CBT

WORKSHOP

(VERSION 20180828)

Program at a glance

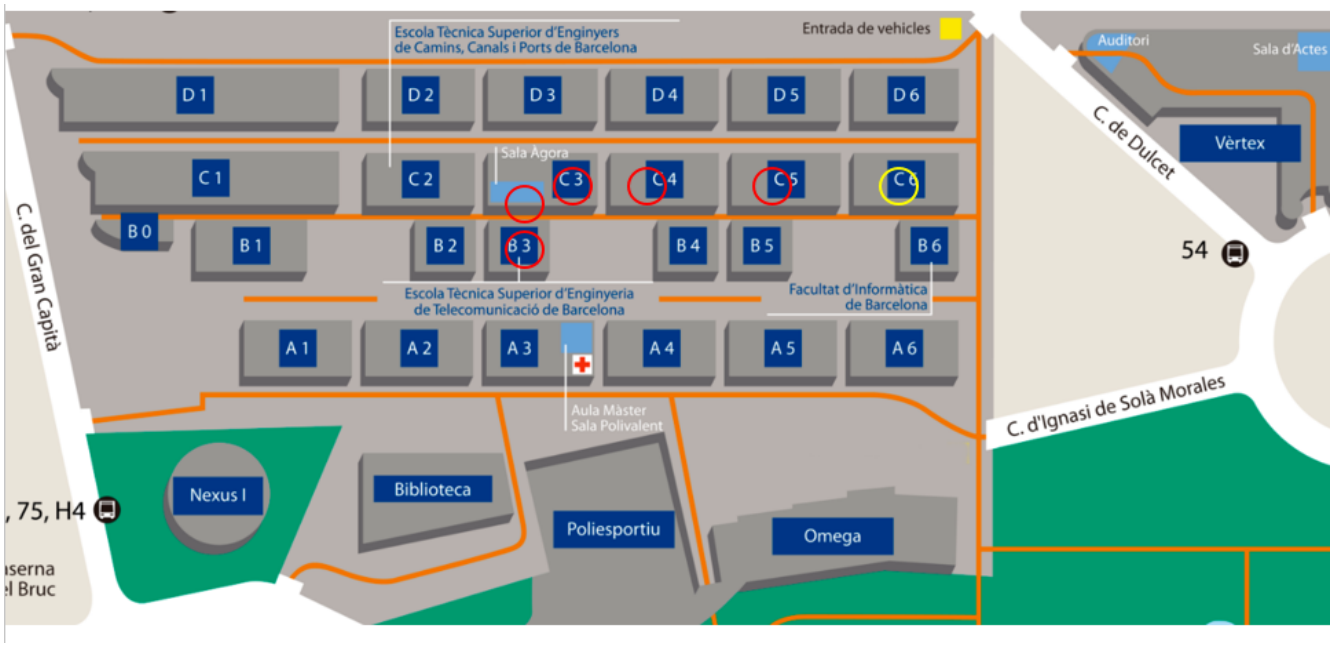
Thursday, September 6, 2018

Workshop	CBT	CSITS	CyberICPS-SECPRE	DPM	PADG-SIoT	STM
08:30 - 08:45	Registration	Registration	Registration	Registration	Registration	Registration
08:45 - 09:00	Registration	Welcome Room C5		Registration	Welcome Room C5	Registration
09:00 - 10:00	Welcome & Keynote Room Agora	Session 1 Room C5		Welcome & Keynote Room Agora	Session 1 Room C4	Welcome & Keynote Room Agora
10:00 - 10:30						
10:30 - 11:00	Coffee Break	Coffee Break		Coffee Break		Coffee Break
11:00 - 11:30	Session 1 Room Agora	Keynote & Session 2		Session 1 Room C3	Coffee Break	
11:30 - 12:00					Session 2 Room C4	Session 1 Room B3
12:00 - 12:30		Room C5				
12:30 - 13:30	Lunch Break	Farewell Lunch	Lunch	Lunch Break	Lunch Break	Lunch Break
13:30 - 14:00			Welcome Room C5			
14:00 - 14:30	Session 2 Room Agora		Session 1 Room C5	Session 2 Room C3	Keynote Room: C4	
14:30 - 15:00						Session 2 Room B3
15:00 - 15:30					& Session 3	
15:30 - 16:00	Coffee Break		Coffee Break	Coffee Break	Coffee Break	Coffee Break
16:00 - 16:30	Session 3 Room Agora		Session 2 Room C5	Session 3 Room C3	Session 4 Room C4	ERCIM STM PhD Award Talk Room B3
16:30 - 17:00						
17:00 - 17:30						
17:30 - 18:00						
18:00 - 18:30						
18:30 - 19:00						
19:00 - 20:00	Social Activity	Social Activity	Social Activity	Social Activity	Social Activity	Social Activity
20:00 - 21:00						
21:00 - 22:00	Gala Dinner	Gala Dinner	Gala Dinner	Gala Dinner	Gala Dinner	Gala Dinner
22:00 - 23:00						

