directed acyclic
5: graph of blocks B_i and pointers P_i
6: $\rho \in (0; 1)$, the portion of the mining power of the system owned by
7: the attacker p_i, typically $\rho < 0.5$
8: d, the difficulty of the crypto-puzzle currently used by the system

9: balance-attack$(\langle V, E \rangle)_i$: ▷ *starts the attack*
10: Select $k \geq 2$ subgraphs $G_1 = \langle V_1, E_1 \rangle, ..., G_k = \langle V_k, E_k \rangle$:
11: $\sum_{\forall v \in V_1} \text{pow}(v) \approx ... \approx \sum_{\forall v' \in V_k} \text{pow}(v')$
12: Let $E_0 = E \setminus \cup_{\forall 0 < i \leq k} E_i$ ▷ *attack communication channels*
13: Stop communications on E_0 during $\tau \geq \frac{(1-\rho)6d\log(\frac{4}{\varepsilon})}{4\rho^2 t}$ seconds
14: Issue transaction tx crediting a merchant in graph G_i with coins C
15: Let b_2 be a block appearing in G_j but not in G_i
16: Start mining on ℓ_i immediately after b_2 ▷ *contributed to correct chain*
17: Send blockchain view ℓ_i to some subgraph G_j where $j \neq i$
18: When τ seconds have elapsed, stop delaying communications on E_0
19: Issue transaction tx' that double spends coins C

block b_2 (line 16). Before the delay expires the attacker sends his blockchain to G_2. After the delay expires, the two local views of the blockchain are exchanged. Once the heaviest branch that the attacker contributed to is adopted, the attacker can simply reuse the coins C in new transactions (line 19).

B. The knowledge about the network

As indicated by the state of Algorithm 5, an attacker has to be knowledgeable about the current settings of the blockchain system to execute a Balance attack. In fact, the attacker must have information regarding the logical or physical communication graph, the mining power of the miners or pools of miners and the current difficulty of the crypto-puzzle. In particular, this information is needed to delay messages for long enough between selected communication subgraphs. As we will show in the next section, this delay can be overestimated, however, underestimating it may make the attack impossible.

The information regarding the mining power and the difficulty of nodes is generally public information and can often be retrieved online. In particular, we got provided an access to the R3 Ethereum network statistics http://r3n1-utils.gcl.r3cev.com/ that included block propagation delays, the list of connected nodes and their individual mining power, the version of their Ethereum client as well as the current difficulty of the crypto-puzzle. The same statistical information regarding the Ethereum public chain is publicly available online at https://ethstats.net/.

It is more difficult, however, to gather information regarding the communication network. Note that some tools exist to retrieve information regarding the communication topology of blockchain systems. The interesting aspects of the Balance attack is that it can apply to the logical overlay used by the peer-to-peer network of the blockchain system or to the physical overlay. While there exist tools to retrieve the logical overlay topology, like AddressProbe [21] to find some information regarding the peer-to-peer overlay of Bitcoin, it can be easier for an attacker of Ethereum to run a DNS poisoinning or a denial-of-service attack rather than a BGP hijacking [19], [1] that requires access to autonomous systems.

IV. Vulnerability of the Ghost Protocol

In this Section, we show that the Balance attack makes a blockchain system based on GHOST (depicted in Alg. 3) block oblivious. A malicious user can issue a Balance attack with less than half of the mining power by delaying the network. Let us first summarize previous and new notations in Table I.

t	total mining power of the system (in million hashes per second, MH/s)
d	difficulty of the crypto-puzzle (in million hashes, MH)
ρ	fraction of the mining power owned by the malicious miner (in percent, %)
k	the number of communication subgraphs
τ	time during which communication between subgraphs is disrupted (in seconds, s)
μ_c	mean of the number of blocks mined by each communication subgraph during τ
μ_m	mean of the number of blocks mined by the attacker during time τ
Δ	the maximum difference of mined blocks for the two subgraphs

TABLE I: Notations of the analysis

For the sake of simplicity in the proof, we assume that $k = 2$ and $\sum_{\forall v \in V_1} \text{pow}(v) = \sum_{\forall v' \in V_2} \text{pow}(v')$ so that the communication is delayed between only two communication subgraphs of equal mining power. We defer the proof for the general case where $k \geq 2$ to Appendix A.

As there is no better strategy for solving the crypto-puzzles than random trials, we consider that subgraphs G_1 and G_2 mine blocks during delay τ. During that time, each of G_1 and G_2 performs a series of $n = \frac{1-\rho}{k} t\tau$ independent and identically distributed Bernoulli trials that returns one in case of success with probability $p = \frac{1}{d}$ and 0 otherwise. Let the sum of these outcomes for subgraphs G_1 and G_2 be the random variables X_1 and X_2, respectively, each with a binomial distribution and mean:

$$\mu_c = np = \frac{(1-\rho)t\tau}{2d}. \quad (1)$$

Similarly, the mean of the number of blocks mined by the malicious miner during time τ is

$$\mu_m = \frac{\rho t \tau}{d}.$$

From line 13 of Alg. 5, we know that $\tau \geq \frac{(1-\rho)6d\log(\frac{4}{\varepsilon})}{4\rho^2 t}$ which leads to:

$$\begin{aligned} \tau &\geq \frac{(1-\rho)6d\log(\frac{4}{\varepsilon})}{4\rho^2 t}, \\ \frac{(1-\rho)t\tau}{2d} &\geq \frac{3(1-\rho)^2\log(\frac{4}{\varepsilon})}{4\rho^2}. \end{aligned}$$

