Analysis of Nakamoto Consensus, Revisited

Jianyu Niu*, Chen Feng*, Hoang Dau†, Yu-Chih Huang‡, Jingge Zhu§

*The University of British Columbia (Okanagan Campus)

†RMIT University ‡National Taipei University

§The University of Melbourne

I. INTRODUCTION

In the Bitcoin white paper [1], Nakamoto proposed a very simple Byzantine fault tolerant consensus algorithm that is also known as Nakamoto consensus. Despite its simplicity, some existing analysis of Nakamoto consensus appears to be long and involved. In this technical report, we aim to make such analysis simple and transparent so that we can teach senior undergraduate students and graduate students in our institutions. This report is largely based on a 3-hour tutorial given by one of the authors in June 2019 [2].

II. SYSTEM MODEL

We closely follow the notations in [3]. Let $\mathcal{N}$ denote the set of participating nodes in the network. Each node $n \in \mathcal{N}$ has p_n fraction of total hashing power so that it mines new blocks at a rate of $p_n f$ blocks per second, where f is the total mining rate.[1] There are two types of nodes: honest nodes who strictly follow the protocol and adversarial nodes who may deviate from the protocol. The set of honest nodes (resp., adversarial nodes) is denoted by $\mathcal{H}$ (resp., $\mathcal{Z}$). The adversarial nodes control β fraction of total hashing power, i.e., $\sum_{n\in\mathcal{Z}} p_n = \beta$. The honest nodes control $1-\beta$ fraction of total hashing power, i.e., $\sum_{n\in\mathcal{H}} p_n = 1-\beta$. If a block is mined by an honest node (resp., adversarial node), we call it an honest block (resp., adversarial block). A block's height is its parent block's height plus one. (The height of the genesis block is set to 0.)

Mining at each node $n \in \mathcal{N}$ is modeled by a Poisson process with rate $p_n f$ as done in the Bitcoin white paper. Hence, the aggregated mining process of the honest nodes (resp., adversarial nodes) is a Poisson process with rate $(1-\beta)f$ (resp., βf). Without loss of generality, we can assume a *single* adversarial node with β fraction of hashing power, and we call this node the adversary.

We assume a bounded network delay of Δ seconds for honest nodes. That is, whenever an honest node mines a new block, it takes up to Δ seconds for the block to reach all other honest nodes. We assume a zero delay from honest nodes to the adversary. That is, whenever an honest node mines a new block, the adversary receives it immediately. These assumptions make the adversary even more powerful in terms of network communication.

Next, we discretize the above continuous-time model into a discrete-time model in a way that generalizes the discretization procedure in [3]. We divide Δ seconds into τ rounds so that each round in our model corresponds

[1] We assume constant mining difficulty here.

TABLE I

KEY NOTATIONS IN THE SYSTEM MODEL

Δ	Upper bound on the network communication delay (in seconds)
f	Total mining rate (in blocks per second)
β	Fraction of adversarial mining rate
$H[r]$	Number of honest blocks mined in round r
$Z[r]$	Number of adversarial blocks mined in round r

to $\frac{\Delta}{\tau}$ seconds. More specifically, round 0 corresponds to the time interval $[0, \frac{\Delta}{\tau})$, and round r corresponds to the interval $[r\frac{\Delta}{\tau}, (r+1)\frac{\Delta}{\tau})$. When $\tau = 1$, our model reduces to the discrete-time model in [3]. On the other hand, when $\tau \to \infty$, our model approaches the continuous-time model in [4]. In this sense, our model provides a unified treatment.