Friday, September 7, 2018

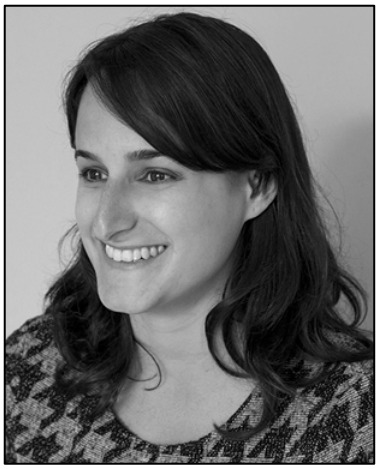
Workshop	CBT	CyberICPS-SECPRE	DPM	ETAA	ISSA	STM
08:30 - 08:45	Registration	Registration	Registration	Registration	Registration	Registration
08:45 - 09:00	Registration	Registration	Registration	Registration	Registration	Registration
09:00 - 09:30	Session 4 Room Agora	Session 3	Session 4 Room C3	Welcome	Welcome & Keynote Room C4	Registration
09:30 - 10:00				& Session 1 Room C6		Session 4 Room B3
10:00 - 10:30		& Keynote Room C5			Coffee Break	
10:30 - 11:00	Coffee Break		Coffee Break	Coffee Break	Session 2 Room C4	Coffee Break
11:00 - 11:30	Session 5 Room Agora	Coffee Break	Session 5 Room C3	Session 2 Room C6		
11:30 - 12:15		Session 4 Room C5				Session 5 Room B3
12:15 - 12:30					Round Table Room C4	
12:30 - 13:00	Farewell Lunch		Farewell Lunch	Lunch Break		Farewell Lunch
13:00 - 13:45		Farewell Lunch			Farewell Lunch	
13:45 - 14:00				Session 3 & Farewell Room C6		
14:00 - 15:00						
15:00 - 15:15						
15:15 - 16:00						
16:00 - 17:30						
17:30 - 18:00						

Rooms



Keynote Speaker

Sarah Meiklejohn



University College London
Gower St, Bloomsbury, London, UK

Title: Anonymity in Cryptocurrencies
Date: Thursday, September 6, 2018
Hour: 09:30
Room: Agora
Workshops: CBT, DPM, STM

Abstract

A long line of recent research has demonstrated that existing cryptocurrencies often do not achieve the level of anonymity that users might expect they do, while at the same time another line of research has worked to increase the level of anonymity by adding new features to existing cryptocurrencies or creating entirely new cryptocurrencies. This talk will explore both of these lines of research, demonstrating both de-anonymization attacks and techniques for anonymity that achieve provably secure guarantees.

Short Biography

Sarah Meiklejohn is Reader (Associate Professor) in Cryptography and Security at UCL, in the Computer Science department. I am affiliated with the Information Security Group, and am also a member of the Open Music Initiative and the Initiative for Cryptocurrencies and Contracts (IC3). Before joining UCL, she received a PhD in Computer Science from the University of California, San Diego under the joint supervision of Mihir Bellare and Stefan Savage. During her PhD, she spent the summers of 2011 and 2013 at MSR Redmond, working in the cryptography group with Melissa Chase. She obtained an Sc.M. in Computer Science from Brown University under the guidance of Anna Lysyanskaya in 2009, and an Sc.B. in Mathematics from Brown University in 2008.

CBT: Cryptocurrencies and Blockchain Technology

Thursday, September 6, 2018

08:45 – 09:00

Registration

09:00 – 10:30

Room: Agora
General Welcome & Invited Talk
Chairs: Jordi Herrera-Joancomarti & Joaquin Garcia-Alfaro
Invited Talk Title: *Anonymity in Cryptocurrencies*
Speaker: Sarah Meiklejohn

10:30 – 11:00

Coffee Break

11:00 – 12:30

Session 1: Privacy, logics, and computational models

Room: Agora
Chair: Guillermo Navarro-Arribas

11:00-11:30 **- Succinctly Verifiable Sealed-Bid Auction Smart Contract**
By Hisham Galal and Amr Youssef (Concordia University, Canada)

