Infnote: A Decentralized Information Sharing Platform Based on Blockchain

Haoqian Zhang
Hong Kong University of Science and Technology, Hong Kong, China
hzhangbi@connect.ust.hk

Yancheng Zhao
Hong Kong University of Science and Technology, Hong Kong, China
yanchengz@ust.hk

Abhishek Paryani
Hong Kong University of Science and Technology, Hong Kong, China
aparyani@connect.ust.hk

Ke Yi
Hong Kong University of Science and Technology, Hong Kong, China
yike@cse.ust.hk

ABSTRACT

Internet censorship has been implemented in several countries to prevent citizens from accessing information and to suppress discussion of specific topics. This paper presents *Infnote*, a platform that helps eliminate the problem of sharing content in these censorship regimes. Infnote is a decentralized information sharing system based on blockchain and peer-to-peer network, aiming to provide an easy-to-use medium for users to share their thoughts, insights and views freely without worrying about data tampering and data loss. Infnote provides a solution that is able to work on any level of Internet censorship. Infnote uses multi-chains architecture to support various independent applications or different functions in an application.

PVLDB Reference Format:
Haoqian Zhang, Yancheng Zhao, Abhishek Paryani, Ke Yi. Infnote: A Decentralized Information Sharing Platform Based on Blockchain. *PVLDB*, 12(xxx): xxxx-yyyy, 2019.
DOI: https://doi.org/10.14778/xxxxxxx.xxxxxxx

1. INTRODUCTION

Freedom of speech is considered a basic human right under Article 19 of the *Universal Declaration of Human Rights* [3]. The evolution of digital telecommunications have brought with it both opportunities and challenges for freedom of speech. On the one hand, we can access or deliver information faster via several mediums, while on the other hand, regulators can use both technical and non-technical methods to control or suppress what can be published or viewed on the Internet. While Internet users can utilize circumvention technologies to bypass Internet censorship to access or publish information, regulators around the world have significantly increased their efforts to control the information flow on social media [9]. A recent report concludes that the internet is growing less free globally, and democracy itself is withering under its influence [10].

Blockchain, as an append-only global ledger, has already been used in a decentralized version of the DNS[13] and data storage [1]. Blockchain is an ideal system for an information sharing platform aimed to circumvent Internet censorship. This is becuase nobody can modify the committed blocks that store the content, which is a precious and useful feature intrinsic to blockchain-based systems. In China, people have already started to use blockchain to battle government censorship. For example, in 2018, an anonymous user attached an open letter to an ether transaction and posted it to the Ethereum blockchain [12].

Infnote, is our answer to the limitations of the existing platforms. The name 'Infnote' comes from providing **inf**inite power through the **note**s that the community of users publish. Infnote will provide a tool to content creators, social activists, journalists and others who simply want their voices to be heard.

Infnote, based on blockchain and P2P technologies, aims at providing a platform for users to share their thoughts, insights and opinions under varying levels of Internet censorship. It is a decentralized platform that can provide the user with pseudo-anonymity and transparency, and allow content to travel and be viewed freely across a network of users. Unlike conventional blockchain, that uses a single chain to store information, Infnote uses multi-chains to support various independent applications or different functions in an application.

2. INTERNET CENSORSHIP

Prior to presenting our solution, we provide a context to the censorship problem by defining the degrees of censorship. In section 4.2, we will analyze our system in different level of censorship.

Little or No Censorship: Little or no censorship is enforced in these countries. There is no need to use any circumvention technology since the majority of content is

Proceedings of the VLDB Endowment, Vol. 12, No. xxx
ISSN 2150-8097.
DOI: https://doi.org/10.14778/xxxxxxx.xxxxxxx

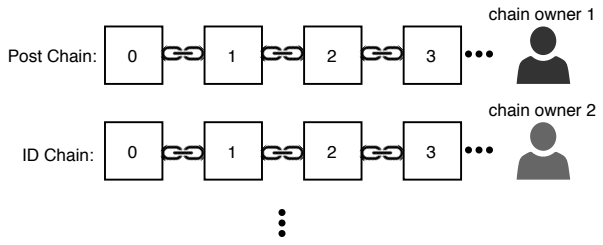


Figure 1: Multi-chains structure

open to access.