Following [3], [5], [6], we assume that blocks can only be mined at the beginning of each round. That is, if new blocks are mined in round r with the interval $[r\frac{\Delta}{\tau}, (r+1)\frac{\Delta}{\tau})$, we will set their generation time to be the beginning of round r (i.e., $r\frac{\Delta}{\tau}$). Note that such an approximation tends to be accurate as $\tau \to \infty$. Let $H[r]$ and $Z[r]$ be the number of blocks mined by the honest nodes and by the adversary, respectively, in round r. Clearly, $H[r]$ and $Z[r]$ are independent Poisson random variables with means $(1-\beta)f\frac{\Delta}{\tau}$ and $\beta f\frac{\Delta}{\tau}$, respectively. In addition, the sequences $\{H[0], H[1], \ldots\}$ and $\{Z[0], Z[1], \ldots\}$ are independent of each other and independent across rounds. Note that the $H[r]$ honest blocks mined at the beginning of round r will reach all the honest nodes in the network by the end of round $r + \tau - 1$, since it takes τ rounds to broadcast any honest block. On the other hand, the $Z[r]$ adversarial blocks can be kept in private until the adversary decides to transmit any of them in later rounds. Once transmitted, any adversarial block will reach all the honest nodes within τ rounds.[2]

Under the above system model, Nakamoto consensus can be described as follows.

- At each round r, an honest node attempts to mine new blocks on top of the longest chain it observes by the end of round $r - 1$ (where ties can be broken arbitrarily). This is often referred to as the longest chain rule.
- At each round r, an honest node confirms a block if the longest chain it adopts contains the block as well as at least k other blocks of larger heights. This is sometimes referred to as the k-deep confirmation rule.

Next, let us make an observation that will be used in our analysis later.

Lemma 1: If an honest block of height ℓ is mined at the beginning of round r, then every honest node observes a chain of length at least ℓ by the end of round $r + \tau - 1$.

Proof: First, this honest block will reach all the honest nodes by the end of round $r + \tau - 1$ as we discussed before. Second, its parent block (no matter honest or adversarial) will reach all the honest nodes by the end of round $r + \tau - 1$. This argument applies to all of its ancestor blocks. Hence, by the end of round $r + \tau - 1$, every honest node will observe a chain consisting of this block, its ancestor blocks, as well as new (honest or adversarial)

[2]In some implementation of Bitcoin, certain blocks of small heights may be discarded by honest nodes so that these blocks won't be broadcasted to the entire network. In our system model, we assume that any block will be broadcasted unless it is kept in private.

blocks mined on top of this block. If there are no such new blocks, the chain length is ℓ. Otherwise, the chain length is greater than ℓ. ■

III. Effective Rounds and Liveness

A round r is called an effective round (ER) if there is some honest block mined in round r and there is no honest block mined in the previous $\tau - 1$ rounds. By effective, we mean two things: 1) at least one honest block is successfully mined in round r and 2) the longest chain (among all the honest nodes) will be increased. When $\tau = 1$, a round r is an ER if and only if $H[r] \geq 1$. When $\tau > 1$, a round r is an ER if and only if $H[r] \geq 1$ and $H[r'] = 0$ for all $r' \in \{r - (\tau - 1), \ldots, r - 1\}$. For convenience, we assume that $H[r'] = 0$ for all $r' < 0$.

Lemma 2: Honest blocks mined in distinct ERs have different heights.

Proof: Suppose for contradiction that two honest blocks B and B' of height ℓ are mined in round r and r' respectively. Without loss of generality, assume that $r < r'$. We have $r' \geq r + \tau$, because otherwise r' cannot be an ER. By Lemma 1, every honest node observes a chain of length at least ℓ by the end of round $r' - 1$ (or even earlier). Therefore, no honest node will mine a new block B' of height ℓ in round r'. ■

Next, we introduce an indicator random variable $X[r]$ for whether round r is an ER, i.e., $X[r] = 1$ when round r is an ER and $X[r] = 0$ otherwise. Note that $\Pr(X[r] = 1) \geq e^{-(1-\beta)f\frac{\Delta}{\tau}(\tau-1)}\left(1 - e^{-(1-\beta)f\frac{\Delta}{\tau}}\right)$, where the equality holds when $r \geq \tau$. For convenience, we write $X[r, r'] \triangleq X[r] + X[r+1] + \cdots + X[r']$. This notation applies to other random variables as well, such as $\{H[r]\}$ and $\{Z[r]\}$.

