Analyzing Soft and Hard Partitions of Global-Scale Blockchain Systems

Kevin Bruhwiler
University of California, Irvine, CA, USA

Fayzah Alshammari
University of California, Irvine, CA, USA

Farzad Habibi
University of California, Irvine, CA, USA

Juncheng Fang
University of California, Irvine, CA, USA

Faisal Nawab
University of California, Irvine, CA, USA

Abstract

Partitioning attacks have been a known threat since the invention of cryptocurrencies. Attackers could deliberately fork the chain by re-routing network traffic into two or more separate chains and spend money on each piece, effectively spending multiples of their money. Apostolaki et. al. [1] were among the first to quantify the threats of such attacks on Bitcoin. They suggest a number of ways to mitigate this risk which were combined into a tool named SABRE.

Jyothi explored the possibility that a solar superstorm could damage the undersea fiber-optic cables that connect the Internets of different continents, and considered the mostly likely ramifications of the damage. She concluded that such an event would likely cause major connectivity issues across the northern hemisphere and may disconnect much of North America's internet from the eastern hemisphere for weeks. There is also concern that undersea cables could be deliberately destroyed as acts of terrorism or war or by natural disasters such as earthquakes.

In this work, we construct a simulation to properly quantify the effects of a global-scale network partition on the blockchain. We hope to provide the groundwork for preventative measures to be taken to minimize the harm that such partitions might cause in the future. We do this by modifying SimBlock [2], a blockchain simulator created to study the effect of different network topologies, to allow initiating and recovering from partitions and also add metrics to capture their effects.

To quantify the severity of partitions we use a number of metrics, including the rate of agreement improvement after a new block has been minted and the average rate of block propagation across regions. We also examine the number of forks in the blockchain that result from partitions and identify the break-points at which forks begin to appear. Finally, we quantify the duration that partitions of various sizes can persist before they begin to generate forks and measure the how long it takes for the system to recover once the partition has been resolved.

2012 ACM Subject Classification Computer systems organization → Reliability; Computer systems organization → Peer-to-peer architectures

Keywords and phrases Blockchain, Partitioning, Resilience, Simulation

Digital Object Identifier 10.4230/OASIcs.FAB.2022.7

Category Poster

References

1 Apostolaki, Maria Aviv, Zohar and Laurent Vanbever. Hijacking bitcoin: Routing attacks on cryptocurrencies. *IEEE Symposium on Security and Privacy (SP). IEEE*, 2017.

2 Yusuke, Aoki et al. Simblock: A blockchain network simulator. *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE*, 2019.