IEEE ICBC'24 1570981543

From Slow Propagation to Partition: Analyzing Bitcoin Over Anonymous Routing

Anonymous Authors

***Abstract*—Cryptocurrency is designed for anonymous financial transactions to avoid centralized control, censorship, and regulations. To protect anonymity in the underlying P2P networking, Bitcoin adopts and supports anonymous routing of Tor, I2P, and CJDNS. We analyze the networking performances of these anonymous routing with the focus on their impacts on the blockchain consensus protocol. Compared to non-anonymous routing, there are inherent-by-design latency performance costs due to the additions of the artificial P2P relays for the anonymous routing. However, we discover that the lack of ecosystem plays an even bigger factor in the performances of the anonymous routing for cryptocurrency blockchain. I2P and CJDNS (both advancing the anonymous routing beyond Tor) in particular lack the ecosystem which results in the Bitcoin experiencing the networking partitioning effects (which has traditionally been studied in the cryptocurrency networking security contexts). We focus on I2P and Tor and compare them with the non-anonymous routing because CJDNS has no active public peers resulting in no connectivity; Tor results in slow propagation while I2P yields soft partition (which is a partition effect long enough to have a substantial impact in the PoW mining). To better study and identify the latency and the ecosystem factors of the cryptocurrency networking and consensus costs, we study the behaviors both in the connection manager (directly involved in the P2P networking) and the address manager (informing the connection manager of the peer selections on the backend). This paper presents our analyses results to inform the state of cryptocurrency blockchain with anonymous routing and includes future work recommendations and discussions to resolve the performance and partition issues.**

***Index Terms*—Cryptocurrency, Bitcoin, P2P Networking, Anonymous Routing, Tor, I2P, CJDNS**

I. Introduction

Cryptocurrency processes financial transactions without relying on a centralized authority and involves multiple nodes for distributed computing and networking. Its popularity and use are significant, for example, Bitcoin, the most widely adopted cryptocurrency, has a market capitalization exceeding USD $500B [1]. Enabled by its distributed operations without the reliance on the centralized authority, cryptocurrency supports anonymity and circumvents censorship and regulation. The cryptocurrency client self-generates and self-signs its public key to construct its account without registration (enabling permissionless operations), and the consensus operation to select the transactions and the block to process involves a set of distributed nodes, e.g., proof-of-work (PoW) consensus protocol for Bitcoin. To protect the cryptocurrency's anonymity and the censorship circumvention, cryptocurrencies utilize anonymous routing in the underlying peer-to-peer (P2P) networking.

The P2P networking is critical for cryptocurrency operations, as the operations rely on the information delivered through the networking. The highly competitive and resource-consuming PoW consensus mining operations in particular heavily rely on networking information delivery. If the blocks and the transactions are not promptly delivered, it reduces the reward incomes of the consensus participants of miners. Furthermore, the distributed P2P networking can cause synchronization failures. While there can be forks and temporary block collisions, there can be more damaging partitioning of the network. The network partition results in a longer discrepancy about the latest block information between the nodes so that the nodes operate on distinct blocks for a longer time. Previous research studied the networking partition as the result of security threats/attacks, and such partitioning can last 10 minutes [2] [3] [4] to an hour [5]. Much of these previous work advanced the Bitcoin security and development got explicitly patched and are no longer feasible in the current Bitcoin practice [6] [7] [8] [9] [10].

We study anonymous routing in the P2P networking for Bitcoin due to Bitcoin's popularity and market dominance. Our analysis study focuses on the networking performances and their impacts on the cryptocurrency consensus operations because poor networking wastes the PoW consensus computing resource and reduces the mining rewards. We discover that the current anonymous routing supported by the Bitcoin implementation can have a range of networking effects, from slow propagation (Tor), soft partition (I2P), and hard partition/no connection (CJDNS), as depicted in Figure 1. *Soft partition* differentiates the partition from the momentary forks (quickly resolved) and the permanent hard partition (difficult to execute and thus low-security risk). A node experiencing a soft partition does not promptly receive the updated information due to poor networking or networking threats, and the delay has a substantial impact on cryptocurrency operations. Our work is therefore related to the aforementioned security research studying partition threats and networking impacts, but differ in two ways: we show that the current anonymous routing can have the partition effects (while previous research introduces the threats/attackers as the reason for partitioning), and the previous security works have a one-time effect for mining on a block when the threat is executed (while our networking impacts are more sustained and apply to every block).

We implement an active Bitcoin node connected to the Mainnet via non-anonymous routing (IP), Tor anonymous routing (Tor), anonymous routing via the Invisible Internet Project (I2P), and CJDNS anonymous routing (CJDNS) for

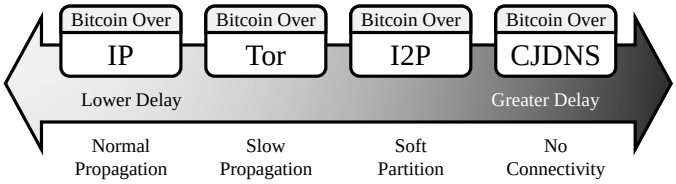


Fig. 1: Overview of our contributions and analysis insights. "IP" corresponds to networking without anonymous routing.

our empirical experimentation and data collection. We analyze both the networking data (from the Connection Manager and the backend Address Manager) and the consensus data to take a systems approach for our analyses and to better identify the factors and reasons for the varying networking performances (end-to-end latency vs. ecosystem). Our analyses therefore make use of the data including peer connection state, Address Manager state, network performance, Bitcoin goodput delivery of blocks and transactions, and the Bitcoin PoW hash rate.

The rest of the paper is organized as follows. Section II includes background information on the Bitcoin P2P network. Section III describes the implementation of our work. Section IV discusses the experimental results, highlighting potential issues. Section V discusses the potential for future research. Section VI discusses the related works and research gaps. Finally, we conclude our work in Section VII.