Lemma 3: Let $\gamma = e^{-(1-\beta)f\frac{\Delta}{\tau}(\tau-1)}\left(1 - e^{-(1-\beta)f\frac{\Delta}{\tau}}\right)$. In a time interval of s consecutive rounds, the expected number of ERs is at least γs.

Proof: The number of ERs in a time interval of s consecutive rounds starting from round r is given by $X[r, r+s-1]$. Hence, we have

$$E\left(X[r, r+s-1]\right) = E\left(X[r]\right) + \cdots + E\left(X[r+s-1]\right) \geq \gamma s, \tag{1}$$

where the equality holds when $r \geq \tau$. ■

Lemma 4: For any positive integer m, in a time interval of τm consecutive rounds starting from round r, the number of ERs has the following Chernoff-type bound: For $0 < \delta < 1$,

$$\Pr(X[r, r+\tau m-1] \leq (1-\delta)\gamma\tau m) \leq e^{-\Omega\left(\delta^2\gamma m\right)}. \tag{2}$$

Proof: Let $X^{(j)} = \sum_{i=0}^{m-1} X[r+j+i\tau]$. Then, $X[r, r+\tau m-1] = X^{(0)} + \cdots + X^{(\tau-1)}$. Our key observation is that $\{X[r+j], X[r+j+\tau], \ldots, X[r+j+(m-1)\tau]\}$ are independent random variables, because $X[r]$ is a function of $\{H[r-(\tau-1)], \ldots, H[r]\}$. By (a slightly modified version of) Lemma 3, we have $E\left(X^{(j)}\right) \geq \gamma m$. By Lemma 10, we have $\Pr\left(X[r, r+\tau m-1] \leq (1-\delta)\gamma\tau m\right) \leq e^{-\Omega\left(\delta^2\gamma m\right)}$. ■

Theorem 1 (Chain growth): If an honest node observes a chain of length ℓ at the beginning of round r, then at the beginning of round $r + \tau(m+2) - 1$, every honest node observes a chain of length at least $\ell + (1-\delta)\gamma\tau m$, except for $e^{-\Omega\left(\delta^2\gamma m\right)}$ probability.

Proof: First, by Lemma 1, every honest node observes a chain of length at least ℓ at the beginning of round $r + \tau$. Next, consider a time interval of τm consecutive rounds starting from round $r + \tau$. By Lemma 4, we have at least $(1-\delta)\gamma\tau m$ ERs from round $r+\tau$ to round $r+\tau+\tau m-1$, except for $e^{-\Omega\left(\delta^2\gamma m\right)}$ probability. We take one honest block from each ER. By Lemma 2, these honest blocks have different heights, all greater than ℓ. In particular, the largest height of these blocks is at least $\ell+(1-\delta)\gamma\tau m$. By Lemma 1, at the beginning of round $r+2\tau+\tau m-1$, every honest node observes a chain of length at least $\ell+(1-\delta)\gamma\tau m$. ∎

Theorem 2 (Chain quality): Suppose $\gamma > (1+\delta)\beta f\frac{\Delta}{\tau}$. In a time interval of τm consecutive rounds starting from round 0, in the longest chain among honest nodes, the fraction of honest blocks is at least $1-(1+\delta)\frac{\beta f\frac{\Delta}{\tau}}{\gamma}$ except for $e^{-\Omega\left(\delta^2\min\{\beta f\Delta,\gamma\}m\right)}$ probability.