The recently growing tokenization process of digital and physical assets over the Ethereum blockchain requires a convenient trade and exchange mechanism. Sealed-bid auctions are powerful trading tools due to the advantages they offer compared to their open-cry counterparts. However, the inherent transparency and lack of privacy on the Ethereum blockchain conflict with the main objective behind the sealed-bid auctions. In this paper, we tackle this challenge and present a smart contract protocol for a succinctly verifiable sealed-bid auction on the Ethereum blockchain. In particular, we utilize various cryptographic primitives including zero-knowledge Succinct Non-interactive Argument of Knowledge (zk-SNARK), Multi-Party Computation (MPC), Public-Key Encryption (PKE) scheme, and commitment scheme for our approach. First, the proving and verification keys for zk-SNARK are generated via an MPC protocol between the auctioneer and bidders. Then, when the auction process starts, the bidders submit commitments of their bids to the smart contract. Subsequently, each bidder individually reveals her commitment to the auctioneer using the PKE scheme. Then, according to the auction rules, the auctioneer claims a winner and generates a proof off-chain based on the proving key, commitments which serve as public inputs, and their underlying openings which are considered the auctioneer's witness. Finally, the auctioneer submits the proof to the smart contract, which in turn verifies its validity, based on the public inputs, and the verification key. The proposed protocol scales efficiently as it has a constant-size proof and verification cost regardless of the number of bidders. Furthermore, we provide an analysis of the smart contract design, in addition to the estimated gas costs associated with the different transactions.

11:30-12:00 - Blockchain-Based Fair Certified Notifications

By Macia Mut-Puigserver, Magdalena Payeras-Capella and Miquel Angel Cabot-Nadal (University of the Balearic Islands, Spain)

Lots of traditional applications can be redefined thanks to the benefits of Blockchain technologies. One of these services is the provision of fair certified notifications. Certified notifications is one of the applications that require a fair exchange of values: a message and a non-repudiation of origin proof in exchange for a non-repudiation of reception evidence. To the best of our knowledge, this paper presents the first blockchain-based certified notification system. We propose two solutions that allow sending certified notifications when confidentiality is required or when it is necessary to register the content of the notification, respectively. First, we present a protocol for Non Confidential Fair Certified Notifications that satisfies the properties of strong fairness and transferability of the proofs thanks to the use of a smart contract and without the need of a Trusted Third Party. Then, we also present a DApp for Confidential Certified Notifications with a smart contract that allows a timeliness optimistic exchange of values with a stateless Trusted Third Party.

12:00-12:25 - Self-Reproducing Coins as Universal Turing Machine (Short Paper)

By Alexander Chepurnoy, Vasily Kharin and Dmitry Meshkov (IOHK Research, Ergo Platform and Research Institute, Russia)

Turing-completeness of smart contract languages in blockchain systems is often associated with a variety of language features (such as loops). In opposite, we show that Turing-completeness of a blockchain system can be achieved through unwinding the recursive calls between multiple transactions and blocks instead of using a single one. We prove it by constructing a simple universal Turing machine using a small set of language features in the unspent transaction output (UTXO) model, with explicitly given relations between input and output transaction states. Neither unbounded loops nor possibly infinite validation time are needed in this approach.

12:30 – 14:00

Lunch and poster session

14:00 – 15:30

Session 2: Economic modeling, transparency and consensus

Room: Agora

Chair: Rainer Böhme

14:00-14:30 - Using Economic Risk to Model Miner Hash Rate Allocation in Cryptocurrencies.

By George Bissias, Brian Levine and David Thibodeau (University of Massachusetts Amherst, USA)

Abrupt changes in the miner hash rate applied to a proof-of-work (PoW) blockchain can adversely affect user experience and security. Because different PoW blockchains often share hashing algorithms, miners face a complex choice in deciding how to allocate their hash power among chains. We present an economic model that leverages Modern Portfolio Theory to predict a miner's allocation over time using price data and inferred risk tolerance. The model matches actual allocations with mean absolute error within 20% for four out of the top five miners active on both Bitcoin (BTC) and Bitcoin Cash (BCH) blockchains. A model of aggregate allocation across those four miners shows excellent agreement in magnitude with the actual aggregate as well a correlation coefficient of 0.649. The accuracy of the aggregate allocation model is also sufficient to explain major historical changes in inter-block time (IBT) for BCH. Because estimates of miner risk are not time-dependent and our model is otherwise price-driven, we are able to use it to anticipate the effect of a major price shock on hash allocation and IBT in the BCH blockchain. Using a Monte Carlo simulation, we show that, despite mitigation by the new

difficulty adjustment algorithm, a price drop of 50% could increase the IBT by 50% for at least a day, with a peak delay of 100%.