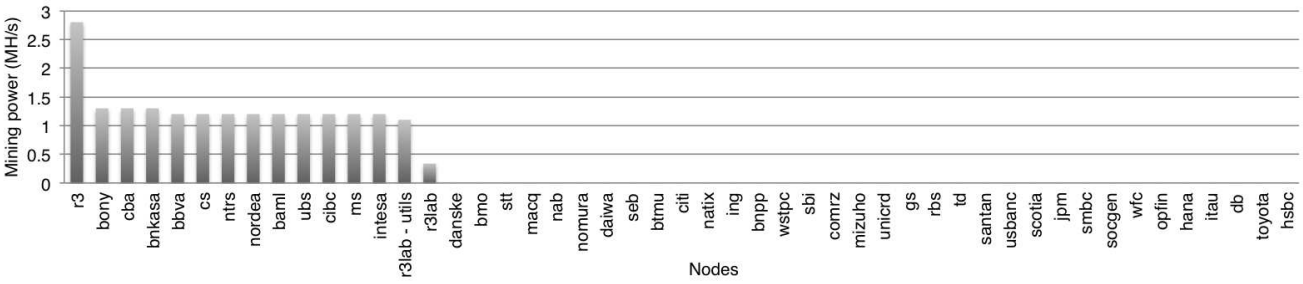


Fig. 4: The mining power of the R3 Ethereum network as reported by `eth-netstats` as of June 2016

By Eq. 4 we have:

$$\begin{aligned} \mu_c &\geq \frac{3(1-\rho)^2 \log(\frac{4}{\varepsilon})}{4\rho^2}, \\ \frac{4\rho^2\mu_c}{3(1-\rho)^2} &\geq \log\left(\frac{4}{\varepsilon}\right), \\ -\frac{4\rho^2\mu_c}{3(1-\rho)^2} &\leq \log\left(\frac{\varepsilon}{4}\right), \\ e^{-\frac{4\rho^2\mu_c}{3(1-\rho)^2}} &\leq \frac{\varepsilon}{4}, \\ 1-4e^{-\frac{4\rho^2\mu_c}{3(1-\rho)^2}} &\geq 1-\varepsilon. \end{aligned} \tag{2}$$

The attack relies on minimizing the difference in mined blocks between any pair of communication subgraphs.

Lemma 3. *After the communication is re-enabled, the expectation of the number of blocks mined by the attacker is greater than the difference $\Delta = |X_1 - X_2|$ of the number of blocks mined on the two subgraphs G_1 and G_2, with probability $1-\varepsilon$.*

Proof: The communication is re-enabled at line 18 of Alg. 5. At this point in the execution, the probability that the numbers of blocks mined by each subgraph are within a $\pm\delta$ factor from their mean, is bound for $0 < \delta < 1$ and $i \in \{1, 2\}$ by Chernoff bounds [22]:

$$\begin{cases} \Pr\left[X_i \geq (1+\delta)\mu_c\right] & \leq e^{-\frac{\delta^2}{3}\mu_c}, \\ \Pr\left[X_i \leq (1-\delta)\mu_c\right] & \leq e^{-\frac{\delta^2}{2}\mu_c}. \end{cases}$$

Thus, we have

$$\Pr[|X_i - \mu_c| < \delta\mu_c] \quad > \quad 1 - 2e^{-\frac{\delta^2}{3}\mu_c}.$$

Observe that the probability that these two random variables are both within a $\pm\delta\mu_c$ is lower than the probability that their difference Δ is upper-bounded by $2\delta\mu_c$:

$$\left(\Pr\left[|X_i - \mu_c| < \delta\mu_c\right]\right)^2 \leq \Pr[\Delta < 2\delta\mu_c].$$

Thus, we obtain:

$$\Pr[\Delta < 2\delta\mu_c] > \left(1 - 2e^{-\frac{\delta^2}{3}\mu_c}\right)^2. \tag{3}$$

As $\mu_c \geq 0$, we have that:

$$\begin{aligned} -\frac{\delta^2}{3}\mu_c &\leq 0, \\ -e^{\frac{-\delta^2}{3}\mu_c} &\geq -1, \end{aligned}$$

and we can apply the Bernoulli inequality to Eq. 3:

$$\Pr[\Delta < 2\delta\mu_c] \quad > \quad 1 - 4e^{-\frac{\delta^2}{3}\mu_c}.$$

If we replace δ by $\frac{2\rho}{1-\rho}$, we obtain:

$$\Pr[\Delta < \mu_m] \quad > \quad 1 - 4e^{-\frac{4\rho^2\mu_c}{3(1-\rho)^2}}.$$

By Eq. 2, we can see that the expectation of the number of blocks mined by the attacker is strictly greater than Δ with high probability:

$$\Pr[\Delta < \mu_m] \quad > \quad 1 - \varepsilon.$$

■

Theorem 4. *A blockchain system that selects a main branch based on the* GHOST *protocol (Alg. 3) is block oblivious.*

Proof: By lines 17–18 of Alg. 3, we know that GHOST counts every mined blocks to compute the weight of a subtree, and to select one blockchain view and discard the other.

Since the expected number of blocks mined by the attacker is greater than the difference Δ with probability $1-\varepsilon$, we know that when the timer expires at line 18 of Alg. 5, the attacker will make the system discard the blockchain view of either G_1 or G_2 by sending its blockchain view to the other subgraph, hence making the blockchain system block oblivious. ■

V. Analysis of the R3 Testbed

The statistics of the R3 testbed were gathered through the `eth-netstat` applications at the end of June 2016.[5] R3 is a consortium of more than 50 banks that has tested blockchain systems and in particular Ethereum in a consortium private chain context over 2016.[6] As depicted in Figure 4, the network consisted at that time of $|V| = 50$ nodes among which only 15 were mining. The mining power of the system was about 20 MH/s and the most powerful miner mines at 2.4 MH/s or 12% of the total mining power while the difficulty of the crypto-puzzle was observed close to 30 MH.

We assume that the attacker selects communication edges E_0 between two subgraphs G_1 and G_2 so that their mining power is 8.8 MH/s each. The probability p of solving the crypto-puzzle per hash tested is $\frac{1}{30\times10^6}$ so that the mean is

[5] http://r3n1-utils.gcl.r3cev.com/.
[6] http://www.coindesk.com/r3-ethereum-report-banks

Number of nodes	50
Number of miners	15
Total mining power (MH/s)	20
Mining power of the most powerful miner (MH/s)	2.4
Difficulty (MH)	30

TABLE II: The R3 settings used in the analysis

$\mu_c = np = 95.3$ if we wait for 19 minutes and 40 seconds. The attacker creates, in expectation, a block every $\frac{30}{2.4} = 12.5$ seconds or $\lfloor \frac{1180}{12.5} \rfloor = 94$ blocks during the 19 minutes and 40 seconds. Hence let us select δ such that the attacker has a chance to mine more than $2\delta\mu_c$ blocks during that period, i.e., $94 = 2\delta\mu_c + 1$ implying that $\delta = 0.1343$. The probability of the difference exceeding 94 is upper bounded by $4e^{-\frac{\delta^2}{3}\mu_c}$ leading to a bound of 49.86%.

