Research project aims to make the blockchain faster and more sustainable

October 28 2022

Credit: Pixabay/CC0 Public Domain

At the Technical University of Munich (TUM), an interdisciplinary research team made up of experts from the fields of informatics, electrical engineering and management science will work to make

blockchain technology significantly faster and prepare it for entirely new applications. In this interview Prof. Georg Carle explains the ACE SUPPRA project.

The term blockchain describes a number of methods to create a decentralized database. Information is incrementally added to this database in units known as blocks. In a cryptocurrency, for example, they contain information on transactions. The list cannot be altered. The accuracy of the information in a new block is not verified by a central unit which the other units must trust.

Instead, a distributed consensus mechanism among computers that do not need to trust each other determines which information is entered into the block and which of the participating units may add the block. The enormous energy costs caused by the cryptocurrency bitcoin relate to its proof-of-work consensus mechanism. Modern blockchain processes use consensus methods that require much less energy.

Prof. Carle, ACE SUPPRA, a new, large-scale research project on blockchain, is starting at TUM. What do you hope to achieve?

In short, we want to make blockchain technology faster, more robust and more sustainable. We have put together an interdisciplinary team from five research chairs at TUM who have already done intensive work in this area. Blockchain technology is known primarily through cryptocurrencies. But it is, in fact, a tool that is suitable for many different tasks. Our goal is to eliminate the weaknesses of this tool in order to make even more blockchain applications possible.

What are the disadvantages of current blockchain technologies?

For example, there is the lack of speed: many well-known blockchain systems, including Bitcoin, work with a probabilistic consensus mechanism. It takes quite some time for a block to become part of the valid blockchain. In the case of a cryptocurrency this means that, once a block is generated—which takes an average of 10 minutes with Bitcoin—a transaction is not finalized until consensus is reached that the block is actually part of the valid blockchain. That can take as long as an hour.

Does it have to take that long?

With modern blockchains, finality of just a few seconds is achievable. That means that it is only a matter of seconds until consensus is reached on the new block and the numerous transactions it verifies. But for some applications, that is still not good enough: for high-frequency trading on stock exchanges, significantly faster speeds would be needed. The same applies in interactive applications and for uses of [blockchain technology](#) in cyber-physical systems.

Does that mean that blockchain technology might be used in networked cars, for example?

If it has real-time capability, yes—and those are the speeds that we will be working on in our project. For example, if you turn the various components of a car into actors in a blockchain network, you could make precise and reliable statements on exactly which components have malfunctioned in case of a breakdown and when. Taking that idea further, it could be applied to multiple networked cars to record tamper-proof evidence of the events leading to an accident using data from various sensors.

What are your goals in the ACE SUPPRA project?

We're taking an interdisciplinary approach. Blockchain technology is complex and there are countless points where it can be tinkered with. This includes the consensus algorithms themselves, but also underlaying mechanisms for the communication among the involved computers. For example Andreas Herkersdorf, the head of the Chair of Integrated Systems, and his team will be doing research on a hardware acceleration for certain blockchain mechanisms on co-processors that can achieve the necessary speeds and also have built-in security mechanisms.

And you will be combining that with the actual blockchain code?

Exactly. My work group will bring together the progress made with the hardware acceleration with advances on consensus protocols. An important priority will be to make privacy protection an integral part of the system and to demonstrate this with reproducible experiments.

What aspects of blockchain will you be addressing apart from speed?

We're very interested in the ways that people can interact with blockchain. There is a lot of potential in that area, too: Alexander Pretschner Professor of Software and Systems Engineering, is working on smart contracts, a very interesting feature of blockchain. He wants to make these automated "contracts" verifiably reliable and available for use in complex applications. Florian Matthes, who holds the chair Software Engineering for Business Information Systems, will investigate the use of blockchains for certain application cases. Among other things, he is interested in how the right incentives can be created for collaboration in the blockchain and where there is potential for abuse. Isabell Welpe, Professor of Strategy and Organization at the TUM School of Management, will study a related aspect: She will explore

governance, in other words the rules that must be put in place in order to achieve pre-defined objectives through the use of a blockchain and how such rules can be built into the code.

Provided by Technical University Munich