II. Background and Primer

A. Anonymous and Distributed Cryptocurrency

Cryptocurrencies' requirements for anonymity and censorship circumvention (e.g., cypherpunk's involvement in cryptocurrency) motivated the distributed and permissionless design of blockchain. The lack of centralized authority enables anonymous operations and censorship circumvention and, because the cryptocurrency network still wants to agree on the processed blocks and transactions, the cryptocurrency blockchain relies on distributed computing and distributed networking. Furthermore, permissionless blockchains (where anyone can freely join its network, validate transactions, or mine new blocks) do not rely on registration control and have the users self-generate and self-sign the public keys, from which the pseudonym account ID is generated. Such permissionless design for cryptocurrency applications is in stark contrast to other permissioned blockchains for different decentralized applications, as the permissioned blockchains build on registration control and thus can utilize the identity-based consensus protocol such as practical Byzantine Fault Tolerance or PBFT. While anybody can read, verify, and track the financial transactions recorded in the blockchain ledger, the transactions use pseudonym IDs and accounts (Bitcoin addresses are not linked to real-world identities) to protect user anonymity. In fact, Nakamoto inventing Bitcoin [11] recommends changing the Bitcoin Address for every transaction for anonymity purposes. Because of these permissionless and anonymous recommendations, Bitcoin supports the options to connect to the network using anonymous routing in Tor, I2P, and CJDNS; Section II-D provides more details about the anonymous routing technologies.

B. Ecosystem Participation in Distributed Computing and Networking

Cryptocurrency blockchain uses distributed computing and distributed (P2P) networking, as discussed in Section II-A, and both rely on the ecosystem and the magnitude of the consensus participants/network. Distributed computing in general (beyond blockchain applications) relies on the adversary controlling less than a threshold of the consensus participation to achieve consensus and agreement. If the adversary compromises greater than this threshold, then it controls the agreement (for example, in the cryptocurrency context, can revoke the transactions and launch double-spending). The threshold for the attacker compromise also applies to blockchain's distributed computing, although blockchain introduces different ways to measure the consensus participation magnitude. For PoW consensus protocol, the threshold is 50% measured by the computing power (known as "51% attack"); for PBFT, the threshold is 33.3% measured by the number of identities; for PoS, the threshold is 33.3% measured by the currency stakes. Because of the attacker compromise threshold, more mature blockchain and greater consensus participation provide stronger ledger/transaction security, e.g., against the adversary controlling the ledger or launching double-spending. For example, Bitcoin with its vast miner network is considered secure in its ledger/transaction integrity, and Bitcoin ledger acting as a trusted ledger can be used to secure the Ethereum PoS [12]. In contrast, the newer currencies with a smaller degree of consensus participation are more vulnerable against the ledger/transaction integrity [13], [14].

Distributed networking also relies on the mass of the networking nodes for its networking performances. More specifically, distributed P2P networking is used in cryptocurrency to broadcast/deliver the blocks and the transactions to all of the nodes participating in the cryptocurrency (both the consensus nodes as well as the client/user nodes of the cryptocurrency) and to make the delivery more efficient.

C. Networking Driving Cryptocurrency Consensus: Forks and Partitioning

The P2P networking is critical for the cryptocurrency operations, as the operations rely on the information delivered through networking. The highly competitive and resource-consuming consensus mining operations in particular heavily rely on the networking information delivery. If the blocks are not promptly delivered, then the miner mines on the outdated block wasting its mining computation resources. If the transactions are not delivered, the miner has less/no transactions in its mining pool to construct the block, and the mining reward in the transaction fees decrease.

The networking does not occur instantaneously due to the transmission delays between the peers, and there is a natural delay for the information to get broadcast across the

cryptocurrency network. Such networking delay yields block *forks* where distinct blocks get mined almost simultaneously and there is a discrepancy (and momentary synchronization failure) within the network about which block got mined first. The forks occur because one block can arrive earlier in one node while the other block arrives earlier in another node, and the two nodes clash in deciding which block got mined first and should be accepted. The fork issue, which can be viewed as a synchronization issue in distributed computing, has been anticipated from the cryptocurrency Bitcoin invention [11] and resulted in early mechanisms to address them, including confirmation mechanisms (to wait for the block processing finalization until multiple blocks get mined), the longest-chain rule (resolving which block to build on to resolve the forks). Newer-generation cryptocurrencies beyond Bitcoin, such as Ethereum Classic, further provide partial rewards for the orphan and uncle blocks (the blocks that lose the forking race and do not get selected for the main chain) to improve the networking fairness across the nodes.

More nefarious networking threats can result in partitioning so that the discrepancy and the synchronization failure about the newest block sustain longer than the naturally occurring forks. The network partition results in a longer discrepancy about the latest block information between the nodes so that the nodes operate on distinct blocks for a longer time. Previous research studied the networking partition sustaining its effect from 10 minutes [2] [3] [4] to 1 hour [5], although much of these previous research works got explicitly patched and are no longer as effective as they were in the current Bitcoin implementation practice [6] [7] [8] [9] [10]. We call this *soft partition* to differentiate between the momentary forks (quickly resolved) and the permanent hard partition (difficult to execute in the network and thus low-security risk). The partition is soft to distinguish from the permanent partition. A node experiencing a soft partition does not promptly receive the updated information due to poor networking or networking threats, and the delay has a significant impact on cryptocurrency operations.

