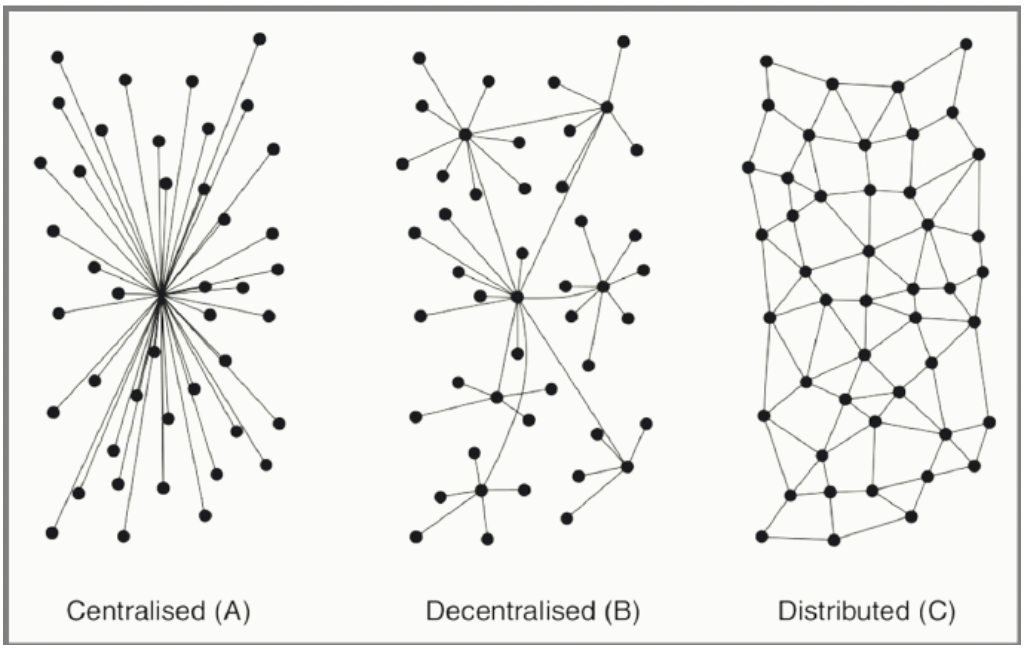
Can peer to peer networks circumvent censorship in authoritarian countries? (2,015 Words)



The difference between Centralised, Decentralised and Distributed networks in abstract terms. (Nguyen et al., 2016)

Contents

Glossary

Word, phrase or abbreviation	Description / Definition
Blockchain	A distributed ledger that is updated through a peer to peer network.
Contact	A person on the network that the user wants to interact with.
Cryptocurrency	A digital currency that is kept on a blockchain
Metadata	Data about data, such as the time and date that a message was sent, who it was sent to / by etc. This doesn't include the data itself.
Node	A single point on a network, in this case a computer or phone.
Super-node	A node that has the ability to see all or a large part of the network at once.
Onion routing	The protocol that is used in the Tor browser to make any user anonymous through its existing peer to peer network.
Peer to Peer Network	A network where each node is equal to another and there is no single point of failure.
ISP	Internet Service Provider
Zero-knowledge proof	A mathematical protocol that allows one party to prove to another that something is true without conveying any further information.
PGP Signature	A method of cryptographically signing a message, allowing anyone to authenticate that a message really came from the sender.