Proof: We let $s=\tau m$ for convenience. On the one hand, $Z[0,s-1]$ is the number of adversarial blocks from round 0 to round $s-1$, which is a Poisson random variable with mean $\beta f\frac{\Delta}{\tau}s$. By Lemma 11, $Z[0,s-1] < (1+\delta_Z)\beta f\frac{\Delta}{\tau}s$ except for $e^{-\Omega\left(\delta^2\beta f\Delta m\right)}$ probability. On the other hand, $X[0,s-1]$ is the number of ERs from round 0 to round $s-1$. By Lemma 4, $X[0,s-1] > (1-\delta_X)\gamma s$ except for $e^{-\Omega\left(\delta_X^2\gamma m\right)}$ probability. Hence, by the end of round $s-1$, some honest node observes an honest block of height at least $(1-\delta_X)\gamma s$. In other words, by the end of round $s-1$, the length of the longest chain among honest nodes, denoted by $L(s)$, is at least $(1-\delta_X)\gamma s$. The honest fraction is smallest if all the adversarial blocks belong to the longest chain of length $L(s)$. That is, the honest fraction is at least $\frac{L(s)-Z[0,s-1]}{L(s)}$, which is lower bounded by $\frac{X[0,s-1]-Z[0,s-1]}{X[0,s-1]}$. Finally, by setting $\delta_Z=\delta_X=\delta/4$ and noticing $\frac{1+\delta/4}{1-\delta/4} < 1+\delta$, we have

$$\frac{X[0,s-1]-Z[0,s-1]}{X[0,s-1]} > 1-\frac{1+\delta_Z}{1-\delta_X}\frac{\beta f\frac{\Delta}{\tau}s}{\gamma s} > 1-(1+\delta)\frac{\beta f\frac{\Delta}{\tau}}{\gamma}, \tag{3}$$

except for $e^{-\Omega\left(\delta^2\min\{\beta f\Delta,\gamma\}m\right)}$ probability. ∎

Finally, we would like to point out that chain growth and chain quality—when putting together—imply *livenss*, which states that every valid transaction will be eventually confirmed by honest nodes with high probability.

IV. Uniquely Effective Rounds and Safety

A round r is called a uniquely effective round (UER) if there is exactly one honest block mined in round r, and there is no honest block mined in the previous and next $\tau-1$ rounds. By uniquely effective, we mean two things: 1) a unique honest block is successfully mined in round r and 2) the honest block has a unique height among all other honest blocks, as stated in Lemma 5. When $\tau=1$, a round r is a UER if and only if $H[r]=1$. When $\tau>1$, a round r is a UER if and only if $H[r]=1$ and $H[r']=0$ for all $r'\in\{r-(\tau-1),\dots,r-1,r+1,\dots,r+(\tau-1)\}$.

Lemma 5: Suppose that an honest block B of height ℓ is mined in a UER. Then B is the only honest block of height ℓ.

Proof: Suppose for contradiction that two honest blocks B and B' of height ℓ are mined in round r and r' respectively. Since round r is a UER, we have $r'\geq r+\tau$ or $r'\leq r-\tau$. If $r'\geq r+\tau$, by Lemma 1, every honest node observes a chain of length at least ℓ by the end of round $r'-1$ (or even earlier). Therefore, no honest node will mine a new block of height ℓ in round r', leading to a contradiction. Similarly, if $r'\leq r-\tau$, every honest node observes a chain of length at least ℓ by the end of round $r-1$ (or even earlier), leading to a contradiction. ∎

Next, we introduce an indicator random variable $Y[r]$ for whether round r is a UER, i.e., $Y[r]=1$ when round r is a UER and $Y[r]=0$ otherwise. Note that $\Pr(Y[r]=1) \geq (1-\beta)f\frac{\Delta}{\tau}e^{-(1-\beta)f\frac{\Delta}{\tau}(2\tau-1)}$, where the equality holds when $r \geq \tau$.

Lemma 6: Let $\eta=(1-\beta)f\frac{\Delta}{\tau}e^{-(1-\beta)f\frac{\Delta}{\tau}(2\tau-1)}$. In a time interval of s consecutive rounds, the expected number of UERs is at least ηs.