14:30-15:00 - Contour: A Practical System for Binary Transparency

By Mustafa Al-Bassam and Sarah Meiklejohn (University College London, UK)

Transparency is crucial in security-critical applications that rely on authoritative information, as it provides a robust mechanism for holding these authorities accountable for their actions. A number of solutions have emerged in recent years that provide transparency in the setting of certificate issuance, and Bitcoin provides an example of how to enforce transparency in a financial setting. In this work we shift to a new setting, the distribution of software package binaries, and present a system for so-called *binary transparency*. Our solution, Contour, uses proactive methods for providing transparency, privacy, and availability, even in the face of persistent man-in-the-middle attacks. We also demonstrate, via benchmarks and a test deployment for the Debian software repository, that Contour is the only system for binary transparency that satisfies the efficiency and coordination requirements that would make it possible to deploy today.

15:00-15:25 - Valuable Puzzles for Proofs-of-Work (Short Paper)

By Colin Boyd and Christopher Carr (Norwegian University of Science and Technology, Norway)

Proof-of-work (PoW) is used as the consensus mechanism in most cryptocurrencies. PoW-based puzzles play an important part in the operation and security of a cryptocurrency, but come at a considerable energy cost. One approach to the problem of energy wastage is to find ways to build PoW schemes from valuable computational problems. This work proposes calibration of public key cryptographic systems as a suitable source of PoW puzzles. We describe the properties needed to adapt public key cryptosystems as PoW functions suitable for decentralised cryptocurrencies and provide a candidate example.

15:30 – 16:00

Coffee and poster session

16:00 – 17:35

Session 3: Attacks, privacy and atomic disclosure

Room: Agora

Chair: Sarah Meiklejohn

16:00-16:25 - Enforcing rule changes through offensive forking- and consensus techniques (Short Paper)

By *Aljosha Judmayer, Nicholas Stifter, Philipp Schindler and Edgar Weippl (SBA Research, Austria)*

The increasing number of cryptocurrencies, as well as the rising number of actors within each single cryptocurrency, inevitably leads to tensions between the respective communities. As with open source projects, (protocol) forks are often the result of broad disagreement. Usually, after a permanent fork both communities *mine their own business* and the conflict is resolved. But what if this is not the case? In this paper, we outline the possibility of malicious forking and consensus techniques that aim at destroying the other branch of a fork. Thereby, we illustrate how merged mining can be used as an attack method against a permissionless Proof-of-Work (PoW) cryptocurrency, which itself involuntarily serves as parent chain for the attacking merge mined branch of a hard fork.

16:25-16:50 - Coloured Ring Confidential Transactions (Short Paper).
By Felix Engelmann, Frank Kargl and Christoph Bosch (Ulm University, Germany)

Privacy in block-chains is considered second to functionality, but a vital requirement for many new applications, e.g., in the industrial environment. We propose a novel transaction type, which enables privacy-preserving trading of independent assets on a common block-chain. This is achieved by extending the ring confidential transaction with an additional commitment to a colour and a publicly verifiable proof of conservation. With our coloured confidential ring signatures, new token types can be introduced and transferred by any participant using the same sized anonymity set as single-token privacy aware block-chains. Thereby, our system facilitates tracking assets on an immutable ledger without compromising the confidentiality of transactions.

16:50-17:15 - Atomic Information Disclosure of Off-Chained Computations using Threshold Encryption (Short Paper)
By Oliver Stengele and Hannes Hartenstein (Karlsruhe Institute of Technology, Germany)

Public Blockchains on their own are, by definition, incapable of keeping data private and disclosing it at a later time. Control over the eventual disclosure of private data must be maintained outside a Blockchain by withholding and later publishing encryption keys, for example. We propose the Atomic Information Disclosure (AID) pattern based on threshold encryption that allows a set of key holders to govern the release of data without having access to it. We motivate this pattern with problems that require independently reproduced solutions. By keeping submissions private until a deadline expires, participants are unable to plagiarize and must therefore generate their own solutions, which can then be aggregated and analyzed to determine a final answer. We outline the importance of a game-theoretically sound incentive scheme, possible attacks, and other future work.