Selective Censorship: A small number of websites are blocked. Unsophisticated censorship methods, like IP address blocking or DNS filtering and redirection are likely to be used. Most democratic countries fall under this category, where websites dealing with illegal or illicit activity may be blocked and freedom of speech is protected by legal systems.

Substantial Censorship: At this level, a large portion of content on the Internet is blocked and several censorship methods are implemented simultaneously. A blacklist of IP addresses and domains is likely to be enforced by the firewall. Anti-censorship circumvention tools may also be targets of censorship, making it extremely difficult for citizens to bypass the censorship.

Pervasive Censorship: At this level, a whitelist is enforced by the firewall at regional boundaries, implying that only approved Internet traffic will be allowed to pass the boundary of a censored region. This makes it theoretically impossible to use any proxy or VPN, whose IP is outside of the boundary.

No Internet: In extreme situations, the Internet service may be completely cut off and circumvention tools that rely on the Internet will not work. It is extremely difficult for citizens to access or distribute digital information. During the Arab Spring, the Egyptian government shut down the Internet in Egypt temporarily.

3. DESIGN AND IMPLEMENTATION

Infnote is a general information sharing platform based on blockchain that can support various applications, such as a portal to share information, a blog to write articles, or a forum to discuss topics. The features that distinguish Infnote from existing platforms is that we are able to provide users access and publish contents in censorship-driven countries without costing any cryptocurrency, preserve all history of content, verify and trust that the source of the content is from the original author, provide assurance that data will not be tampered or lost once published and offer access to the platform regardless of what type of device the user owns. This is made possible through the use of P2P, blockchain and our unique architecture.

3.1 Blockchain

It is possible to directly use or fork popular blockchain systems such as bitcoin or Ethereum and build Infnote upon them. However, in order to transact in these blockchain systems, crytocurrency is a necessity, which is a huge barrier to entry for many users. The open letter sent to Ethereum against Chinese government censorship costed cryptocurrency that worth 52 cents [12]. Keeping this barrier in mind, we decided against any monetary element. We assume that, as a free-for-all information sharing platform against censorship, freedom of speech is an already strong enough incentive for people to join and contribute to Infnote.

Infnote utilizes blockchain technology to store information. When a user wishes to publish a post on the platform, the post will be signed with the user's private key. Later, the post will be bundled with other posts and additional information (like timestamp etc.) together into a block. The *chain owner*, who has the authority to insert blocks into the blockchain, will sign the block with his private key. The block will be broadcasted to the P2P network, and every node in the network will verify it.

3.1.1 Cryptography

We utilize a digital signature scheme implemented using *ECDSA* with *secp256k1* curve [11] and a cryptographic hash function *SHA-256* [14], the same building blocks as bitcoin.

3.1.2 Consensus mechanism

Infnote uses Proof of Authority (POA) as its underlying consensus mechanism. POA only allows authorized nodes to insert blocks into the blockchain. Only a chain owner can insert blocks into a chain and therefore control the information on the platform.

3.1.3 Block

A typical block structure contains the following attributes: ChainID, Height, Time, PrevHash, Hash, Signature and Payload. Similar to the role of a miner in bitcoin, a chain owner's role is to generate a new block signed with his or her private key and broadcast it to the nodes that are connected to it.

3.1.4 Multi-chains

Infnote uses a multi-chains architecture, which means there are several independent parallel chains. Each chain is controlled by its chain owner. Multi-chains architecture can be used in various independent applications or different functions in an application. **Figure 1** demonstrates an example of a simple discussion forum, in which posted data is stored in the Post Chain while user data is saved into the ID Chain which can be shared among other applications.