Proof: The number of UERs in a time interval of s consecutive rounds starting from round r is given by $Y[r,r+s-1]$. Hence, we have

$$E\left(Y[r,r+s-1]\right)=E\left(Y[r]\right)+\cdots+E\left(Y[r+s-1]\right) \geq \eta s, \tag{4}$$

where the equality holds when $r \geq \tau$. ■

Lemma 7: For any positive integer m, in a time interval of $(2\tau-1)m$ consecutive rounds starting from round r, the number of UERs has the following Chernoff-type bound: For $0<\delta<1$,

$$\Pr(Y[r,r+(2\tau-1)m-1] \leq (1-\delta)\eta(2\tau-1)m) \leq e^{-\Omega\left(\delta^2\eta m\right)}. \tag{5}$$

Proof: Let $Y^{(j)}=\sum_{i=0}^{m-1}Y[r+j+i(2\tau-1)]$. Then, $Y[r,r+(2\tau-1)m-1]=Y^{(0)}+\cdots+Y^{(2\tau-2)}$. Our key observation is that $\{Y[r+j],Y[r+j+(2\tau-1)],\ldots,Y[r+j+(m-1)(2\tau-1)]\}$ are independent random variables. By (a slightly modified version of) Lemma 6, we have $E\left(Y^{(j)}\right) \geq \eta m$. By Lemma 10, we have $\Pr\left(Y[r,r+(2\tau-1)m-1] \leq (1-\delta)\eta(2\tau-1)m\right) \leq e^{-\Omega\left(\delta^2\eta m\right)}$. ■

Lemma 8: Suppose $\eta>(1+\delta)\beta f\frac{\Delta}{\tau}$. In a time interval of $(2\tau-1)m$ consecutive rounds starting from round r, the number of UERs is greater than the number of adversarial blocks except for $e^{-\Omega\left(\delta^2\min\{\eta,\beta f\Delta\}m\right)}$ probability. That is,

$$\Pr\left(Y[r,r+(2\tau-1)m-1] \leq Z[r,r+(2\tau-1)m-1]\right) \leq e^{-\Omega\left(\delta^2\min\{\eta,\beta f\Delta\}m\right)}. \tag{6}$$

Proof: We let $s=(2\tau-1)m$ for convenience. Let $Y=Y[r]+\cdots+Y[r+s-1]$ and $Z=Z[r]+\cdots+Z[r+s-1]$. Then, by Lemma 7, $Y>(1-\delta_Y)\eta s$ except for $e^{-\Omega\left(\delta_Y^2\eta m\right)}$ probability. Similarly, by Lemma 11, $Z<(1+\delta_Z)\beta f\frac{\Delta}{\tau}s$ except for $e^{-\Omega\left(\delta_Z^2\beta f\Delta m\right)}$ probability. By setting $\delta_Y=\delta_Z=\delta/4$ and noticing $\frac{1+\delta/4}{1-\delta/4}<1+\delta$, we have $(1-\delta_Y)\eta>(1+\delta_Z)\beta f\frac{\Delta}{\tau}$. Therefore, $Y>Z$ except for $e^{-\Omega\left(\delta^2\min\{\eta,\beta f\Delta\}m\right)}$ probability. ■

Remark 1: Note that the condition $\eta>(1+\delta)\beta f\frac{\Delta}{\tau}$ is equivalent to $f\frac{\Delta}{\tau}(2\tau-1)<\frac{1}{1-\beta}\ln\left(\frac{1-\beta}{\beta}\frac{1}{1+\delta}\right)$. This implies $\beta<0.5$. When $\tau=1$, the condition says $f\Delta<\frac{1}{1-\beta}\ln\left(\frac{1-\beta}{\beta}\frac{1}{1+\delta}\right)$. When $\tau\to\infty$, the condition says $f\Delta<\frac{1}{2}\frac{1}{1-\beta}\ln\left(\frac{1-\beta}{\beta}\frac{1}{1+\delta}\right)$.

Theorem 3 (Safety): Suppose $\eta>(1+\delta)\beta f\frac{\Delta}{\tau}$. If B and B' are two distinct blocks of the same height, then they cannot be both confirmed, each by an honest node. This property holds, regardless of adversarial action, except for $e^{-\Omega\left(\delta^2\min\{\frac{\eta}{f\Delta},\beta\}k\right)}$ probability.