To conclude a single miner of the R3 testbed needs to delay edges of E_0 during less than 20 minutes to execute a Balance attack and discards blocks that were previously decided (even if $m = 18$ was chosen) with a chance of success greater than $\frac{1}{2}$.

A. Tradeoff between communication delays and mining power

Malicious nodes may have an incentive to form a coalition in order to exploit the Balance attack to double spend. In this case, it is easier for the malicious nodes to control a larger portion of the mining power of the system, hence such a coalition would not need to delay messages as long as in our example of Section V. For simplicity, we again consider the case where the attacker delay messages between $k = 2$ communication subgraphs.

To illustrate the tradeoff between communication delay and the portion of the mining power controlled by the attacker, we consider the R3 testbed with a 30 MH total difficulty, a 20 MH/s total mining power and plot the probability as the communication delay increases for different portions of the mining power controlled by the adversary. Figure 5 depicts this result. As expected, the probability increases exponentially fast as the delay increases, and the higher the portion of the mining power is controlled by the adversary the faster the probability increases. In particular, in order to issue a balance attack with 90% probability, 51 minutes are needed for an adversary controlling 12% of the total mining power whereas only 11 minutes are sufficient for an adversary who controls 20% of the mining power.

B. Tradeoff between communication delays and difficulties

Another interesting aspect of proof-of-work blockchain is the difficulty parameter d. As already mentioned, this parameter impacts the expected time it takes for a miner to succeed in solving the crypto-puzzle. When setting up a private chain, one has to choose a difficulty to make sure the miners would mine at a desirable pace. A too high difficulty reduces the throughput of the system without requiring leader election [10] or consensus sharding [20]. A too low difficulty increases the probability for two correct miners to solve the crypto-puzzle

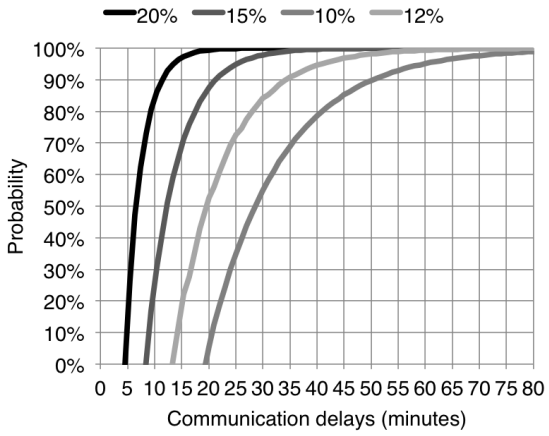


Fig. 5: Probability of Balance attack in the R3 testbed as the communication delay increases for different portions of the mining power controlled by the attacker

before one can propagate the block to the other, a problem of Bitcoin that motivated the GHOST protocol [29].

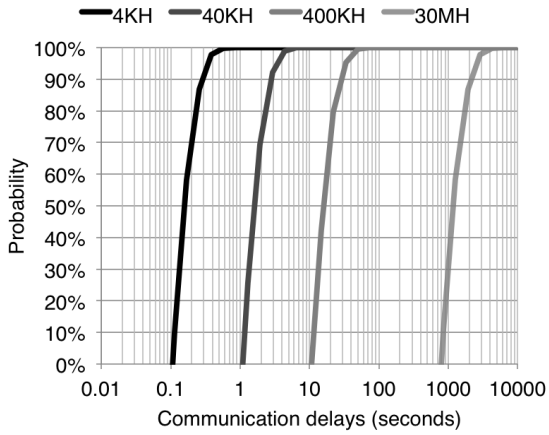


Fig. 6: Probability of Balance attack in the R3 testbed (with 20 MH/s of total mining power, 12% of the mining power at the attacker) for different difficulties as the communication delay increases

Figure 6 depicts the probability of the Blockchain anomaly when the communication delay increases for different difficulties without considering the time for a block to be decided. Again, we consider the R3 Ethereum network with a total mining power of 30 MH/s and an attacker owning $\rho = 12\%$ of this mining power and delaying communications between $k = 2$ subgraphs of half of the remaining mining power ($\frac{1-\rho}{2} = 44\%$) each. The curve labelled 4 KH indicates a difficulty of 4000 hashes, which is also the difficulty chosen by default by Ethereum when setting up a new private chain system. This difficulty is dynamically adjusted by Ethereum at runtime to keep the mining block duration constant in

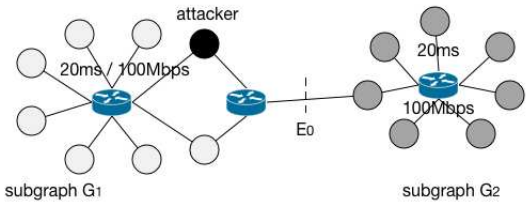


Fig. 7: The topology of our experiment involving 15 miners with subgraph G_1 including the attacker depicted in black and subgraph G_2 depicted in grey

expectation, however, this adaptation is dependent on the visible mining power of the system. The curve labelled 30 MH indicates the probability for the difficulty observed in the R3 Ethereum network. We can clearly see that the difficulty impacts the probability of the Balance attack. This can be explained by the fact that the deviation of the random variables $X_1, ..., X_k$ from their mean μ_c is bounded for sufficiently large number of mined blocks.

VI. Experimenting the Balance Attack on an Ethereum Private Chain

In this section, we experimentally produce the attack on an Ethereum private chain involving up to 18 physical distributed machines. To this end, we configure a realistic network with 15 machines dedicated to mining as in the R3 Ethereum network we described in Section V and 3 dedicated network switches.