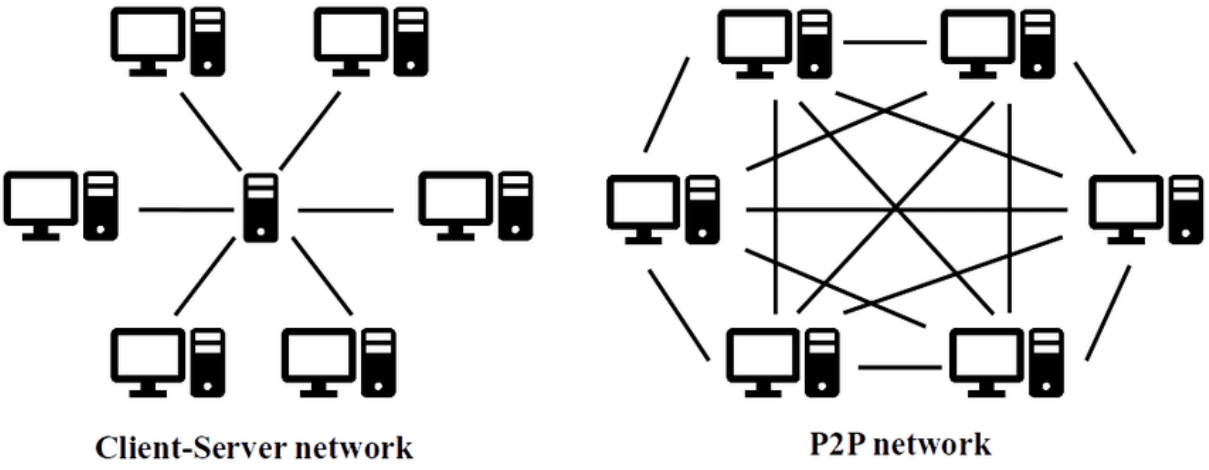
Introduction

Over a billion people around the world live in repressive regimes where they do not have the liberty to speak freely and criticise. Governments now have the ability to shape their people's perception of reality through social media (Ding, 2021).

In order to circumvent such censorship, a peer to peer network; a network that is distributed and exists between individual users, can make it impossible for a government to enforce regulations that govern such speech (Peterson, 2014). If a large proportion of the population is able to access such a network and does so regularly then it becomes impossible to police any speech; especially if posts can be made anonymously and contact between people is indistinguishable from other network traffic.

This report will focus on the anonymity that a peer to peer network can provide as shown in the cryptocurrency networks as well as on platforms such as Mastodon and Diaspora. It will also explore the effect that this may have on authoritarian regimes and their means of control of their population.

The combination of a flat structure peer to peer network with suitable encryption protocols could allow oppressed communities to access otherwise difficult to find news or contact people anonymously.



Client-Server vs Peer to Peer networks (Veeramani, 2019)

How peer to peer networks can provide anonymity

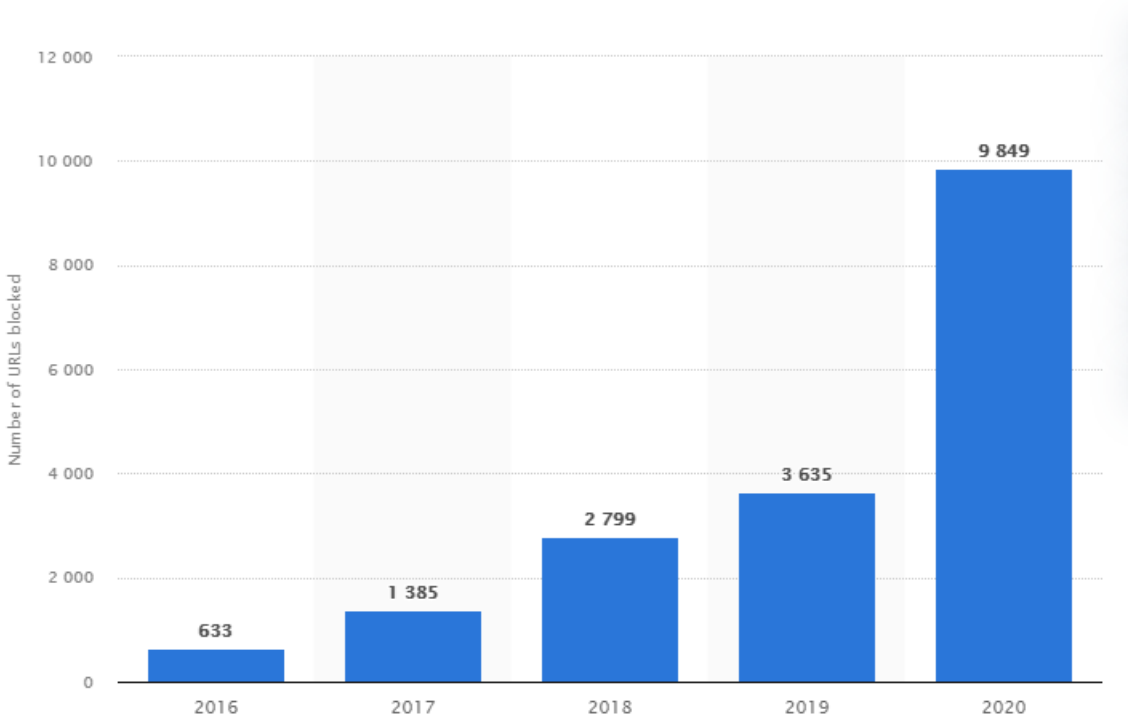
Peer to peer networks can provide any user with anonymity, be it using a protocol such as onion routing, (Reed et al., 1998) for internet browsing, or through zero-knowledge proofs for the purposes of cryptocurrency transactions (Alsalami et al., 2019). This kind of network architecture, if designed in the right way, can avoid the centralisation of power to a single person or entity (Peterson, 2014). This decentralisation makes it much more difficult for anyone to monitor any large part of the network (Piatek et al., 2008) [Appendix 1.1].