D. Anonymous Routing

Anonymizing Proxy and Mixnet, Building Blocks: Anonymizing Proxy and Mixnet provide networking mechanisms to hide the identity to achieve anonymity and protect their privacy. To understand anonymizing proxy, assume Alice is visiting a website, but she does not want Eve to recognize her. Instead of directly connecting to the website, Alice uses Bob's computer as an anonymizing proxy. Alice sends all traffic to Bob, and Bob forwards them to the website. In Eve's perspective, it looks like Bob is visiting this website. In Mixnet, Alice uses a chain of anonymizing proxies to make it harder to track. In addition, Mixnet provides Alice with different nodes to randomly mix the traffic. Mixnet can even encrypt Alice's traffic through public key encryption by using the Diffie-Hellman key exchange algorithm. The random mix nodes and the encryption create anonymity and better protect Alice's privacy.

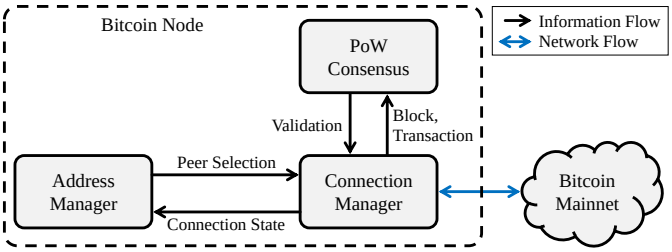


Fig. 2: The architecture including Connection Manager, Address Manager, and their interplay with the Consensus Protocol. Our implementation has sensors and data collection in these Bitcoin components.

Tor (Onion Routing): Tor builds on Anonymizing Proxy and Mixnet that enhances anonymity. It also uses public key encryption to secure users' communication. In a Tor circuit, a user directly connects to the entry node, and the destination directly connects to the exit node, middle nodes lay in between the entry and exit nodes [15]. Through this design, no single node can see the entry and destination of a packet, hence, the anonymity and privacy. The more middle nodes in a circuit, the more anonymization. However, this comes with a price of increased latency. More middle nodes mean a longer latency. Tor's hidden service, which the current Bitcoin over Tor implementation practice uses, worsens the user experience. While a hidden service mainly provides anonymity to the content sharers, it also adds network latency because of the rendezvous design which creates a six-node circuit [15]. Compared to the regular Tor circuit, this significantly increases the latency for Tor users to reach a hidden service content.

I2P (Garlic Routing): I2P differs from Tor in two ways. First, the Invisible Internet Project (I2P) traffic does not reach destinations on the public Internet by design [16]. This adds more anonymity than Tor because information is not leaking to the outside. Therefore, I2P is better for peer-to-peer communication, file sharing, etc. In case if an I2P user wants to connect to the public Internet, there are volunteer outproxy service providers. Second, while Tor network uses bidirectional communication in which inbound and outbound traffic goes through the same route, I2P uses multiple tunnels for outbound traffic but only two tunnels for inbound traffic [16]. For each outbound and inbound tunnel, there are multiple nodes between the user and the destination.

CJDNS (IPv6-based Routing): CJDNS places an additional constraint on peer discovery and selection in that they require a known acquaintance, i.e., a common peer connection.

III. Our Implementations of Bitcoin Over IP, Tor, I2P, and CJDNS Networking

We implement and build an active Bitcoin node on a Linux machine connected to the Mainnet. The machine specs are 2.46GHz Processor and 64 GB DDR4 RAM. The node includes network sensors to collect data at different logical components within a Bitcoin node (more specifically, the Connection Manager, Address Manager, and PoW Consensus

as shown in Figure 2). Our node is a private node, i.e., the IP address is not publicly advertised, and therefore do not accept inbound connections. We make our node a private node to limit the randomness factors and focus on the IP vs. Tor vs. I2P. To collect more samples across different connection settings, we reset our node and change the peer connections (and the entry guards for Tor and I2P) every 16 minutes. These are the only deviations that we make from the default Bitcoin and Tor/I2P settings.

While maintaining the experimental setup, we vary the networking types between the following three cases: "IP" disabling anonymous routing, "Tor," "I2P," and "CJDNS". These anonymous routing protocols are described in greater details in Section II-D. Other than varying the networking, we retain the same implementation setup for comparison and analyses fairness.

A. Connection Manager, Address Manager, and PoW Consensus

We implement sensors and collect data on the Connection Manager, PoW Consensus, and Address Manager to take a systems approach for our analyses. This section describes and explains the interplay and relations between these logical entities within a Bitcoin node.

Figure 2 depicts the information flows and relations between the Connection Manager, Address Manager, and the Consensus Protocol. Bitcoin node connects to other peers in the Bitcoin Mainnet via P2P networking, as shown on the right in Figure 2 with a blue bidirectional arrow to denote the network flow. Within a Bitcoin Node, the Connection Manager builds the networking sockets and implements the P2P networking. While the Connection Manager focuses on the current connections based on TCP/IP, the internal Address Manager manages the pool of possible candidate peer addresses. The internal Address Manager selects and provides the peer information when the Connection Manager wants to make a new connection.

While information is being propagated throughout the network, the Connection Manager sends blocks and transactions to the PoW consensus as shown with a black unidirectional arrow labeled "Blocks, Transactions". The PoW Consensus is responsible for validating the blocks and transactions. Upon validating the blocks and transaction, the PoW Consensus sends information back to the Connection Manager as shown with a unidirectional arrow named "Validation". Newly mined blocks are now being relayed throughout the network. The Connection Manager also keeps track of active connections in Address Manager as shown with a unidirectional arrow named "Connection State". If Connection Manager finds any malfunctioning, it assigns a ban score to the peer. Peers with a ban score of 100 get temporarily banned from the network. While the Connection Manager checks the connection status, the Address Manager stores the list of new addresses and tried addresses. When a new peer needs to be selected, the Address Manager uses a pseudorandom procedure. The Address Manager sends the address and the connection ID of the selected peers to the Connection Manager as shown with a unidirectional arrow named "Peer Selection".

TABLE I: Measured vs. calculated parameters.

