

MSc thesis defense presentation

Aikaterini-Panagiota Stouka defends his MSc thesis

Date:	Wednesday, 06 May 2015
Time:	12:00
Location:	School of Electrical and Computer Engineering (old buildings), 1.1.31 Smart contracts and
Thesis title:	Payments using Bitcoin and Ethereum
Committee:	<ul style="list-style-type: none">• Aggelos Kiayias• Aristeidis T. Pagourtzis• Efstathios Zachos

Thesis abstract

This Thesis focuses on Bitcoin ,a digital currency, which was proposed by Satoshi Nakamoto [3] in 2008 . We describe both its function and its security [1],[2]. Bitcoin is a cryptocurrency, which is decentralized, as there is not any trusted authority that mints coins or controls transactions. Consequently, we describe some smart contracts [12], which use Bitcoin to solve problems of trust. In addition, we study a construction (and its security) , Zerocoin [22], which can be implemented in Bitcoin in order to achieve anonymity (it was proposed by Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin in 2013) ,as well as a dynamic accumulator published by J. Camenisch and A. Lysyanskaya [23] that is used in the above construction . Finally, we analyze Ethereum 's function .Ethereum is a decentralized system that uses a Turing complete language in order to make the contract creation easier and was proposed by Vitalik Buterin and Gavin Wood [20],[21] in 2013- 2014.

Download date: 2019-09-19, 03:35.