While monitoring the whole network might be a challenge, it may still be easy to monitor one node in particular if you know that a certain node is of interest. The obvious solution to this is to encrypt the messages that any person sends to a contact, but this doesn't account for the metadata that comes along with a message. Metadata can often be just as revealing as the messages themselves (Conley, 2014), encrypting the metadata that you share with any particular node only limits the problem. That particular node still needs to know who you're sending that message to; if the node that you're using happens to belong to a government or someone who might be interested in reading your messages, then they still have access to the metadata [Appendix 1.2]. This is another point where zero-knowledge proofs are useful; because the node can find out if they have the contact that you're looking for without gaining the knowledge of who you are or who you're talking to (Alameda, 2020).

The next question might be why this cannot be achieved through a centralised system such as those already employed in services such as WhatsApp, Snapchat or Facebook. The answer lies in who has the control over these services; whoever has control over the central server can decide what kind of protocol to use, what kind of protections should be in place. Even if they do encrypt all of your data, it is still stored in one place for an attacker to find: it also creates a single point of failure where if that one server goes down, then suddenly the whole service is unavailable. Because there is a single, central point of failure, anyone who has control over physical infrastructure such as local network administrators, regional ISPs or national governments can simply block the servers that host a service (Economy, 2018).

The effect that anonymity has on an authoritarian regime's control

Authoritarian regimes use their physical infrastructure to exercise control over their populations (Sloss, 2019), by only allowing services that they can control or by cutting off access to services whenever there is unrest (Statista, 2021).



Number of URLs blocked by Indian Government 2016 - 2020 (Statista, 2021)

One way that a regime might seek to control a population is by monitoring the people that they communicate with and what they communicate about (Karp et al., 2019). If a government cannot find out what someone has said, to whom they have said it or they cannot find out if anything was said at all, then they have no way of controlling the narrative around a subject.

Usually when there is dissent or unrest, it is quashed uncompromisingly by such authoritarian states, while the public narrative is controlled and shaped by them.

"...state dominance enables regimes to put pro-government narratives front and centre while using the power of editorial omission to limit criticism..." (Orttung et al., 2014)

The state media is essential to influence public opinion and any free media organisation is immediately banned, harassed or its functioning made impossible. Therefore, if any form of mass communication is created where it becomes easier to publish stories, pictures or videos without state control; then that platform immediately begins to undermine the state media and government narrative while allowing people to speak freely without repercussions (Wang, 2020) [Appendix D].

