1. BITCOIN

Introduced in 2009 in [6] bitcoin is one of the first decentralized currency. It’s called crypto-currency, since it uses cryptography to secure transactions and assets. Bitcoin operation is based on so-called public ledgers that can be shortly described as follows.

Assume there are two parties Alice and Bob (as usual), such that Alice wants to buy something from Bob. Assume they both have wallets that are public. That is, we can trace transactions from one person to another. Let say that both Alice and Bob have 10฿ on their accounts. So, if Alice has to pay Bob 4฿ we know that Alice’s balance is 6฿ and Bob’s is 14฿ and everyone knows that now Bob can spend all his 14฿.

Since the information about wallets are public, money transfer can be reduced to Alice publicly announcing "I, Alice, pay Bob 4฿.". However, because of various technical reasons, we need to aggregate such claims for the whole network. That is, if in the similar time there are other transactions than that between Alice and Bob, they should be taken together and confirmed. How this confirmation should be done is a major open problem in almost all modern crypto-currencies.

**Project 1: Proof-of-work, revisited.** The original proposal by [6] forces parties who want to confirm they transactions to perform huge (and useless) computation. Precisely, they need to find a preimage x of a hash function h such that h(x) < t, for some target t. Since the number of bitcoin users grows and computers are becoming more and more powerful, this target value t should be adjusted to the changing environment. Designing a mechanism that computes t securely is not an easy task. A paper by Garay et al. [3] from the recent Crypto conference deals with this problem.

**Task:** Read, understand and present the paper [3].

**Project 2: Proof-of-stake.** As said above, the problem with proof-of-work is that work that is needed to confirm transactions is usually useless. Thus, Kiayias et al. [5] shown an alternative – proof-of-stake. They proposed that a single party should be picked from the parties participating in transfers to confirm the whole block of transactions. They also shown a mechanism to decide which party to choose.

**Task:** Read, understand and present the paper [5].

**Project 3: Proof-of-space.** Another alternative to proof-of-work was presented by Dziembowski et al. [2]. They proposed that instead of computational power, parties show they have disk space at their disposal.

**Task:** Read, understand and present the paper [2].

**Project 4: How not to wait long.** One of the biggest problem connected to using blockchains is long waiting time between transaction commitments. This means that Alice who paid Bob for some goods need to wait for, e.g. half an hour before Bob is convinced he received the payment. Thus, using bitcoin in everyday operations needs some workaround. Recently, Dziembowski et al. [1] proposed such a workaround.

**Task:** Read, understand and present the paper [1].

2. SUCCINCT NON-INTERACTIVE ARGUMENTS

Zero knowledge. Let L be an NP language. Let Alice knows an instance, witness pair (x, w) such that x ∈ L.
It has been shown that Alice can create a proof π for a statement “x ∈ L” such that:

1. Bob can verify π and if the verification passes, he is convinced that x ∈ L.
2. Bob learns nothing about the witness w from π.
3. Alice cannot convince Bob that x′ ∈ L if it is not a case.

We call such proof succinct if π is short. It is non-interactive since Bob does not need to send any message to Alice, he just needs to get a single message π.

Falsifiable assumption.

We call an assumption falsifiable if it is possible to conceive of an observation or an argument which could negate it. For example, the universal generalisation that All swans are white is falsifiable since it is logically possible to falsify it by observing a single black swan.

Thus, the term falsifiability is sometimes synonymous to testability.

(from Wikipedia)
Project 5: Impossibility of SNARGs. Unfortunately, Gentry et al. [4] shown that no SNARGs are possible under falsifiable assumptions.

Task: Read, understand and present the paper [4].

DISCLAIMER
I won’t be able to supervise more than 4 projects. First come, first served.

REFERENCES