All experiments were run on 18 physical machines of the Emulab environment where a network topology was configured using ns/2 as depicted in Figure 7. The topology consists of three local area networks configured through a ns/2 configuration file with 20 ms latency and 100 Mbps bandwidth. All miners run the `geth` Ethereum client v.1.3.6 and the initial difficulty of the crypto-puzzle is set to 40 KH. The communication graph comprises the subgraph G_1 of 8 miners that includes the attacker and 7 correct miners and a subgraph G_2 of 7 correct miners.

A. Favoring one blockchain view over another

We run our first experiment during 2 minutes. We delayed the link E_0 during 60 seconds so that both subgraphs mine in isolation from each other during that time and end up with distinct blockchain views. After the delay we take a snapshot, at time t_1, of the blocks mined by each subgraphs and the two subgraphs start exchanging information normally leading to a consensus regarding the current state of the blockchain. At the end of the experiment, after 2 minutes we take another snapshot t_2 of the blocks mined by each subgraph.

Table III lists the prefix of the hashes of blocks (excluding uncles) of the blockchain views of G_1 and G_2 at times t_1, while the two subgraphs did not exchange their view, and at time t_2, after the subgraphs exchanged their blocks. Note that

blocks viewed at G1 at t1

0x01d7...	0x57a6...	0xd159...
0x044a...	0x5b12...	0xd27a...
0x0b02...	0x628f...	0xd451...
0x0d45...	0x675d...	0xd4e8...
0x120d...	0x6f53...	0xda82...
0x1341...	0x74ca...	0xe3d5...
0x15e8...	0x7529...	0xe8ee...
0x16e0...	0x8ba9...	0xead5...
0x1c88...	0x9ad4...	0xedb2...
0x2372...	0x9bd0...	0xf0e7...
0x288a...	0x9f08...	0xf96b...
0x28fe...	0xabe4...	0xfab2...
0x2e77...	0xacf9...	0xfaf4...
0x2f6a...	0xb2af...	
0x2fd9...	0xb334...	
0x37ae...	0xb4f4...	
0x3a2f...	0xb51d...	
0x3f37...	0xb788...	
0x3f7a...	0xb901...	
0x4190...	0xbec6...	

blocks viewed at G2 at t1

0x019d...	0x5e2b...	0xc09a...
0x072b...	0x6084...	0xc208...
0x0913...	0x6481...	0xc396...
0x10dc...	0x64aa...	0xc56d...
0x1479...	0x665b...	0xc608...
0x1d41...	0x6a31...	0xc666...
0x1f03...	0x7004...	0xc897...
0x1f67...	0x7084...	0xd840...
0x2602...	0x70a8...	0xd972...
0x3337...	0x7396...	0xe28c...
0x33fd...	0x73d1...	0xe4f1...
0x36e7...	0x8254...	0xe51e...
0x3840...	0x835a...	0xea17...
0x3a2c...	0x8392...	0xedf1...
0x3b50...	0x9cb8...	0xef24...
0x3f85...	0x9e12...	0xf05a...
0x4627...	0xa054...	0xfdc4...
0x4aa3...	0xa1ec...	0xfe8c...
0x50a9...	0xa549...	
0x559b...	0xac05...	

blocks viewed at G1 and G2 at t2

0x00d2...	0x27aa...	0x5122...	0x816b...	0xada0...	0xcb76...	0xf9e0...
0x0474...	0x27b9...	0x534b...	0x81b8...	0xaf8a...	0xcff1...	0xfab2...
0x079d...	0x282a...	0x5694...	0x891a...	0xb002...	0xd159...	0xfc57...
0x0919...	0x2a0b...	0x56ed...	0x8945...	0xb0c4...	0xd1d5...	0xff78...
0x0927...	0x2fd3...	0x5b12...	0x8faf...	0xb128...	0xd463...	0xffd8...
0x09a7...	0x2fd9...	0x64ee...	0x9096...	0xb14f...	0xd792...	
0x09f1...	0x3077...	0x6758...	0x92a1...	0xb334...	0xdd61...	
0x0c33...	0x3244...	0x675d...	0x9456...	0xb51d...	0xe50d...	
0x0fb7...	0x32b1...	0x6bda...	0x96f9...	0xb68f...	0xe6a0...	
0x1115...	0x37e3...	0x6c82...	0x9749...	0xb6c3...	0xe970...	
0x11ef...	0x381b...	0x6e38...	0x980f...	0xb891...	0xeb43...	
0x1341...	0x386e...	0x720b...	0x9a7b...	0xbdda...	0xedb2...	
0x15cc...	0x389f...	0x7485...	0x9bd0...	0xbec7...	0xeeec...	
0x1b54...	0x39ed...	0x74d5...	0x9c80...	0xbf58...	0xef42...	
0x1be5...	0x3cf7...	0x76fb...	0x9c94...	0xc240...	0xefa9...	
0x1c76...	0x3d7b...	0x781b...	0x9e33...	0xc484...	0xf219...	
0x1c88...	0x3f7a...	0x79db...	0xaa4e...	0xc615...	0xf324...	
0x20a6...	0x4558...	0x7a68...	0xabe4...	0xc768...	0xf5bc...	
0x23af...	0x4a41...	0x7cf9...	0xabeb...	0xc871...	0xf828...	
0x259a...	0x4c0c...	0x7fa1...	0xad18...	0xca35...	0xf86e...	

TABLE III: Hash prefixes of the blocks of the main branch (excluding uncles) selected by the subgraphs G_1 and G_2; the blocks of G_2 at time t_1 do no longer appear at time t_2

we did not represent the uncle blocks to focus on the main branches. We observe that the blockchain view of the subgraph G_1 was adopted as the valid chain while the other blockchain view of the subgraph G_2 was not. For example, one of the listed blocks viewed by G_1 at time t_1 whose hash starts with `0xfab2` appears as well in the final blockchain at time t_2. More generally, we can see that only blocks of the blockchain view of G_1 at time t_1 were finally adopted at time t_2 as part of the blocks of the global view of the blockchain. All the blocks of G_2 at time t_1 were discarded from the blockchain by time t_2.