For	Measured	Calculated
Connection Manager	Peer IP Address	Time to Convergence
	Connection Duration	
	Number of Connections	
Address Manager	Address in New Bucket	
	Address in Tried Bucket	
	Duration of Addresses	
Network Performance	Bitcoin Ping RTT	Response Duration
	Bandwidth I/O	
Bitcoin Goodput Delivery	Block Propagation Delay	Unique vs. Redundant
	Transaction Per Second	
Consensus Protocol Mining	Hash Rates	Wasted Hashes

B. Measured vs. Calculated

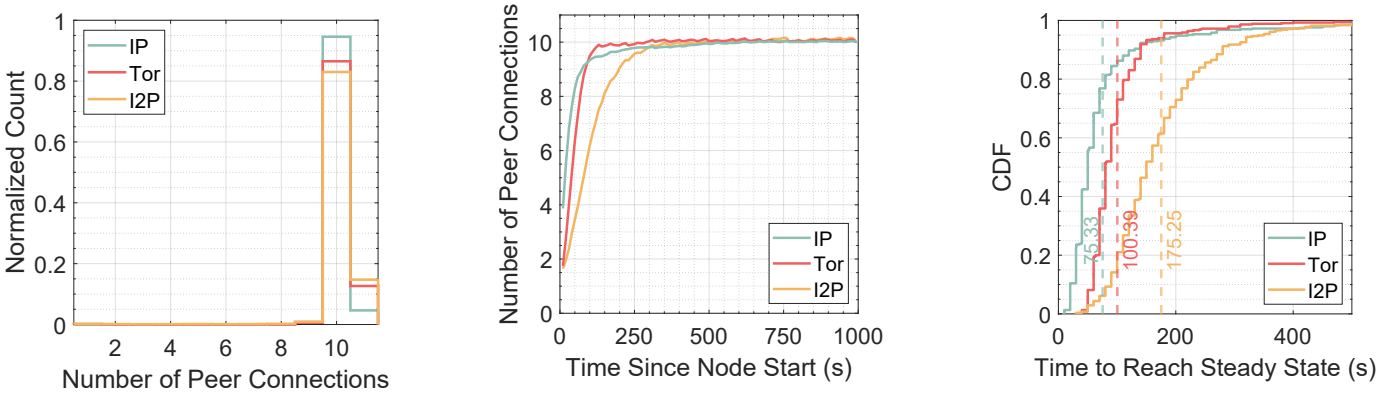
We measure the following Bitcoin network parameters: (i) Peer Connection State: quantify number of peer connections and time to reach peer convergence. (ii) Address Manager State: measured number of addresses, duration of addresses in new and tried buckets. (iii) Networking Performance: surveyed Bitcoin PING RTT and incoming and outgoing Bandwidth. (iv) Bitcoin Goodput Delivery: measured block propagation delay and unique vs. redundant transaction rate. Table I lists these parameters in greater detail and distinguishes between the measured and calculated data. The measured column refers to the information we collect using our network sensors, while the calculated refers to values that we calculated based on sensing/measured data (for example, we calculate the time to convergence for each peer using a number of connections and connection duration in the measured column).

IV. Experimental Results

In this section, we present and explain our experimental results while varying just IP (disabling non-anonymous routing), Tor, and I2P. Our analyses generally focus more on IP without anonymous, Tor, and I2P, because CJDNS yields hard partition and no networking; after Section IV-A, our analyses compare IP vs. Tor vs. I2P and largely omit CJDNS. We organize this section presentation based on the parameter categorization in Section III-B. For the random and statistical experimental results, we present the averages and the 95% confidence intervals.

A. CJDNS: No Peers and No Networking

We implement and study CJDNS anonymous routing, which is available in the Bitcoin Core implementation (along with Tor, I2P, and disabling anonymous routing). However, we observe no connectivity when connecting to other Bitcoin nodes via CJDNS, resulting in the hard permanent synchronization failure, at the time of writing. This is due to the lack of Bitcoin peer nodes participating in the Bitcoin Mainnet through CJDNS. While Bitcoin Over CJDNS has been implemented, there are no active, public nodes to connect to and the Address Manager in our Bitcoin prototype cannot find any address supporting CJDNS. We empirically observe and verify that there are no nodes for Bitcoin over CJDNS from May 2023 to

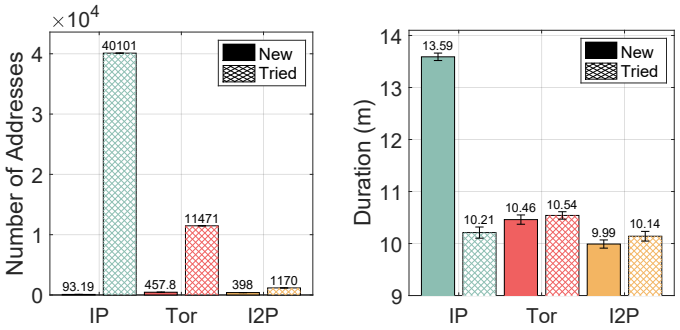


(a) Distribution of connectivity.

(b) Peer connections over time.

(c) Time to reach steady state.

Fig. 3: Empirical analyses of peer connection state for IP, Tor, and I2P networks. The dashed lines denote the averages.



(a) Number of addresses

(b) Address duration

Fig. 4: Measurements from the Address Manager. The number of addresses in the new and tried buckets (left) and the average time duration that an address stays within the address before ejection (right).

December 2023. Because CJDNS connections and networking are effectively disabled so its results are trivial, we focus our study more on the anonymous routing of Tor and I2P when implementing the anonymous routing on Bitcoin networking. The rest of the paper focuses on just IP (not anonymous routing), Tor, and I2P.