3.2 Nodes

We fully expect multiple types of devices to join the network, such as laptops, desktops, servers, smart-phones and so on. In Infnote, there are two kinds of nodes, full nodes and light nodes. Full nodes are devices that have sufficient bandwidth and computational resources (such as personal computers and servers) to support all the functions of Infnote which include: storing all the data in the blockchain, providing logic to view and publishing content and acting as a server by listening for connections and providing services to clients. Many devices, such as smart-phones or web browsers cannot be full nodes, due to limited resources and processing power. Hence, they must rely on the full nodes to provide comprehensive services. At the same time, light nodes can still use their limited resources to cache and broadcast blocks.

3.3 Network

In Infnote, once a new block is generated, it will immediately be sent out so that every node can obtain the new block

quickly. A publish-subscribe pattern is followed, where publishers (chain owners) send blocks and subscribers receive these blocks in a short time. This feature allows nodes to automatically obtain new posts in Infnote in real time.

3.4 Preventing Attacks

In order to prevent flooding messages into the system, chain owners could use all techniques that have been implemented in traditional websites, such as utilizing CAPTCHA or binding with users' social media accounts. Additionally, Infnote uses the same set of cryptography building blocks like bitcoin, making it possible to verify users' accounts and even requiring payments in bitcoin blockchain. For the malicious chain owners or adversaries who have made up identities to be chain owners, a node can simply disconnect itself from the P2P network automatically, based on local settings. As there is no restriction of becoming a chain owner by creating a new chain, all nodes will not automatically maintain new chains, unless users or the developing community decide to maintain them, preventing useless or low quality chains.

4. EVALUATION

4.1 Throughput and Latency

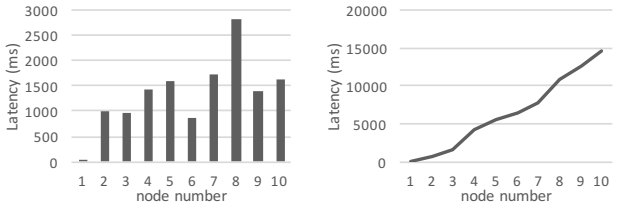
We evaluate our system quantitatively in comparison to bitcoin, focusing on two aspects of the system: throughput and latency. Throughput is how many posts the system can handle per second. Latency is the amount of time it takes for a block to be confirmed by all nodes on the P2P network. For testing, we assume that the size of a post in Infnote is 250 bytes, around the same size as a basic bitcoin transaction. We also assume that the size of a block is 1 megabyte.

Throughput: Our experiment shows that Infnote's throughput can reach approximately 150,000 posts per second, running the Go version of the Infnote program on a 2015 version Macbook Pro. The result could be further improved by deploying better hardware or optimizing the code. Bitcoin, which takes approximately ten minutes to confirm a block, achieves only 7 transactions per second maximum throughput [6].

Latency: We simulated a global environment using nodes that were spread across the world geographically. In a test environment, as it is impossible to deploy a P2P network on a large scale due to limited resources, we speculate on the performance of such a system by using only a small number of nodes. We utilize ten nodes in different geographic regions around the world, with eight full nodes and two light nodes. [1] Node No.8 is a light node running on an iPhone 8, and node No.10 is another light node running on a JavaScript program of Infnote on a Chrome web browser. Node No.1 is the chain owner who generates new blocks. We tested both systems in a star topology network and a linear topology network.

Figure 2(a) shows the results in the star topology network. On average, the latency is 1.3 seconds, for every node in the network to receive a 1 megabyte block, which basically matches the network latency. **Figure 2(b)** shows the results

[1]The nodes are located in Tokyo (node No.1), Singapore (node No.2), Kuala Lumpur (node No.3), Sydney (node No.4), Mumbai (node No.5), Hong Kong (node No.6), Dubai (node No.7), Hong Kong (node No.8), Silicon Valley (node No.9) and Hong Kong (node No.10).