B. Blocks mined by an attacker and two subgraphs

We now report the total number of blocks mined, especially focusing on the creation of uncle blocks. More precisely, we compare the number of blocks mined by the attacker against the difference of the number of blocks Δ mined by each subgraph. We know from the analysis that it is sufficient for

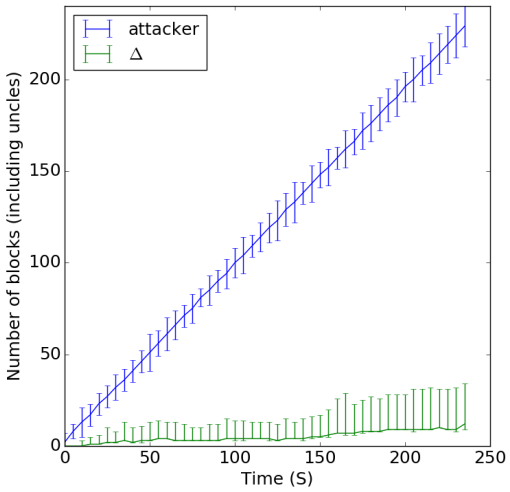


Fig. 8: The total number of blocks (including uncles) mined by the attacker and the difference Δ in the total number of blocks (including uncles) mined by the two subgraphs G_1 and G_2 (error bars indicate minimum and maximum observed over 10 runs)

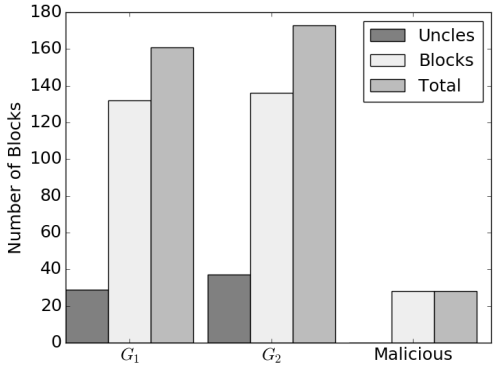


Fig. 9: The total number of blocks (including uncles and non-uncles) mined by the attacker and the two subgraphs G_1 and G_2

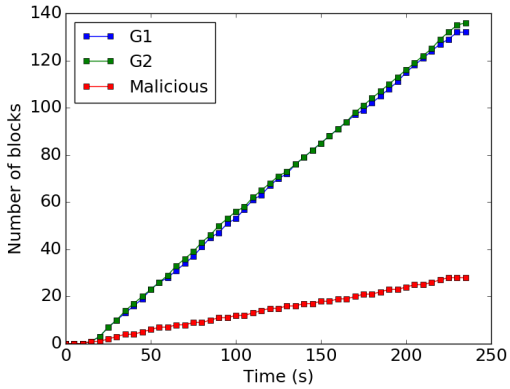


Fig. 10: The depth of the blockchains mined by the attacker and two subgraphs G_1 and G_2

the attacker to mine at least $\Delta + 1$ blocks in order to be able to discard one of the k blockchain views, allowing for double spending. The experiment is similar to the previous experiment in that we also used Emulab with the same ns/2 topology, however, we did not introduce delays and averaged results over 10 runs of 4 minutes each.

Figure 8 depicts the minimum, maximum and average blocks obtained over the 10 runs. The vertical bars indicate minimum and maximum. First, we can observe that the average difference Δ is usually close to its minimum value observed during the 10 runs. This is due to having a similar total number of blocks mined by each subgraph in most cases with few rare cases where the difference is larger. As we can see, the total number of blocks (including uncles) mined during the experiment by the attacker is way larger than the difference in blocks Δ mined by the two subgraphs. This explains the success of the Balance attack as was observed in Section VI-A.

C. The role of uncle blocks in Ethereum

In the previous experiment, we focused on the total number of blocks without differentiating the blocks that are adopted in the main branch and the uncle blocks that are only part of the local blockchain views. The GHOST protocol accounts for these uncle blocks to decide the current state of the blockchain as we explained previously in Section II.

Figure 9 indicates the number of uncle blocks in comparison to the blocks accepted on the current state of the blockchain for subgraphs G_1 and G_2, and the attacker (referred to as 'Malicious'). As expected, we can observe that the malicious node does not produce any uncle block because he mines the block in isolation of the rest of the network, successfully appending each mined block consecutively to the latest block of its current blockchain view. We note several uncle blocks in the subgraphs, as correct miners may mine blocks concurrently at the same indices.

Figure 10 depicts the creation of the number of mined blocks (excluding uncle blocks) over time for subgraphs G_1 and G_2, and the attacker (referred to as 'Malicious'). As we can see the difference between the number of blocks mined on the subgraphs is significantly smaller than the number of blocks mined by the attacker. This explains why the Balance attack was observed in this setting.

D. Relating connectivity to known blocks

Figure 11 illustrates the execution of two subgraphs resolving connectivity issues and adopting a chain. This experiment outlines one of the fundamental aspects of the balance attack, in which the chosen subgraph resolves the network delay and attempts reconnection with another subgraph. At this point, the subgraphs will initiate the consensus protocol and select

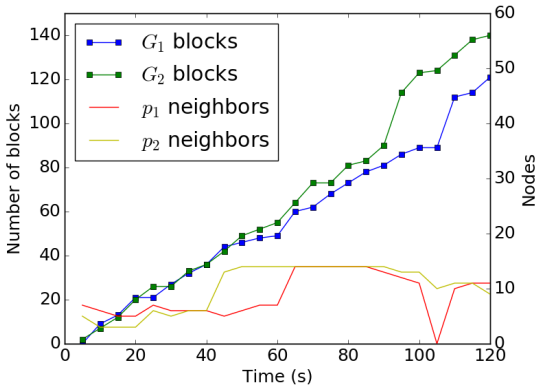


Fig. 11: Execution where the attacker in G_1 delays the communication between G_1 and G_2 for one minute

the branch to adopt as the main branch. The experiment was set up with two subgraphs G_1 and G_2 where $|V_1| = |V_2| = 7$. The attacker selects a subgraph and delays messages between this subgraph and another, enforcing an isolated mining environment. Once the delay is set, the attacker joins one of the subgraphs and begins to mine onto the current chain. The attacker then delays the messages until there is a sufficient amount of blocks mined onto the isolated blockchain for it to be adopted as the correct chain by the other subgraph. In this experiment, at $t = 60\,s$, the delay between subgraphs is resolved, and the subgraphs maintain a connection. Upon reconnection, the subgraphs invoke the consensus protocol to select and adopt the correct chain. In this case, using the GHOST protocol, the heaviest chain is selected for both subgraphs, meaning the chain mined by G_1 is chosen, to which the attacker contributed.