Proof: Consider the event $\mathcal{E}$ that "B and B' of the same height are both confirmed, each by an honest node." We will show that this event happens with probability at most $e^{-\Omega\left(\delta^2\min\{\frac{\eta}{f\Delta},\beta\}k\right)}$, regardless of adversarial action. Let r (resp., r') be the smallest round at the beginning of which B (resp., B') is confirmed. Without loss of generality, we assume that $r \geq r'$. Let B_1 be the most recent ancestor of B and B'. That is, there are two disjoint subchains mined on top of B_1, one containing B and the other containing B'. Let B_0 be the most recent *honest* ancestor of B and B'. Note that B_0 can be B_1 (if B_1 is honest) or the genesis block. Suppose that B_0 is mined (by some honest node) at the beginning of round r_0. For convenience, we assume that the genesis block is mined at the beginning of round 0. This makes r_0 well defined. We next define the following two events:

- $\mathcal{E}_1(r_0, r)$: At the beginning of round r, there are two disjoint subchains mined on top of B_1, each containing at least $k+1$ blocks mined from round r_0 to round r;
- $\mathcal{E}_2(r_0, r)$: $Y[r_0+\tau, r-\tau] \leq Z[r_0, r]$.

We will show that $\mathcal{E} \subseteq \mathcal{E}_1(r_0, r) \subseteq \mathcal{E}_2(r_0, r)$, regardless of adversarial action.

- $\mathcal{E} \subseteq \mathcal{E}_1(r_0, r)$: At the beginning of round r, one subchain contains B as well as k blocks mined on top of B (due to the k-deep confirmation rule). Similarly, the other subchain contains B' as well as k other blocks on top of B'. These blocks cannot be mined before r_0, because B_0 is an honest block.
- $\mathcal{E}_1(r_0, r) \subseteq \mathcal{E}_2(r_0, r)$: We will show that whenever there is a unique honest block of height ℓ mined in a UER between round $r_0+\tau$ and round $r-\tau$, there must be a "matching" adversarial block of height ℓ mined between round r_0 and round r. To see this, suppose that an honest block B^* is mined in a UER without a matching adversarial block. By Lemma 1, B^* has a larger height than B_0. On the one hand, if B^* has a smaller height than B, then B^* must be an honest ancestor of B and B', because B^* is the only block at its height. This contradicts with the fact that B_0 is the most recent honest ancestor. On the other hand, if B^* has a larger height than B, then both subchains will contain B^* at the beginning of round r. This is because B^*—the only block at its height—will reach all the honest nodes by the end of round $r-1$. As a result, the subchain with B will certainly contain B^* and so the height of B^* is at most the height of B plus k. Similarly, the subchain with B' will contain B^*, since there are at least k blocks on top of B'. This leads to a contradiction.

By (a slightly modified version of) Lemma 8, for any given r_0 and r, we have

$$\Pr(\mathcal{E}_2(r_0, r)) \leq e^{-\Omega\left(\delta^2 \min\{\eta, \beta f \Delta\} \frac{r-r_0+1}{2\tau-1}\right)}. \tag{7}$$

Finally, we will bound $r-r_0$ and complete the proof. We claim that

$$r - r_0 + 1 > \frac{2k+2}{(1+\delta) f \frac{\Delta}{\tau}} \tag{8}$$

except for $e^{-\Omega\left(\delta^2 k\right)}$ probability, regardless of adversarial action. To see this, recall that $\mathcal{E}_1(r_0, r)$ states that two subchains contain at least $2k+2$ blocks. Hence, $r-r_0+1$ is smallest if all the mined blocks from round r_0 to round r (the number of which is $H[r_0, r] + Z[r_0, r]$) belong to these two subchains. By Lemma 11,

$$\Pr\left(H[r_0, r] + Z[r_0, r] \geq (1+\delta) f \frac{\Delta}{\tau}(r - r_0 + 1)\right) \leq e^{-\delta^2 f \frac{\Delta}{\tau}(r-r_0+1)/3}. \tag{9}$$

So, if we set $r - r_0 + 1 = \frac{2k+2}{(1+\delta) f \frac{\Delta}{\tau}}$, then we have

$$\Pr\left(H[r_0, r] + Z[r_0, r] \geq 2k+2\right) \leq e^{-\delta^2 \frac{(2k+2)}{1+\delta}/3}. \tag{10}$$

This proves our claim.

