A New Generation of Services and Applications Based on the Bitcoin Infrastructure

Contact:
Prof. Roman Vitenberg (romanvi@ifi.uio.no), Prof. Frank Eliassen (frank@ifi.uio.no)

Motivation and background:
Bitcoin is a widely successful implementation of digital currency. As of February 2017, the total value of all bitcoins in circulation exceeds 16 billion US dollars, with millions of dollars worth of bitcoins exchanged daily[1]. It is accepted by such reputable merchants as PayPal, Expedia, and many others. The basic technological principles behind Bitcoin have been adopted by Microsoft[2] and IBM[3] in their financial products and offerings. The widespread success of Bitcoin has also elicited significant interest among startups and enterprises in Norway.

What makes Bitcoin unique is that the implementation is entirely distributed, without any centralized authority that would inject the money or issue digital certificates. In a nutshell, it is based on a secure mechanism for distributed transactions in a decentralized P2P network. Information about transactions is stored in a transactional ledger, which is globally replicated across all the nodes in the system. The P2P network helps to protect the ledger against tampering, as long as no adversary can gain control over a majority of the nodes.

This unique distributed solution that does not require centralized authority has facilitated a vision of new applications based on similar principles. Bitcoin has facilitated crowdfunding, which is a form of alternative financing that allows funding a project or venture by raising monetary contributions from a large number of people. In particular, Bitcoin has been used to crowdfund Greenpeace, the Mozilla Foundation, the Wikimedia Foundation, and WikiLeaks. Furthermore, there are promising efforts towards a globally accepted certificate verification system. Recently, some universities[4] have begun experiments issuing degree certificates that are recorded in the publicly available transaction ledger.

Main objective and summary:
Extend the functionality of the existing Bitcoin infrastructure, scale it up, and design new applications that provide certified transactions without centralized authority.

Scientific challenges:

- How to reuse the same infrastructure for applications with different semantics and consistency requirements? How to scale the infrastructure with the number of different applications?

---

[1] https://bitcoincharts.com/bitcoin/

[2] https://azure.microsoft.com/en-us/blog/ethereum-blockchain-as-a-service-now-on-azure/

[3] http://www.coindesk.com/ibm-goes-big-on-blockchain-unveiling-ambitious-new-service-offerings-and-strategy/

[4] http://www.coindesk.com/university-nicosia-issues-block-chain-verified-certificates/

- As the rate of transaction ever increases, how can we scale both processing and storage of transactions?
- Can we reduce energy consumption by Bitcoin or propose innovative Bitcoin-enabled consumer-oriented energy services?
- How can we improve mechanisms for construction and maintenance of the P2P network as well as communication protocols exploiting it?
- The current Bitcoin implementation does not focus on confidentiality or privacy of participants. Improving identity protection is an open problem.

The PhD student is not expected to address all the challenges listed above. However, a successful student should be able make substantial progress on several of these topics.

What we offer in a nutshell

- A strong research environment. Our students have won best paper and best demo awards[5] at several conferences. Our alumni are employed by IBM Research, Microsoft, Spotify, and highly reputable academic institutions in Europe.
- The group of Networks and Distributed Systems[6] offers a work environment that is well equipped with the newest hard- and software technology. The research group has tight bonds with Simula Research Laboratory. Furthermore, we have well-established links to national and international research institutions. We conduct collaborative research projects that are funded by Norwegian research funds, and the European Community.
- Highly relevant for the prioritized initiatives at the department such as the Strategic Research Initiative for Concurrent Security and Robustness of Networked Systems (Conserns)[7]**.**
- Opportunities for research stays with our renowned collaborators worldwide, including University of Toronto, TU Munich, and UC Irvine.
- Well-paid PhD positions, in a country which has been ranked by the UN as having the highest standard of living in the world, and which is known for its unique scenic beauty. The work is in a smart futuristic building that has won multiple awards.

Suitable Background and Requirements:

- Applicants must have a degree in Computer Science, or in a related study, with excellent results. They must also be able to demonstrate interest in scientific research. The evaluation considers many aspects of excellence, as well as the personal drive and organizational skills. The ideal candidate for the position will have strong background in distributed computing.
- You may apply if you have not yet completed your degree, but expect to do so before the position starts.
- Knowledge of Norwegian is not a prerequisite for application. English is our working language for research.

---

[5] http://www.mn.uio.no/ifi/om/aktuelt/utmerkelser/acm-debs-poster-award-2014.html

[6] http://www.mn.uio.no/ifi/english/research/groups/nd/index.html

[7] http://www.mn.uio.no/ifi/english/research/groups/conserns/