This result reveals that the adoption of a chosen blockchain is plausible, given that the attacker is able to sufficiently delay messages between subgraphs.

VII. Application to Nakamoto's Consensus Protocol

Although the GHOST protocol was shown to be less vulnerable to message delays than Nakamoto's consensus protocol [29], it is interesting to note that our analysis can be extended to Nakamoto's consensus protocol. As described in Section II, Nakamoto's consensus protocol differs from the GHOST protocol in the way a node chooses the current state of the blockchain in case of forks. We present below an intuition of the proof that the Bitcoin is vulnerable to the Balance attack.

As noted previously [29], [27] Nakamoto's protocol suffers from delays for the following reasons. Let us assume that p pools of miners mine p concurrent blocks at the same time in Bitcoin. Assuming that all these mining pools share the same view of the blockchain with only a genesis block when this occurs, then all mining pools update their local blockchain view with a new block at index 1 that differs from one pool to another. Finally, all miners exchange their blockchain view and selects one of these views as the current state of the blockchain. Consider that the process repeats for the f^{th} time, where miners mine concurrently, now at index f, and exchange the blockchain view. At each iteration of the process, the chain depth increases by 1 while the number of blocks mined effectively by the correct miners is p leading to a final blockchain of depth f while the number of mined blocks is fp. Intuitively, this means that for an external attacker to be able to make the system discard a particular chain, the attacker simply needs to have slightly more than a p^{th} of the total mining power or the other miners to have a chance to mine a longer chain than the other miners.

Theorem 5. *A blockchain system that selects a main branch based on Nakamoto's protocol (Alg. 2) is block oblivious.*

To show that the same result holds for Bitcoin, we need to slightly change the Balance attack. While in Ethereum it was sufficient for the attacker to mine on any branch of the blockchain view of G_j after the block b_2 (Alg. 5, line 15), in Bitcoin the attacker has to mine at the top of the blockchain view of G_j. By doing so, the attacker increases the length of the Nakamoto's main branch in graph G_j. Considering that each correct miner mines at the top of the longest branch of their subgroup with the same probability π, the mean of the number of blocks added to the main chain will become $\mu_c^{bitcoin} = \frac{(1-\rho)t\tau}{2d\pi}$. We can then define two binomial random variables X_i' and X_j' for the expected number of blocks in the main branch of G_i and G_j, respectively, and apply the reasoning of the proof of Lemma 3.

VIII. Related Work

Traditional attacks against Bitcoin consist of waiting for some external action, like shipping goods, in response to a transaction before discarding the transaction from the main branch. As the transaction is revoked, the issuer of the transaction can reuse the coins of the transaction in another transaction. As the side effects of the external action cannot be revoked, the second transaction appears as a "double spending".

Perhaps the most basic form of such an attack assumes that an application takes an external action as soon as a transaction is included in a block [12], [18], [2]. The first attack of this kind is called Finney's attack and consists of solo-mining a block with a transaction that sends coins to itself without broadcasting it before issuing a transaction that double-spends the same coin to a merchant. When the goods are delivered in exchange of the coins, the attacker broadcasts its block to override the payment of the merchant. The vector76 attack [30] consists of an attacker solo-mining after block b_0 a new block b_1 containing a transaction to a merchant to purchase goods. Once another block b_1' is mined after b_0, the attacker quickly sends b_1 to the merchant for an external action to be taken. If b_1' is accepted by the system, the attacker can issue another transaction with the coins spent in the discarded block b_1.

The attacks become harder if the external action is taken after the transaction is committed by the blockchain. Rosenfeld's

attack [28] consists of issuing a transaction to a merchant. The attacker then starts solo-mining a longer branch while waiting for m blocks to be appended so that the merchant takes an external action in response to the commit. The attack success probability depends on the number m of blocks the merchant waits before taking an external action and the attacker mining power. However, when the attacker has more mining power than the rest of the system, the attack, also called *majority hashrate attack* or *51-percent attack*, is guaranteed successful, regardless of the value m. To make the attack successful when the attacker owns only a quarter of the mining power, the attacker can incentivize other miners to form a coalition [11] until the coalition owns more than half of the total mining power.

Without a quarter of the mining power, discarding a committed transaction in Bitcoin requires additional power, like the control over the network. It is well known that delaying network messages can impact Bitcoin [9], [27], [29], [15], [25]. Decker and Wattenhoffer already observed that Bitcoin suffered from block propagation delays [9]. Godel et al. [15] analyzed the effect of propagation delays on Bitcoin using a Markov process. Garay et al. [14] investigated Bitcoin in the synchronous communication setting, however, this setting is often considered too restrictive [5]. Pass et al. extended the analysis for when the bound on message delivery is unknown and showed in their model that the difficulty of Bitcoin's crypto-difficulty has to be adapted depending on the bound on the communication delays [27]. This series of work reveal an important limitation of Bitcoin: delaying propagation of blocks can waste the computational effort of correct nodes by letting them mine blocks unnecessarily at the same index of the chain. In this case, the attacker does not need more mining power than the correct miners, but simply needs to expand its local blockchain faster than the growth of the longest branch of the correct blockchain.

Ethereum proposed the GHOST protocol to cope with this issue [29]. The idea is simply to account for the blocks proposed by correct miners in the multiple branches of the correct blockchain to select the main branch. As a result, growing a branch the fastest is not sufficient for an attacker of Ethereum to be able to double spend. Even though the propagation strategy of Ethereum differs from the pull strategy of Bitcoin, some network attacks against Bitcoin could affect Ethereum. In the Eclipse attack [17] the attacker forces the victim to connect to 8 of its malicious identities. The Ethereum adaptation would require to forge $3\times$ more identities and force as many connections as the default number of clients is 25. Apostolaki et al. [1] proposed a BGP hijacking attack and showed that the number of Internet prefixes that need to be hijacked for the attack to succeed depends on the distribution of the mining power. BGP-hijacking typically requires the control of network operators but is independent from Bitcoin and could potentially be exploited to delay network messages and execute a Balance attack in Ethereum.