Define the event $\mathcal{D}$ as $r - r_0 + 1 > \frac{2k+2}{(1+\delta) f \frac{\Delta}{\tau}}$. Then, $\Pr(\mathcal{D}^c) \leq e^{-\Omega\left(\delta^2 k\right)}$, where $\mathcal{D}^c$ is the complement of $\mathcal{D}$. Therefore, for any adversarial action, we have

$$\begin{aligned}
\Pr(\mathcal{E}) &= \Pr(\mathcal{D}^c) \Pr(\mathcal{E}|\mathcal{D}^c) + \Pr(\mathcal{D}) \Pr(\mathcal{E}|\mathcal{D}) && (11)\\
&\leq \Pr(\mathcal{D}^c) + \Pr(\mathcal{D}) \Pr(\mathcal{E}_2(r_0, r)|\mathcal{D}) && (12)\\
&\leq \Pr(\mathcal{D}^c) + \Pr(\mathcal{E}_2(r_0, r)|\mathcal{D}) && (13)\\
&\leq e^{-\Omega\left(\delta^2 \min\{\frac{\eta}{f\Delta}, \beta\} k\right)} && (14)
\end{aligned}$$

where the last inequality follows from $k \geq \min\{\frac{\eta}{f\Delta}, \beta\}k$. ■

Finally, we would like to point out that our safety property stated in Theorem 3 is equivalent to the common-prefix property in the previous analysis, such as [3], [5].

V. Discussion

The analysis of Nakamoto consensus was started by Garay, Kiayias and Leonardos in their landmark work [5], which was later refined by Bagaria et. al. [3] in the context of parallel chains. Both papers only considered the case of $\tau = 1$. The extension to the case of $\tau > 1$ was presented by Pass, Seeman and shelat[3] [6], which was later refined by Kiffer, Rajaraman and shelat [7] as well as Zhao [8] via Markov chain analysis. Our analysis is simpler and more transparent than the previous analysis in that it introduces two events $\mathcal{E}_1(r_0, r)$ and $\mathcal{E}_2(r_0, r)$ explicitly and avoids the use of Markov chains.

At the final stage of completing this report, we notice an independent work by Ling Ren [4], which focuses on a continuous-time model instead of a discrete-time model. His elegant analysis can be viewed as a counterpart of our analysis. For instance, his safety condition $g^2\alpha > (1+\delta)\beta$ is as tight as our safety condition $\eta > (1+\delta)\beta f \frac{\Delta}{\tau}$ as $\tau \to \infty$.[4] We will leave it for future work to carefully compare his analysis with ours.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Chen Feng. Theoretical Foundation of Blockchain Technology. In *16th Canadian Workshop on Information Theory*, June 2019.

[3] Vivek Bagaria, Sreeram Kannan, David Tse, Giulia Fanti, and Pramod Viswanath. Deconstructing the blockchain to approach physical limits. arXiv preprint arXiv:1810.08092 (2018). Accepted by CCS'2019.

[4] Ling Ren. 2019. Analysis of Nakamoto Consensus. Cryptology ePrint Archive, Report 2019/943. (2019). https://eprint.iacr.org/2019/943.

[5] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 281-310. Springer, 2015.

[6] Rafael Pass, Lior Seeman, and abhi shelat. Analysis of the blockchain protocol in asynchronous networks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643-673. Springer, 2017.

[7] Lucianna Kiffer, Rajmohan Rajaraman, and abhi shelat. A better method to analyze blockchain consistency. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 729-744. ACM, 2018.

[8] Jun Zhao. An analysis of blockchain consistency in asynchronous networks: Deriving a neat bound. arXiv preprint arXiv:1909.06587. (2019).

[3]Dr. abhi shelat often writes his name in lower-case and so we follow his style.

[4]We also notice that the safety condition $g\alpha > (1+\delta)(\alpha+\beta)/2$ in his first version is not as tight as ours.

