Beyond Bitcoin

Bitcoin is a system that is known to work in practice better than in theory, and researchers especially have trouble explaining how the consensus is reached/works. Nevertheless, it would still be very useful to develop the theory behind it completely, which could help predict what kind of future is expected from bitcoin, it's stability, development options and even help alt coins.

Scaling - One of the main limitations of bitcoin is transaction rate, which is currently at maximum of 7 transactions per second. There are many factors that lead to this, mostly artificial limits/values such as 1 block / 10 minutes boundary, but this is all subject to change, except it is not that easy. Changing bitcoins system would at least require a soft fork, in many cases a hard fork or complete redesign.

Because of the nature of distributed system and the fact that transactions/verifications need to propagate through the network, it is a limiting factor, a bottleneck for current bitcoin and there is no obvious solution. Delays can be decreased but we need to be very careful when redesigning such protocols as they might threaten the security of the system, which is essential for its existence.