One powerful example of how such anonymity can damage state control over the population is the 1989 Tiananmen Square massacre and in particular the iconic image of the "tank man" [Appendix C]. The anonymity of the man who stopped the tanks on the 5th of July that year captured the imagination of the world. Within China not much is known anymore about the protests or the implications of what followed; due to a massive suppression campaign on the part of the Chinese government (Time, 2019). As a result of this campaign not much is known about the man in the picture but it is entirely possible that he was never found or punished due to the anonymity he enjoyed. This shows the power that people can hold in anonymity and how this can be used to fight the power of repressive regimes; that image will be an icon of such movements for decades if not centuries to come.

Conclusion

Throughout the world there are many oppressive regimes that use social media to oppress minorities or their populations as a whole. This report outlines the way that peer to peer networks can be utilised to create a more anonymous kind of social media that makes it easier to circumvent the controls that governments have over the internet. This could be achieved through use of techniques like encryption and zero-knowledge proofs. The report also tries to find what kind of effect that this anonymity might have and how it might allow citizens to subvert state controls and undermine the way that their governments might handle criticism and dissent. A peer to peer network, of the specifications described, might go most of the way to combatting the way that governments control their populations online but it could never eliminate that control completely.

References

Alameda, T. (2020) *Zero Knowledge Proof: how to maintain privacy in a data-based world.* BBVA. Available at: https://www.bbva.com/en/zero-knowledge-proof-how-to-maintain-privacy-in-a-data-based-world/ [Accessed 18 November 2021]

Alsalami, N. and Zhang, B. (2019) *SoK: A systematic study of anonymity in Cryptocurrencies.* IEEE. Available at: https://core.ac.uk/display/266984898 [Accessed 10 November 2021]

BBC (2015) *JeffreySterling's trial by metadata: Free speech stories.* BBC. Available at: https://www.bbc.co.uk/news/blogs-trending-31141256 [Accessed 18 November 2021]

Conley, C.(2014) *Metadata: Piecing together a privacy solution*. ACLU of Northern California. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2573962 [Accessed 11 November 2021]

Ding, J. (2021) *Social Media: Threat to or Tool of Authoritarianism?*. Harvard International Review. Available at: https://hir.harvard.edu/social-media-threat-to-or-tool-of-authoritarianism/ [Accessed 13 October 2021]

Economy, E.C. (2018) *The great firewall of China: Xi Jinping's internet shutdown.* The Guardian. Available at: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown [Accessed 18 November 2021]

Karp, P. and Taylor, J. (2019) *Police made illegal metadata searches and obtained invalid warrants targeting journalists.* The Guardian. Available at: https://www.theguardian.com/australia-news/2019/jul/23/police-made-illegal-metadata-searches-and-obtained-invalid-warrants-targeting-journalists [Accessed 25 November 2021]

Naughton, J. (2018) *How China censors the net: by making sure there's too much information.* The Guardian. Available at: https://www.theguardian.com/commentisfree/2018/jun/16/how-china-censors-internet-information [Accessed 9 December 2021]

Nguyen, T., Upul, J., Tai-Won, U. and Myoung, L.G. (2016) **A survey of Trust in the Internet of things.** *The Journal of Korean Institute of Communications and Information Sciences,* 33, 10-27. Available at: https://www.researchgate.net/publication/316042146_A_Survey_on_Trust_Computation_in_the_Internet_of_Things/citation/download [Accessed 16 December 2021]

Orttung, R. and Walker, C. (2014) *Authoritarian regimes retool their media-control strategy.* Washington Post. Available at: https://www.washingtonpost.com/opinions/authoritarian-regimes-retool-their-media-control-strategy/2014/01/10/5c5bfa6e-7886-11e3-af7f-13bf0e9965f6_story.html [Accessed 25 November 2021]

Peterson, A. (2014) *Using peer-to-peer technology to crowdsource a way around online censorship.* The Washington Post. Available at: https://www.washingtonpost.com/news/the-switch/wp/2014/08/21/using-peer-to-peer-technology-to-crowdsource-a-way-around-online-censorship/ [Accessed 13 October 2021]