The R3 consortium has been experimenting Ethereum since more than half a year now and our discussion with the R3 consortium indicated that they did not investigate the dependability of the GHOST consensus protocol and that they also worked with Ripple, Axoni, Symbiont. Some work already evoked the danger of using proof-of-work techniques in a consortium context [16]. In particular, experiments demontrated the impossibility of ordering even committed transactions in an Ethereum private chain without exploring the impact of the network delay [24]. As a private blockchain involves typically a known and smaller number of participants than a public blockchain, it is also well-known [8], [31] that many Byzantine Fault Tolerance (BFT) solutions [7], [26], [20], [6] could be used instead. At the time of writing, R3 has just released Corda [4] as a proposed solution for private chains. Corda does not yet recommend a particular consensus protocol but mentions BFT and favors modularity by allowing to plug any consensus protocol instead [4]. Our work confirms that proof-of-work, besides being unnecessary for consortium private chain when the set of participants is known, is not recommended especially for dependability reasons.

IX. Conclusion

In this paper, we show how main proof-of-work blockchain protocols can be badly suited for consortium blockchains. To this end, we propose the Balance attack a new attack that combines mining power with communication delay to affect prominent proof-of-work blockchain protocols like Ethereum and Bitcoin. This attack simply consists of convincing correct nodes to disregard particular proposed series of blocks to lead to a double spending. We analyzed the tradeoff inherent to Ethereum between communication delay and mining power, hence complementing previous observations made on Bitcoin.

There are several ways to extend this work. First, the context is highly dependent on medium-scale settings where statistics about all participants can be easily collected. It would be interesting to extend these results when the mining power of participants is unknown. Second, the success of the Balance attack despite a low mining power requires communication delay between communication subgraphs. The next step is to compare denial-of-service and man-in-the-middle attacks and evaluate their effectiveness in introducing this delay.

Acknowledgements.

We are grateful to the R3 consortium for sharing information regarding their Ethereum testbed and to Seth Gilbert and Tim Swanson for comments on an earlier version of this paper.

References

[1] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Large-scale network attacks on cryptocurrencies," arXiv, Tech. Rep. 1605.07524, 2016.

[2] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten, "Have a snack, pay with bitcoins," in *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013, Trento, Italy, September 9-11, 2013, Proceedings*, 2013, pp. 1–5.

[3] A. Black, "Hashcash - a denial of service counter-measure," Cypherspace, Tech. Rep., 2002. [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf

[4] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda: An introduction," 2016.

[5] C. Cachin, "Distributing trust on the internet," in *Proceedings of the International Conference on Dependable Systems and Networks (DSN)*, 2001, pp. 183–192.
[6] C. Cachin, S. Schubert, , and M. Vukolic, "Non-determinism in byzantine fault-tolerant replication," in *Proceedings of the 20th International Conference on Principles of Distributed Systems (OPODIS)*, 2016.
[7] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, 2002.
[8] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, and R. Wattenhofer, "On scaling decentralized blockchains," in *3rd Workshop on Bitcoin Research (BITCOIN), Barbados*, February 2016.
[9] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Proc. of the IEEE International Conference on Peer-to-Peer Computing*, 2013.
[10] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2016.
[11] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Proceedings of the 18th Int'l Conference Financial Cryptography and Data Security (FC)*, 2014, pp. 436–454.
[12] H. Finney, "Finney's attack," February 2011. [Online]. Available: https://bitcointalk.org/index.php?topic=3441.msg48384#msg48384
[13] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of distributed consensus with one faulty process," *J. ACM*, vol. 32, no. 2, pp. 374–382, Apr. 1985.
[14] J. A. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *34th Annual Int'l Conf. on the Theory and Applications of Crypto. Techniques*, 2015, pp. 281–310.
[15] J. Göbel, H. Keeler, A. Krzesinski, and P. Taylor, "Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," *Performance Evaluation*, Juy 2016.
[16] V. Gramoli, "On the danger of private blockchains," in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16)*, 2016.
[17] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *24th USENIX Security Symposium*, 2015, pp. 129–144.
[18] G. Karame, E. Androulaki, and S. Capkun, "Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin," *IACR Cryptology ePrint Archive*, vol. 2012, p. 248, 2012.
[19] P. Litke and J. Stewart, "BGP hijacking for cryptocurrency profit," August 2014. [Online]. Available: https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit
[20] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 17–30.
[21] Miller, Litton, Pachulski, Gupta, Levin, Spring, and Bhattacharjee, "Discovering Bitcoin's network topology and influential nodes," University of Marylan, Tech. Rep., 2015.
[22] R. Motwani and P. Raghavan, *Randomized Algorithms*. Cambridge University Press, 1995.
[23] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008, http://www.bitcoin.org.
[24] C. Natoli and V. Gramoli, "The blockchain anomaly," in *Proceedings of the 15th IEEE International Symposium on Network Computing and Applications (NCA'16)*, Oct 2016.
[25] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *IEEE European Symposium on Security and Privacy, EuroS&P 2016, Saarbrücken, Germany, March 21-24, 2016*, 2016, pp. 305–320.
[26] R. Padilha and F. Pedone, "Scalable byzantine fault-tolerant storage," in *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W 2011), Hong Kong, China, June 27-30, 2011.*, 2011, pp. 171–175.
[27] R. Pass, L. Seeman, and A. Shelat, "Analysis of the blockchain protocol in asynchronous networks," Crytology ePrint Archive, Tech. Rep. 454, 2016.
[28] M. Rosenfeld, "Analysis of hashrate-based double-spending," 2012.
[29] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers*, 2015, pp. 507–527.
[30] vector76, "The vector76 attack," August 2011. [Online]. Available: https://bitcointalk.org/index.php?topic=36788.msg463391#msg463391
[31] M. Vukolíc, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proceedings of the IFIP WG 11.4 Workshop on Open Research Problems in Network Security (iNetSec 2015)*, 2015, pp. 112–125.
[32] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," 2015, yellow paper.

