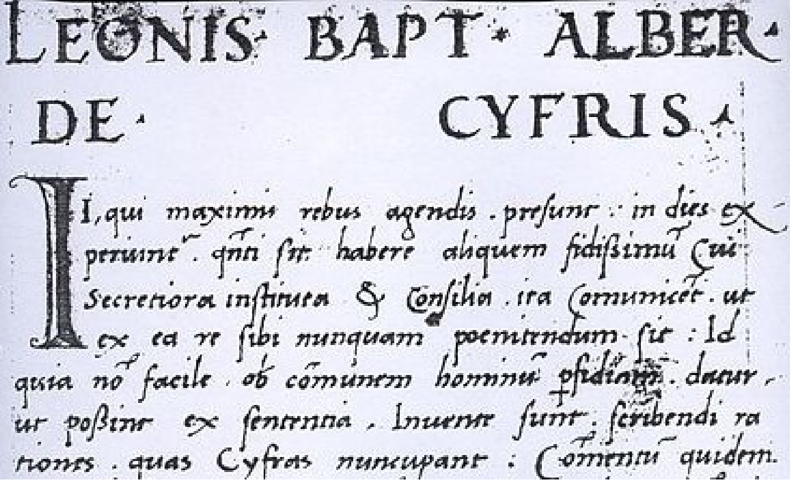

LEONIS BAPT· ALBER·
DE· CYFRIS·

I, qui maximis rebus agendis præsunt: in dies experiunt. quanti sit habere aliquem fidissimu cui Secretiora instituta & Consilia. ita comunicet. ut ex ea re sibi nunquam poenitendum sit: Id quia no facile. ob comunem hominu pfidiam. datur, ut poſsint ex sententia. Inventi sunt, scribendi rationes. quas Cyfras nuncupant: Comentu quidem.

De Cifris Augustae Taurinorum

Thursday, 16 May 2019 – at 14.30
Aula Buzano, Politecnico di Torino

Fabio Fiori
Quadrans

Distributed consensus algorithm, a novel approach

Abstract: A blockchain is a decentralized peer-to-peer system with no central authority. In these kind of systems is mandatory to avoid any corruption from a single source. Since a blockchain has no "leader", to make decisions they need to come to a consensus using some kind of "consensus mechanism". In example, Bitcoin uses a Proof-of-Work (PoW) based on the SHA-256 algorithm to reach the consensus. This seminar focuses on what consesus is and how is reached on the main blockchains, analyzing some examples of PoW, Proof-of-Stake (PoS) and comparing each others. In particular, we will focus on Hashcash and some alternatives for the PoW and the various alternatives of PoS used in different cryptocurrencies. At the end, the focus will be on a novel approach for a PoW algorithm, based on mathematics problems like Discrete Logarithm Problem in the group defined by an elliptic curve over a finite field. This work comes from a research collaboration with the CryptoLabTN at the University of Trento.

For Information: fabio.fiori@food-chain.it, guglielmo.morgari@telsy.it, nadir.murru@polito.it, lea.terracini@unito.it.

CONTATTI
Associazione De Componendis Cifris
direttore@decifris.it, segreteria@decifris.it