Summary Scaling Blockchain Alexander Wandrup

Side chains:

Implementations of altcoins in bitcoin is hard. In blockchains like zerocash coins are minted by putting a basecoin in an escrow. We can then burn the zerocash later to get the basecoin back. In bitcoin this is not possible because bitcoin transactions can not depend on events from other blockchains. It’s there we get idea to soft-fork different chains and that's where sidechains come from. The simplest way to extend Bitcoin to allow for converting coins from a sidechain back to bitcoin is to encode all of the sidechains rules into bitcoin. That includes validating all of the sidechain’s transaction and checking it’s proof of work. This is impractical as this would require too complex.

SPV trick:

A way to avoid having to encode is to use “SPV(Simplified Payment Verification) proofs”.
SPV nodes don’t validate transactions, they just make sure that the transactions they care about is in the longest branch. Then we can add an instruction to bitcoin that verifies proofs that a transaction of for example a burned coin happens on the sidechain.

This is a better solution than the last one but it still have the problem of havving to much happen on bitcoins side. Instead we want a transaction that tries to convert coins back to bitcoin contain all information bitcoin needs in order to verify that the transaction that happened on a sidechain actually happened.