(a) latency with different number of nodes

(b) latency with different network diameters

Figure 2: Latency of the Infnote

in the linear topology network. The experiment aims to represent the results of a large network with different network diameters. The first node in the chain is the chain owner. Infnote takes 14.6 seconds to transmit a 1 megabyte block in the entire network with 10 diameters. For the bitcoin network at that time with around 3500 reachable nodes, one result shows that the median latency is 6.5 seconds whereas the mean is at 12.6 seconds and after 40 seconds there are still 5% of nodes that have not yet received the block [7].

4.2 Effectiveness

In this part, we analyze the effectiveness of Infnote on different levels of internet censorship. In a little or selective censorship environment, it is not necessary to use Infnote as a circumvention tool. Infnote is a way of preserving the history of all users and site owners permanently and providing everyone the ability to fork its database, with acceptable overhead. In a regime with substantial censorship, since Infnote does not rely on a single point, it is extremely hard to completely shut down all the Infnote nodes, provided there are sufficient nodes. At the pervasive censorship level, it is impossible to obtain sensitive information from outside of censored regions. However, Infnote could provide a solution to build a P2P information sharing network inside the censored region. In extreme situations, access to the Internet may be disconnected. Although it is impossible for citizens to access the Internet, the infrastructure of the Internet can still be utilized. Every router can establish an internal network, so that as long as nodes are in the same internal network, they can still join the P2P network and send blocks to other nodes. Each smart-phone can be a data trunk that transfers the blocks via different internal networks.

5. DEMONSTRATION PLAN

We will demonstrate a simple discussion forum based on Infnote. Currently, it supports two platforms: web browser and iOS. **Figure 3** and **Figure 5(a)** present the interfaces of the discussion forum containing the basic functions as a discussion forum, such as viewing and posting an article, registering a new user and logging in a existing account. Similarly to bitcoin, a user needs to use his or her private key to log in to the system. On the iOS platform, we are able to provide more functions to the users, such as logging in an account by scanning QR code that contains the private key and saving the private key to the iCloud service.

When the iOS app is running, it automatically becomes a light node that is able to receive and broadcast blocks in real time. **Figure 5(b)** shows the detail of a block which