Piatek, M., Kohno T. and Krishnamurthy A. (2008) *Challenges and directions for monitoring P2P file sharing networks-or: Why my printer received a DMCA Takedown Notice.* Association for Computing Machinery. Available at: https://dl.acm.org/doi/10.5555/1496671.1496683 [Accessed 11 November 2021]

Qureshi, H. (2019) *Bitcoin's P2P Network.* Nakamoto. Available at: https://nakamoto.com/bitcoins-p2p-network/ [Accessed 15 December 2021]

Reed, M.G., Syverson, P.F. and Goldschlag, D.M. (1998) **Anonymous connections and onion routing.** *IEEE Journal on selected areas in communications,* 16, (4) 482-494. Available at: https://ieeexplore.ieee.org/abstract/document/668972 [Accessed 10 November 2021]

Sloss, D.L. (2019) *Weaponization of social media by authoritarian states.* Markkula Center for applied ethics at Santa Clara University. Available at: https://www.scu.edu/ethics-spotlight/social-media-and-democracy/weaponization-of-social-media-by-authoritarian-states/ [Accessed 24 november 2021]

Statista (2021) *Number of URLs blocked by the Indian government on social media platforms from 2016 to 2020.* Statista. Available at: https://www.statista.com/statistics/1102154/india-urls-blocked-on-social-media-by-government/ [Accessed 11 November 2021]

Time (2019) *'I've been told lies.' Young Chinese Recall When They First Learned of Tiananmen.* Time. Available at: https://time.com/5600385/tiananmen-june-4-1989-china-30th-anniversary-censorship/ [Accessed 2 December 2021]

Veeramani, K. and Jaganathan, S. (2019) **A quick synopsis of blockchain technology.** *International Journal of Blockchains and Cryptocurrencies,* 1, (1) 54. Available at: https://www.researchgate.net/publication/335480185_A_quick_synopsis_of_blockchain_technology [Accessed 15 December 2021]

Wang, Y. (2020) *In China, the 'Great Firewall' Is Changing a Generation.* Politico. Available at: https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385 [Accessed 15 December 2021]

Appendix

1.1	While decentralisation is an effective way to make large scale monitoring of a network difficult, it is not impossible. It would however be helped if there was also a protocol to establish how many connections a given node might have and therefore, be able to terminate any node from the network if it has more connections than allowed.
1.2	Today even your metadata can, independently from the data itself, be enough to convict you of a crime (BBC, 2015).
1.3	In July of 1989 a massive student protest was organised at Tiananmen Square. Eventually the government cracked down on the protests by sending in Army troops on the night of 3 / 4th who began shooting protesters. The next day a man walking in the road decided to stand in front of, and thereby block, a convoy of tanks who did nothing in response, creating a now infamous image (BBC, 2019).
1.4	Interestingly in an article in the Guardian, John Naughton, professor of Public Understanding at the Open University, suggests that there are 3 ways that China censors on the internet (Naughton, 2018). The first 2; fear and friction, we have already managed to circumvent using anonymity and the distributed nature of our hypothetical network. The third however remains elusive: flooding - when an actor uses many different false stories or narratives to make it difficult to identify the truth. This tactic is most effectively used by the Russian state on social media but can also be applied in other places. Obviously there are easy ways to overcome bots on our network but finding ways to stop malicious actors in humans is more difficult. One way might be to add a community verification function like the "verified" check mark used by centralised social media, perhaps also using something along the lines of PGP signatures.

1.5	The Dandelion Protocol is a way for a peer to peer network to increase anonymity, essentially it splits the propagation of any message into 2 phases: the stem phase and the fluff phase, making the resulting diagram look like a dandelion. In the stem phase, the message is passed only onto one other node at a time making a long line, none of these nodes know how many nodes have come before it so it's impossible to know who sent the message. Then, at the end of the stem a node begins passing it to more nodes at the same time, allowing the message to propagate through the network (Qureshi, 2019).