APPENDIX

A. Analysis for the general case

As we show below, if the attacker can delay communications for long enough between k subgraphs of the communication graph where $k \geq 2$ then the attacker does not need a large portion ρ of the mining power for the blockchain system to be block oblivious. We consider an attacker that can delay messages of the communication graph G between k subgraphs $G_1, ..., G_k$, each graph owning the same portion $\frac{1-\rho}{k}$ of the total mining power.

Similarly to Section IV, we consider that for $0 < i \leq k$, each of the subgraph G_i mine blocks during delay τ. During that time, each G_i performs a series of $n = \frac{1-\rho}{k} t\tau$ independent and identically distributed Bernoulli trials that returns one in case of success with probability $p = \frac{1}{d}$ and 0 otherwise. Let the sum of these outcomes be the random variable X_i $(0 < i \leq k)$ with a binomial distribution and mean:

$$\mu_c = np = \frac{(1-\rho)t\tau}{kd}. \tag{4}$$

Similarly, the mean of the number of blocks mined by the malicious miner during time τ is

$$\mu_m = \frac{\rho t\tau}{d}. \tag{5}$$

We are interested in measuring the probability that an attacker can select a candidate blockchain among the existing ones and make it adopted by the system. Note that this is easier than rewriting the history with the attacker personal blocks but is sufficient to double spend by simply making sure the initial transaction that spend the coins is only part of blockchains candidate that will be discarded.

The attack relies on minimizing the difference in mined blocks between any pair of communication subgraphs. Hence, let us denote Δ the difference of the number of blocks mined on any two subgraphs:

$$\Delta = \max_{\forall 0<i,j\leq k} (|X_i - X_j|).$$

To this end, we bound the difference between the number of blocks mined in two subgraphs so that the attacker can mine more than the difference.

Fact 6 (Bernoulli's inequality). $1 + nt \leq (1+t)^n$ *for* $n \geq 1$ *and* $t \geq -1$.

Theorem 7. *An attacker decomposing the communication graph into k subgraphs upper-bounds their difference Δ in mined blocks by $2\delta\mu_c$ with probability* $\Pr[\Delta < 2\delta\mu_c] > 1 - 2ke^{-\frac{\delta^2}{3}\mu_c}$ *where* $\delta > 0$.

Proof: This difference is less than $2\delta\mu_c$ with probability larger than the probability that all random variables are within a $\pm\delta$ multiplying factor from the mean, we have:

$$\Pr[\Delta < 2\delta\mu_c] \geq \Pi_{i=1}^{k} \Pr\left[|X_i - \mu_c| < \delta\mu_c\right]. \quad (6)$$

The probability that the numbers of blocks mined by each subgraph are within a $\pm\delta$ factor from their mean, is bound for $0 < \delta < 1$ and $0 < i \leq k$ by Chernoff bounds [22]:

$$\begin{cases} \Pr\left[X_i \geq (1+\delta)\mu_c\right] & \leq e^{-\frac{\delta^2}{3}\mu_c}, \\ \Pr\left[X_i \leq (1-\delta)\mu_c\right] & \leq e^{-\frac{\delta^2}{2}\mu_c}. \end{cases}$$

Thus, we have

$$\begin{aligned} \Pr[|X_i - \mu_c| \geq \delta\mu_c] &\leq 2e^{-\frac{\delta^2}{3}\mu_c}, \\ \Pr[|X_i - \mu_c| < \delta\mu_c] &> 1 - 2e^{-\frac{\delta^2}{3}\mu_c}. \end{aligned}$$

and with Eq. 6 we obtain:

$$\Pr[\Delta < 2\delta\mu_c] > \left(1 - 2e^{-\frac{\delta^2}{3}\mu_c}\right)^k. \quad (7)$$

As $\mu_c \geq 0$, we have that:

$$\begin{aligned} -\frac{\delta^2}{3}\mu_c &\leq 0 \\ -e^{\frac{-\delta^2}{3}\mu_c} &\geq -1 \end{aligned}$$

and as $k \geq 1$ we can apply the Bernoulli inequality to Eq. 7.

Hence, Eq. 7 becomes:

$$\Pr[\Delta < 2\delta\mu_c] > 1 - 2ke^{-\frac{\delta^2}{3}\mu_c}. \quad (8)$$

■

The next theorem bounds the number of blocks the attacker needs to mine to force the system to adopt the candidate blockchain of its choice.

Theorem 8. *If the attacker delays the links of E_0 while the miners on each of the k subgraphs mine for*

$$\tau \geq \frac{3kd\log(\frac{2k}{\varepsilon})}{\delta^2(1-\rho)t}$$

seconds, then with probability $1-\varepsilon$ the difference between the number of blocks mined on the two subgraphs is lower than $\frac{2\delta(1-\rho)t\tau}{kd}$.

Proof: The proof relies on upper bounding $2ke^{-\frac{\delta^2}{3}\mu_c}$ by ε:

$$\begin{aligned} 2ke^{-\frac{\delta^2}{3}\mu_c} &\leq \varepsilon, \\ \mu_c &\geq \frac{3\log(\frac{2k}{\varepsilon})}{\delta^2}. \end{aligned}$$

By replacing μ_c by the expression of Eq. 4, we obtain:

$$\tau \geq \frac{3kd\log(\frac{2k}{\varepsilon})}{\delta^2(1-\rho)t}.$$

■

Let us now bound the probability that the number of blocks mined on k subgraphs is always lower than the expectation of the number of blocks mined by the malicious node.

Theorem 9. *If $\delta = \frac{\mu_m - 1}{2\mu_c}$ then*

$$\Pr[\Delta < \mu_m] > 1 - 2ke^{-\frac{(\mu_m-1)^2}{12\mu_c}}.$$

Proof: The proof follows from replacing δ by $\frac{\mu_m-1}{2\mu_c}$ in Eq. 8. ■