[9] Michael Mitzenmacher and Eli Upfal. Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge University Press, NY, USA, 2015.

APPENDIX

Lemma 9 (Chernoff bounds): Let $X = \sum_{i=1}^{n} X_i$ be the sum of n independent indicator random variables with $E(X_i) = p_i$. Let $\mu = E(X) = \sum_{i=1}^{n} p_i$. Then, for $0 < \delta < 1$, $\Pr(X \geq (1+\delta)\mu) \leq e^{-\delta^2\mu/3}$ and $\Pr(X \leq (1-\delta)\mu) \leq e^{-\delta^2\mu/2}$.

The proof of Lemma 9 is elementary. See, e.g., the proof for Theorem 4.5 in [9].

Lemma 10 (Chernoff bound for a sum of dependent random variables): Let T be a positive integer. Let $X^{(j)} = \sum_{i=0}^{n-1} X_{j+iT}$ be the sum of n independent indicator random variables and $\mu_j = E\left(X^{(j)}\right)$ for $j \in \{1, \ldots, T\}$. Let $X = X^{(1)} + \cdots + X^{(T)}$. Let $\mu = \min_j\{\mu_j\}$. Then, for $0 < \delta < 1$, $\Pr(X \leq (1-\delta)\mu T) \leq e^{-\delta^2\mu/2}$.

Proof: Let $\bar{X} = \frac{X}{T} = \frac{1}{T}\sum_{j=1}^{T} X^{(j)}$. Then, for any $t < 0$, we have

$$\Pr(X \leq (1-\delta)\mu T) = \Pr\left(\bar{X} \leq (1-\delta)\mu\right) \leq \frac{E(e^{t\bar{X}})}{e^{t(1-\delta)\mu}}. \tag{15}$$

Note that $\exp(\cdot)$ is a convex function, we use Jensen's inequality to obtain $E(e^{t\bar{X}}) \leq \frac{1}{T}\sum_{j=1}^{T} E\left(e^{tX^{(j)}}\right)$. Hence,

$$\Pr(X \leq (1-\delta)\mu T) \leq \frac{1}{T}\sum_{j=1}^{T}\frac{E\left(e^{tX^{(j)}}\right)}{e^{t(1-\delta)\mu}} \leq \frac{1}{T}\sum_{j=1}^{T}\frac{E\left(e^{tX^{(j)}}\right)}{e^{t(1-\delta)\mu_j}}, \tag{16}$$

where the last inequality comes from the fact that $\mu_j \geq \mu$ for all j. Setting $t = \ln(1-\delta) < 0$ and following the footsteps in the proof of Theorem 4.5 in [9], we have $\frac{E\left(e^{tX^{(j)}}\right)}{e^{t(1-\delta)\mu_j}} \leq e^{-\delta^2\mu_j/2}$ for all j. Finally, we note that $e^{-\delta^2\mu_j/2} \leq e^{-\delta^2\mu/2}$ for all j and this completes the proof. ■

Lemma 11 (Chernoff bounds for Poisson random variables): Let X be a Poisson random variable with mean μ. Then, for $0 < \delta < 1$, $\Pr(X \geq (1+\delta)\mu) \leq e^{-\delta^2\mu/3}$.

Proof: For any $t > 0$, we have

$$\Pr(X \geq (1+\delta)\mu) = \Pr\left(e^{tX} \geq e^{t(1+\delta)\mu}\right) \leq \frac{E(e^{tX})}{e^{t(1+\delta)\mu}}. \tag{17}$$

Since $E(e^{tX}) = e^{(e^t-1)\mu}$ for a Poisson random varaible, we have

$$\Pr(X \geq (1+\delta)\mu) \leq \frac{e^{(e^t-1)\mu}}{e^{t(1+\delta)\mu}}. \tag{18}$$

Setting $t = \ln(1+\delta) > 0$, we have

$$\Pr(X \geq (1+\delta)\mu) \leq \left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu}. \tag{19}$$

Finally, note that $\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}} \leq e^{-\delta^2/3}$ for $0 < \delta < 1$. This completes the proof. ■