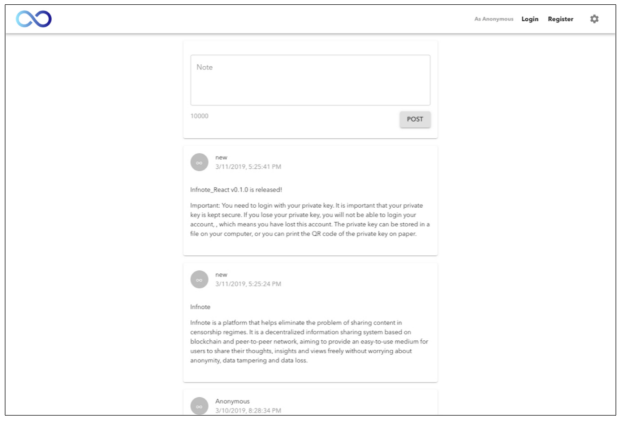


Figure 3: Web interface of a simple discussion forum based on Infnote

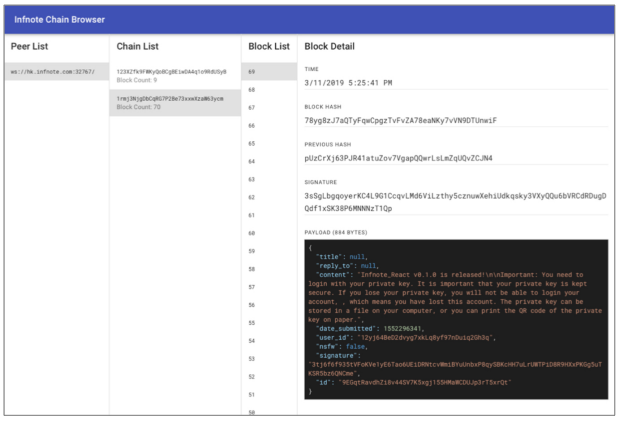
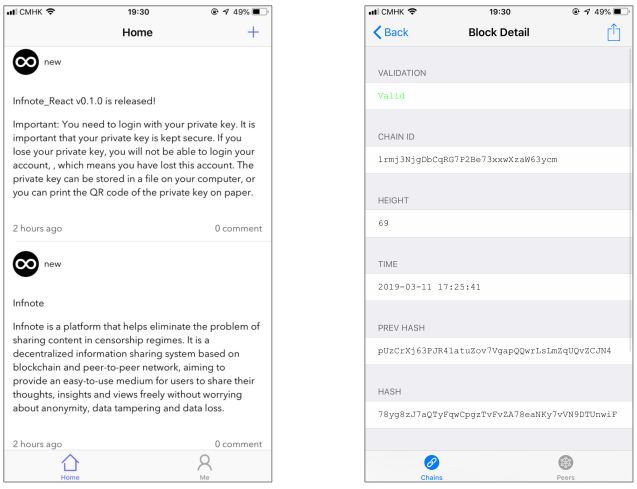


Figure 4: Infnote blockchain browser



(a) Discussion forum (b) Blockchain browser

Figure 5: Infnote App on iOS

has been saved to the local database of the phone. The blocks are also possible to be received and broadcasted by a light node client implemented by JavaScript running in a web browser environment, as displayed in **Figure 4**.

Software for full nodes is implemented using Go, which provide all necessary operations for a full node as a normal user or chain owner. This includes broadcasting and receiving new blocks, creating a new chain or a block, deleting a chain, querying a block in a chain and maintaining a new chain, in the command line environment.

6. RELATED WORK

IPFS [4] and Blockstack [1] are two existing data storage platforms based on blockchain. However, IPFS currently does not support the publish-subscribe pattern, and Blockstack utilizes centralized cloud servers to store data [2]. FreeNet, similar to IPFS, uses a distributed data storage mechanism [5]. However, unpopular files might disappear from the network [8].

7. REFERENCES

[1] M. Ali, J. C. Nelson, R. Shea, and M. J. Freedman. Blockstack: A global naming and storage system secured by blockchains. In *USENIX Annual Technical Conference*, pages 181–194, 2016.

[2] M. Ali, R. Shea, J. Nelson, and M. J. Freedman. Blockstack: A new decentralized internet. *Whitepaper, May*, 2017.

[3] U. G. Assembly. Universal declaration of human rights. *UN General Assembly*, 1948.

[4] J. Benet. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*, 2014.

[5] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong. Freenet: A distributed anonymous information storage and retrieval system. In *Designing privacy enhancing technologies*, pages 46–66. Springer, 2001.

[6] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, et al. On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*, pages 106–125. Springer, 2016.

[7] C. Decker and R. Wattenhofer. Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings*, pages 1–10. IEEE, 2013.

[8] R. Hasan, Z. Anwar, W. Yurcik, L. Brumbaugh, and R. Campbell. A survey of peer-to-peer storage techniques for distributed file systems. In *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on*, volume 2, pages 205–213. IEEE, 2005.

[9] F. House. Freedom on the net 2017. 2017.

[10] F. House. Freedom on the net 2018. 2018.

[11] D. Johnson, A. Menezes, and S. Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1):36–63, 2001.

[12] L. Y. C. Keith Zhai. Chinese metoo student activists use blockchain to fight censors, 2018.

[13] A. Loibl and J. Naab. Namecoin. *namecoin. info*, 2014.

[14] F. PUB. Secure hash standard (shs). *FIPS PUB 180*, 4, 2012.