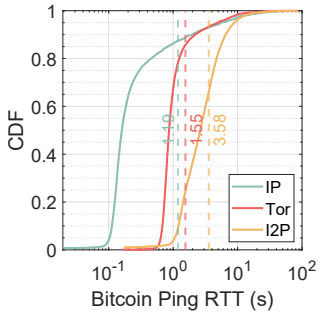
B. Peer Connections

We study the number of peer connections. Figure 3a shows the probability distribution/histogram of the number of peer connections. Because our Bitcoin node is a private node and does not publicly advertise or invite incoming peer connections, our Bitcoin node is designed to maintain ten connections. It succeeds in doing so, although IP does better than Tor and Tor better than I2P; IP maintains 10 connections with a probability of 0.9458, and Tor and I2P maintains a probability of 0.8651, and 0.83, respectively. On average, IP, Tor, and I2P has 10.04, 10.10, and 10.07 connections. We also observe non-zero probabilities where the number of connections exceed ten due to the feeler connections, which are short-lived connections to move the new address to tried address (Bitcoin does implement up to one feeler connection in excess of the ten connections).

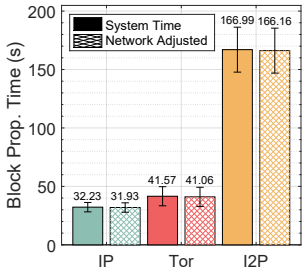
Figure 3b shows our Bitcoin prototype's progression in its number of connections after the initial reset and bootstrapping. In general, IP is quicker in making its connections than Tor and I2P. When our Bitcoin node first achieves ten connections, we call that the *steady state*. From our results in Figure 3c, we observe that Tor and I2P take longer to reach their steady states than IP. IP takes 75.33 seconds compared to 100.39 seconds and 175.25 seconds for Tor and I2P, respectively. Similarly, the standard deviation for IP to reach steady state is significantly smaller than Tor and I2P (0.235, 0.5114, and 0.7856 for IP, Tor, and I2P, respectively). IP is thus more efficient in establishing its connectivity to the network than the other networks.

C. Peer Addresses

The P2P networking size and the magnitude of participation affects the networking performances as discussed in Section II-B. Our sensing and measurements in the Address Manager inform the ecosystem and the number of P2P networking participants in IP vs. Tor vs. I2P. In Bitcoin, the Address Manager is the component which provides the pool of the peer addresses in the network, as described in Section III-A, and is internal to the Connection Manager actually making the connectivity. While the Address Manager has the capacity to list up to 1024 new and 256 tried buckets, each of which holds a maximum of 64 addresses, the actual number of peer addresses in the Bitcoin networks are less than such capacity. More specifically, as shown in Figure 4a, Bitcoin network over IP, Tor, and I2P have 40101, 11471, and 1170 new addresses, respectively. On the other hand, we observe the reverse behaviors in tried addresses where Tor and I2P exceed IP, which only has 93.19 addresses, with 457.8 and 398 addresses, respectively, on average. We also observe that IP has comparable or better reliability given a peer address and that it stays in the Address Manager pool longer. As shown in Figure 4b, the new addresses for IP stays longer in the Address Manager pool before ejection than when using anonymous routing; on average, an address in Bitcoin over

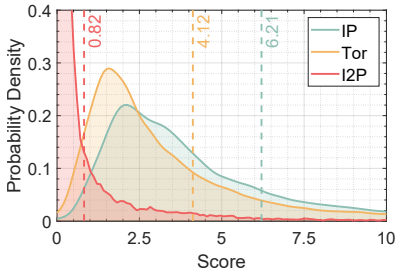


(a) Bitcoin PING RTT.

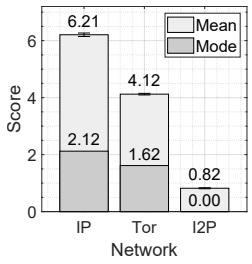


(b) Block propagation delay.

Fig. 5: Empirical analyses of network performance and Bitcoin block for IP, Tor, and I2P networks.



(a) The score distribution in PDF. The vertical dashed lines are the averages.



(b) The mean and mode of the score.

Fig. 6: The score analyses results for Bitcoin over IP, Tor, and I2P.

IP has a duration of 13.59 minutes, longer compared to Tor's peer address duration of 10.46 minutes and I2P's peer address duration of 9.99 minutes.

D. Network Round Trip Time

We measure the round-trip time (RTT) between the peer nodes using the Bitcoin ping protocol. Figure 5a shows the Cumulative Distribution Function (CDF) with a vertical dash line denoting average Bitcoin PING Round Trip Time (RTT). IP has the smallest RTT at 1.19 seconds, making it the fastest responsive. On the other hand, Tor takes a moderately longer 1.55 seconds and I2P exhibits the longest RTT of 3.58 seconds. It highlights that IP performs better than Tor and Tor better than I2P. while IP provides the swiftest RTT, Tor and I2P introduce delays inherently as discussed in Section II-D. We also measure and analyze the networking bandwidth but omit the results in this paper due to space constraint.

E. Blocks and Transactions Delivery and Impacts on Consensus

We measure and analyze the goodput delivery performances based on the block propagation time and the number/rate of transactions delivered because of their importance for the cryptocurrency operations including mining as described in Section II-C. Figure 5b shows block propagation delay. We measure propagation delay using network-adjusted time as well as system time. The network-adjusted time, known as "median time past" (MTP), is a time based on the median timestamp of the blockchain's latest 11 blocks, while the system time refers to the local system time of a machine or node in the Bitcoin network. We use both of them because they show distinct but redundant measurements capturing the same behaviors. From Figure 5b, we observe clear differences in the propagation efficiency. Our results reflect the trade-offs between efficiency and anonymity as discussed in Section II-D. As we use more advanced anonymous routing from disabling it and just using IP to Tor to I2P, there is a cost in efficiency and the block propagation delay increase. IP, disabling anonymous routing communication, has the lowest block propagation delay at 32.23 seconds in system time and at 31.93 seconds in network adjusted time. Tor, which provides anonymity as discussed in Section II-D, has a higher delay than IP at 41.57 seconds in system time and at 41.08 seconds in network adjusted time. Using Bitcoin over Tor results in slow propagation of the blocks compared to IP with no anonymous routing.

