Redbelly Announces World's First Verified Consensus Protocol

The Australian-made blockchain has become the first blockchain in history to have its Consensus Protocol – the heart of blockchain security – formally verified, as its work on accountability wins global acclaim.

28 July, 2022 (Sydney): Redbelly Network, the Australian blockchain ecosystem, announced today at the ACM Symposium on Principles of Distributed Computing (PODC) in Italy that it had become the first blockchain to have its Consensus Protocol fully formally verified.

The most complex component of the blockchain software, the Consensus Protocol is also the most vulnerable and is the entry point for successful cyber attacks against blockchains that have been made in the past. Redbelly runs a unique consensus protocol – the Democratic Byzantine Consensus Protocol – that prevents forking, and these types of attacks.

Several attempts have historically been made to verify blockchain consensus, said Redbelly CTO Vincent Gramoli, but they were incomplete. "The model checking of blockchain consensus has never been fully achieved before, because those attempts could not model check the entire protocol, or could only verify that the protocol works with a specific number of machines," he said. "This is due to the complex nature of the mathematical representation derived from consensus protocols that requires too many computing resources to be verified."

Redbelly was able to solve these issues by using a new method that breaks down the formal verification process with a model that allows verification with any number of participants, and despite less than a third of malicious participants within the ecosystem. [The research,](#) resulting from a long-term scientific collaboration with researchers from Australia, Austria, France, Germany and USA, was presented to global peers at PODC today.

Entitled "Holistic Verification of Blockchain Consensus" this work is an important milestone in cybersecurity and for blockchain technologies in particular. It promises to drastically reduce the amount of human errors that are too common in blockchains and that hackers exploit regularly to steal assets. This is particularly relevant to use-cases where the assets are of high value.

Gramoli has also won international acclaim for his work on accountability – one of the key differentiators between Redbelly and other blockchains. Two of his papers on this topic have been awarded Best Paper at important conferences in June and July this year. ''[Crime and Punishments in Distributed Decision Tasks](#)'' by Gramoli and a team of researchers won Best Paper Award at the IEEE International Conference on Distributed Computing Systems in Bologna, Italy in July. This followed an award for Best Paper for "[As easy as ABC: Optimal (A)ccountable (B)yzantine (C)onsensus is easy!](#)" at the IEEE International Parallel and Distributed Processing Symposium in Lyon, France in June.

For interviews with Vincent Gramoli:
Kristin Westlake | kwestlake@thecontinuumpartners.com | +61 416 219 358