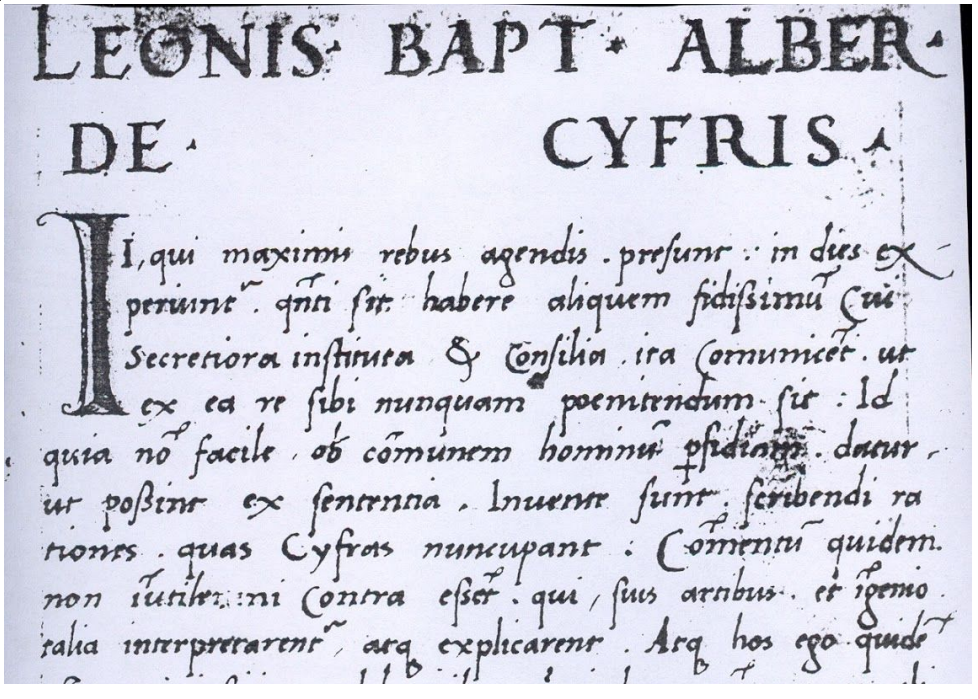
LEONIS BAPT. ALBER-
DE CYFRIS

II, qui maximis rebus agendis . presunt : in dies ex-
periunt . quã sit habere aliquem fidissimũ cui
Secretiora instituta & Consilia ita Communicet . ut
ex ea re sibi nunquam poeniteadum sit : Id
quia nõ facile . ob cõmunem hominũ pfidiam . datur
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentu quidem
non iutilem Contra esset . qui , suis armis . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

FONDAZIONE BRUNO KESSLER
ICT CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY

Wednesday 27th November 2019 – at 12:00 a.m.
University of Trento
Room 203, "Polo Ferrari" - Povo 1 - *Via Sommarive, 5*

MATTEO BONINI
Politecnico di Milano

Analisi sulla De-anonimizzazione di blockchain

Abstract: Le criptovalute registrano le transazioni in un registro pubblico distribuito chiamato blockchain, esponendo al pubblico tutta la loro storia delle transazioni. Le transazioni Bitcoin, in particolare, sono state accuratamente studiate, e hanno dimostrato di essere vulnerabili alla de-anonimizzazione sia attraverso uno studio del grafo delle transazioni sia attraverso attacchi side-channel.

Negli ultimi anni, sono state create altre criptovalute, che sostengono di fornire maggiore garanzie di sicurezza (e per questo chiamate generalmente privacy coins).

In questo seminario verrà presentata una panoramica delle proposte per migliorare le garanzie di anonimato delle criptovalute e dei possibili attacchi alle loro blockchain. In particolare ci si concentrerà ai casi di studio fatti su Bitcoin, Zcash e Monero (e a tutte le valute con blockchain affini a queste).

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it