The more striking result for the Bitcoin goodput block delivery is with I2P, which presents a block propagation delay of 166.99 seconds in system time and 166.16 seconds in network adjusted time, significantly higher than IP and Tor. While IP and Tor has less than 10 seconds of difference between each other, I2P's block propagation delay is greater than Tor by more than two minutes. Because Bitcoin automatically adjusts its mining difficulty to have the new blocks get mined every ten minutes, the additional delay by using I2P over IP accounts for more than 20% of mining wastage. More than two minutes over the 10 minutes would get wasted mining on the earlier block compared to another miner using IP networking (non-anonymous routing). Bitcoin over I2P therefore yields soft partition and the effects are worse than known networking security threats on Bitcoin, as discussed in Section II-C. We also measure and analyze the transaction delivery rate and verify the consensus mining wastage in implementation and experimentation by measuring the hash computation wastage on mining on an outdated block but omit in this paper due to the space constraint.

F. Networking Score Analysis for Aggregating the Block and Transactions Goodputs

In this section, we introduce a score that counts and aggregates the block arrivals and the transaction arrivals from each peer connection. A peer delivering a unique block or a unique transaction increases its score and therefore an increased score means that the peer connection provides better information. Only the unique blocks/transactions count for the score, and the redundant/repeated blocks and transactions do not improve the score. We focus on the blocks and the transactions because those are the critical information inputs for the mining consensus operation, as described in Section II-C. The score also incorporates a decay function which decreases the score in constant amounts to model and capture the forgetfulness,

i.e., the effect of a good behavior on the score decreases as time passes. We adopt the score from the previous research quantifying the positive reputation based on a peer behavior in Bitcoin P2P networking, and more details about the score are in [17]. After the weighted-sum aggregation and normalization, we observe the score measurements going up to 391, i.e., a peer's score ranges between 0 and 391 in our empirical experimentation. Figure 6a shows the PDF distribution of our empirical score measurements, while Figure 6b shows the mean and the mode. IP outperforms Tor, and Tor outperforms I2P in our score analyses. IP yields the greatest mean and mode with the mean being 1.51 times larger than Tor, and Tor being 5.02 times larger than I2P.

V. Future Work Discussions

A. Build the Ecosystem

As demonstrated with our study with Tor, the soft partition effects that we observe with I2P (and the hard partition with CJDNS) can be resolved by building greater ecosystem and, more specifically, greater nodes participating in the anonymous routing. The cryptocurrency blockchain can achieve this by incentivizing the participation on the anonymous routing. For example, the relay nodes can detect the miner's anonymous routing participating and the cryptocurrency can reward such miners with greater rewards than the miners not participating in the anonymous routing.

B. Anonymous Routing Cost Mitigation

The anonymous routing induces greater latency costs than non-anonymous routing (just IP). This has not only been widely studied but also impacts our work and the cryptocurrency operations relying on the information delivered through the anonymous networking. We can mitigate or reduce such costs. The anonymous routing can be adapted for better networking performances and reduced transmission latencies, e.g., [18]–[23].

C. Cryptocurrency-Specific Anonymous Routing

While the traditional anonymous routing has been designed to be oblivious to the networking applications (e.g., cryptocurrency operations to process financial transactions), we can explore designing and building a cryptocurrency-specific anonymous routing. For example, Tor can be adapted to have a cryptocurrency-specific Tor by involving the block information (such as the CompactBlock) when the peer builds the Tor circuit; the peer node can receive the CompactBlock directly from the relay nodes as the peer node handshakes with the individual relays during the circuit construction (which precedes the use of the circuit for other goodput deliveries).

D. Delay-Tolerant Consensus

There are other consensus protocols more networking-delay-tolerant than PoW. The second most popular consensus protocol (in the market capitalization) is the proof-of-stake (PoS) whose fairness is based on the amount of currency the validator deposits/stakes. As is shown by the newer-generation blockchains adopting PoS consensus and the Ethereum cryptocurrency transitioning from PoW and PoS, the cryptocurrency blockchain can use such consensus protocol. PoS consensus protocol is more networking-delay tolerant than PoW because the networking in-synchronization due to the broadcasting delays has less of an impact in PoS, i.e., the consensus is more deterministic with respect to the networking broadcasting. The analyses study adopting the anonymous routing on PoS and the tradeoff between PoW and PoS in such anonymous routing are left for future work. (Practical byzantine fault tolerance or PBFT which is a voting- and registered-identity-based consensus protocol is not as relevant as PoS or PoW for cryptocurrency. PBFT is more appropriate for blockchains for non-permissionless applications as it assumes and relies on the registration control and thus irrelevant for anonymity-important cryptocurrencies.)

VI. Related Work

Our research conducts an empirical study on the use of anonymous routing for Bitcoin cryptocurrency and identifies potential issues on Bitcoin's performance over anonymous routing. We divide our related works into: Partitioning Attacks, Bitcoin Over Tor, and Bitcoin Performance Analysis.

A. Partitioning Attack

Our work shows that anonymous routing can have Bitcoin network partitioning effects due to the lack of ecosystem and participation, such as the soft partitioning wasting two out of the ten minutes (20% of the mining) for I2P (Section IV-E) and hard partitioning for CJDNS (Section IV-A). As discussed in Section II-C, network partitioning in cryptocurrency/Bitcoin previously have been studied in the security context where a security adversary causes the partitioning.

Bitcoin and cryptocurrency networking design and implementations have been advancing in its security and robustness against the harmful partitioning thanks to the previous research studying the partitioning threats. The initial study on partitioning attack was conducted by Heilman et al. [24] in 2015. They demonstrated an adversary can partition Bitcoin nodes by adding non-existent Bitcoin IP addresses into a targeted node's internal databases. However, Bitcoin developers developed a peer eviction mechanism to mitigate the Eclipse attack [6]. In 2020, Tran et al. [3] introduced a stealthier version of the attack proposed in [24], where the partition has a 10-minute delay. They illustrated an adversarial Autonomous System (AS) could flood the IP tables of a victim node to occupy the incoming and outgoing connections of the node. Considering this, the Bitcoin Core team developed two patches to mitigate the attack [7] [8]. In 2018, Apostolaki et al. [2] proposed a BGP hijacking attack that similarly causes a partition of Bitcoin and has a 10-minute duration. They examined the network hash rate and discovered that by hijacking three ISPs, an attacker can reduce the hash rate by more than 60%. As a solution to this, a new Bitcoin relay, called SABRE was proposed by Apostolaki et al. in [10]. Saad et al. [25] reported that the Bitcoin network is getting centralized at the AS-level

which makes it more vulnerable to partitioning attacks. They investigated that after five minutes, around 62.7% of nodes are one or two blocks behind the most recent block. The attacker in the SyncAttack [4] proposed by Saad et al. splits the whole Bitcoin P2P network by monopolizing the incoming connection slots of all public Bitcoin nodes for ten minutes. However, similar to [24], the Bitcoin Core mitigated the attack [7] [8]. The optimization techniques for the two attacks in [3] and [4] were proposed by Ha et al. [5] in 2023. They showed that their partition effects sustained for an hour. Tran et al.'s Routing-Aware Peering (RAP) approach [9] can defend against the attack in addition to the Bitcoin's countermeasures in [7] and [8]. However, although showing comparable effects in the older versions of Bitcoin/cryptocurrency as our work, these previous works studied partition threats, whereas our work focuses on studying anonymous routing that can have partition effects. We demonstrate that the current anonymous routing can have partition effects but differ from these previous research studying partitioning threats in two ways: first, the cause of partitioning are security threats and attackers in this previous literature; second, these previous works had a one-time effect for mining on a block when the threat is executed, whereas our networking effects last longer and apply to every block.

B. Bitcoin Over Tor

Previous research works studied Bitcoin over Tor anonymous routing but for different purpose as ours; these literature uses Tor to attack Bitcoin node's availability and anonymity/privacy. Biryukov et al. [26] proposed an attack that targets a Bitcoin node linked via Tor. The attacker takes advantage of Bitcoin's DoS protection function to force all of its connections through the adversary-controlled Tor exit nodes. Biryukov et al. [27] disclosed that using Tor to access Bitcoin not only provides limited anonymity but also exposes the user to man-in-the-middle attacks. An attacker can gain control over which blocks and transactions a user is aware of. Mastan et al. [28] proposed a deannonymization attack on unreachable nodes that are hidden behind NAT and using Tor. They leveraged block-request patterns to track a victim over consecutive sessions. However, these previous works studied Bitcoin threats over anonymous routing, whereas our work is focused on studying anonymous routing that can yield slow propagation and partitioning.

C. Bitcoin Performance Analysis

Previous research literature analyzed the Bitcoin's networking performances but without anonymous routing. Saad et al. [25] studied on centralization of Bitcoin nodes over the internet. They highlighted that the growing centralization of the Bitcoin network results in spatial, temporal, spatio-temporal, and logical attacks. Shahsavari et al. [29] analyzed network performance using Bitcoin inventory protocol and identified two significant network performance parameters: the average number of default connections for peers and block size. In 2020, Shahsavari et al. [30] investigated compact block propagation delay and traffic overhead. They emphasized the trade-offs in propagation delay and network overhead, especially over relay networks. Their work showed that increasing peer connections could reduce block propagation delay but may increase network traffic overhead. Wuthier et al. [31] conducted an empirical analysis of block propagation time, focusing on the number of peer connections at the node level. Their study, however, did not account for other parameters that might offer a broader perspective on the ecosystem beyond individual nodes.

Most of these previous research, e.g., [25], [29], [30], use a simulator to evaluate their analyses, except for [31]. However, in our research, we collect real-world data to empirically analyze Bitcoin network performance over IP, Tor, and I2P networks. In addition, unlike their works that consider only peer connection states, we implement our sensors and collect data on distinct logical components in Bitcoin (Connection Manager, Address Manager, and Consensus) in order to take a systems approach to enable the analyses and mapping between the causes and effects.

VII. Conclusion

Bitcoin and cryptocurrencies are designed for anonymous transaction processing. To support such anonymity in the cryptocurrency applications, the underlying P2P networking uses anonymous routing, for example, the current Bitcoin implementation (Bitcoin Core) supports and provides the options for Tor, I2P, and CJDNS. We study and analyze the networking of Bitcoin with anonymous routing. We take an empirical approach by building sensors and and collect data from the Bitcoin's Connection Manager and Address Manager and deploying an active Bitcoin prototype connected to the Mainnet. We take a systems approach to analyze the anonymous networking impacts on the PoW consensus protocol and compare with the non-anonymous routing. In addition to introducing additional latencies inherent-by-design of the anonymous routing, the P2P ecosystems of these anonymous routing are underdeveloped. Bitcoin therefore faces unique networking challenges with these protocols; while CJDNS yields no connectivity because there is no active public peer, Tor suffers slow propagation and I2P causes soft partition, both affecting the effectiveness of consensus mining. Bitcoin over I2P causes soft partition by delaying the block propagation for every block arrivals by more than two minutes compared to Bitcoin over Tor, which difference accounts for more than 20% mining wastage of the PoW consensus protocol. Our research informs the current state of practice when incorporating cryptocurrency over anonymous routing and provides recommendations and discussions for future directions.

References

[1] "The global crypto market cap, 2023," 2023. [Online]. Available: https://coinmarketcap.com/

[2] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *2017 IEEE symposium on security and privacy (SP)*. IEEE, 2017, pp. 375–392.

[3] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang, "A stealthier partitioning attack against bitcoin peer-to-peer network," in *2020 IEEE symposium on security and privacy (SP)*. IEEE, 2020, pp. 894–909.

[4] M. Saad, S. Chen, and D. Mohaisen, "Syncattack: Double-spending in bitcoin without mining power," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 1668–1685.

[5] J. Ha, S. Baek, M. Tran, and M. S. Kang, "On the sustainability of bitcoin partitioning attacks," in *Financial Cryptography and Data Security: 27th International Conference, FC 2023*. International Financial Cryptography Association, 2023.

[6] "The peer eviction mechanism implementation of bitcoin core (august 2015)," 2015. [Online]. Available: https://github.com/bitcoin/bitcoin/commit/2c701537c8fc7f4cfb0163ec1f49662120

[7] "Supplying and using asmap to improve ip bucketing in addrman, 2020," 2020. [Online]. Available: https://github.com/bitcoin/bitcoin/pull/16702

[8] "Try to preserve outbound block-relay-only connections during restart," 2020. [Online]. Available: https://github.com/bitcoin/bitcoin/pull/17428

[9] M. Tran, A. Shenoi, and M. S. Kang, "On the {Routing-Aware} peering against {Network-Eclipse} attacks in bitcoin," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 1253–1270.

[10] M. Apostolaki, G. Marti, J. Müller, and L. Vanbever, "Sabre: Protecting bitcoin against routing attacks," *arXiv preprint arXiv:1808.06254*, 2018.

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, 2008.

[12] E. N. Tas, D. Tse, F. Gai, S. Kannan, M. A. Maddah-Ali, and F. Yu, "Bitcoin-enhanced proof-of-stake security: Possibilities and impossibilities," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 126–145.

[13] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. "O'Reilly Media, Inc.", 2014.

[14] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM*, vol. 61, no. 7, pp. 95–102, 2018.

[15] R. Dingledine, N. Mathewson, P. F. Syverson *et al.*, "Tor: The second-generation onion router." in *USENIX security symposium*, vol. 4, 2004, pp. 303–320.

[16] "The invisible internet project i2p." [Online]. Available: https://geti2p.net/en/about/intro

[17] S. Wuthier, N. Sakib, and S.-Y. Chang, "Positive reputation score for bitcoin p2p network," in *IEEE Consumer Communications Networking Conference*. IEEE, 2023.

[18] M. Akhoondi, C. Yu, and H. V. Madhyastha, "LASTor: A Low-Latency AS-Aware Tor Client," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, May 2012, simulation based and planetlab based.

[19] M. Sherr, M. Blaze, and B. T. Loo, "Scalable link-based relay selection for anonymous routing," in *Proceedings of Privacy Enhancing Technologies, 9th International Symposium (PETS 2009)*, ser. Lecture Notes in Computer Science, I. Goldberg and M. J. Atallah, Eds., vol. 5672. Springer, August 2009, pp. 73–93, authors proposed weighted latency calculation method for the link-based relay selection. first they rank randomly generated paths accroding to their predicted e2e performance, then user sort the paths by their cost. simulation based.

[20] M. AlSabah, K. Bauer, and I. Goldberg, "Enhancing tor's performance using real-time traffic classification," in *Proceedings of the 19th ACM conference on Computer and Communications Security (CCS 2012)*, October 2012.

[21] A. Kate and I. Goldberg, "Using sphinx to improve onion routing circuit construction," in *Proceedings of Financial Cryptography (FC '10)*, R. Sion, Ed., January 2010, improving based on new circuit construction algorithm.

[22] C. Tang and I. Goldberg, "An improved algorithm for Tor circuit scheduling," in *Proceedings of the 2010 ACM Conference on Computer and Communications Security (CCS 2010)*, A. D. Keromytis and V. Shmatikov, Eds. ACM, October 2010, proposed a method to provide QoS for both downloading and broswinng activities in Tor network.This ethod has been implemented in Tor.

[23] M. Imani, M. Amirabadi, and M. Wright, "Modified Relay Selection and Circuit Selection for Faster Tor," Aug. 2018, arXiv:1608.07343 [cs]. [Online]. Available: http://arxiv.org/abs/1608.07343

[24] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on {Bitcoin's}{peer-to-peer} network," in *24th USENIX security symposium (USENIX security 15)*, 2015, pp. 129–144.

[25] M. Saad, V. Cook, L. Nguyen, M. T. Thai, and D. Mohaisen, "Exploring partitioning attacks on the bitcoin network," *IEEE/ACM Transactions on Networking*, vol. 30, no. 1, pp. 202–214, 2021.

[26] A. Biryukov and I. Pustogarov, "Bitcoin over tor isn't a good idea," in *2015 IEEE Symposium on Security and Privacy*. IEEE, 2015, pp. 122–134.

[27] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 2014, pp. 15–29.

[28] I. D. Mastan and S. Paul, "A new approach to deanonymization of unreachable bitcoin nodes," in *Cryptology and Network Security: 16th International Conference, CANS 2017, Hong Kong, China, November 30—December 2, 2017, Revised Selected Papers 16*. Springer, 2018, pp. 277–298.

[29] Y. Shahsavari, K. Zhang, and C. Talhi, "Performance modeling and analysis of the bitcoin inventory protocol," in *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*. IEEE, 2019, pp. 79–88.

[30] ——, "A theoretical model for block propagation analysis in bitcoin network," *IEEE Transactions on Engineering Management*, vol. 69, no. 4, pp. 1459–1476, 2020.

[31] S. Wuthier, P. Chandramouli, X. Zhou, and S.-Y. Chang, "Greedy networking in cryptocurrency blockchain," in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2022, pp. 343–359.