17:15-17:35 – Poster Presentations (1/2)

- ***17:15-17:20 – Livio Pompianu,*** *Stefano Lande, Massimo Bartoletti, Andrea Bracciali. "BlockAPI: Blockchain analytics API"*
- ***17:20-17:25 –Alejandro Ranchal-Pedrosa,*** *Sara Tucci-Piergiovanni, Maria Potop-Butucaru, Yannick Seurin. "Scalable Funding of Bitcoin's Layer2"*
- ***17:25-17:30 –Sergio Serusi,*** *Stefano Lande, Massimo Bartoletti, Barbara Pes. "Bitcoin Deponzifier: data mining for detecting Bitcoin Ponzi schemes"*
- ***17:30-17:35 – Siamak Solat.*** *"RDV: An Alternative to Proof-of-Work"*

19:00 – 21:00

Social Activity

21:00 – 23:00

Gala Dinner

Friday, September 7, 2018

09:00 – 10:30

Session 4: Second Layer and lightning networks

Room: Agora

Chair: Hannes Hartenstein

09:00-09:25 - Split payments in payment networks (Short Paper)

By Dmytro Piatkivskyi and Mariusz Nowostawski (Norwegian University of Science and Technology, Norway)

Off-chain payments are a novel concept that has yet received very little academic attention. Nevertheless, the first publications have demonstrated that the net- work cannot achieve all the desirable properties and a number of trade offs will have to be made at some point. On top of that, the network formation and its usage are highly uncertain for the time being, yet utterly determinative. For that reason, we are set to study the network properties and begin with suggesting an operational mode that improves upon a number of them. Our suggestion is to split atomic payments and spread them timely. We demonstrate in this paper that such a trick not only solves principle issues within the network, but also increases the liquidity, while investing less.

09:25-09:50 - Payment Network Design with Fees (Short Paper)

By Georgia Avarikioti, Gerrit Janssen, Yuyi Wang and Roger Wattenhofer (ETH Zurich, Switzerland)

Payment channels are the most prominent solution to the blockchain scalability problem. We introduce the problem of network design with fees for payment channels from the perspective of a Payment Service Provider (PSP). Given a set of transactions, we examine the optimal graph structure and fee assignment to maximize the PSP's profit. A customer prefers to route transactions through the PSP's network if the cheapest path from sender to receiver is financially interesting, i.e., if the path costs less than the blockchain fee. When the graph structure is a tree, and the PSP facilitates all transactions, the problem can be formulated as a linear program. For a path graph, we present a polynomial time algorithm to assign optimal fees. We also show that the star network, where the center is an additional node acting as an intermediary, is a near-optimal solution to the network design problem.

09:50-10:15 - Avoiding Deadlocks in Payment Channel Networks (Short Paper)

By Shira Werman and Aviv Zohar (The Hebrew University of Jersualem, Israel)

Payment transaction channels are one of the main proposed approaches to scaling cryptocurrency payment systems. Recent work by Malavolta et al. has shown that the privacy of the protocol may conflict with its concurent nature and may lead to deadlocks. In this paper we ask the natural question: can payments in routing networks be routed so as to avoid deadlocks altogether? Our results show that it is in general NP-complete to determine whether a deadlock-free routing exists in a given payment graph. Given some fixed routing, we propose another way to resolve the problem of deadlocks. We offer a modification of the protocols in lightning netwoks and in the Fulgor algorithm that pre-locks edges in an order that guarantees progress, while still maintaining the protocol's privacy requirements.

10:15-10:30 – Poster Presentations (2/2)

- ***10:15-10:20 – Stefano Lande,*** *Nicola Atzei, Massimo Bartoletti, Roberto Zunino.*
  "Balzac: a DSL for Bitcoin transactions"
- ***10:20-10:25 – Sergi Delgado-Segura*** *and Cristina Pérez-Solà.*
  "STATUS: Don't trust, analyse"
- ***10:25-10:30 – Alexei Zamyatin****.*
  "Multisignatures for Cryptocurrency-Backed Tokens"

10:30 – 11:00

Coffee and poster session

11:00 – 12:30

Session 5: Bitcoin proposals and mining pools

Room: Agora

Chair: Joaquin Garcia-Alfaro

11:00-11:30 - On symbolic verification of Bitcoin's SCRIPT language.

By Rick Klomp and Andrea Bracciali (University of Stirling, UK)

Validation of Bitcoin transactions relies upon the successful execution of scripts written in a simple and effective, non-Turing-complete by design language, simply called SCRIPT. This makes the validation of closed scripts, i.e. those associated to actual transactions and bearing full information, straightforward. Here we address the problem of validating open scripts, i.e. we consider validation against the whole set of possible inputs, e.g., under which general conditions can Bitcoin be redeemed? Even if likely not one of the most demanding verification problems, merits of formally addressing the validation of open SCRIPTs are 1) contributing to the formalisation of (a fragment of) the language; 2) providing a novel symbolic approach to SCRIPT verification; 3) providing formal validation for newly defined and non-standard payment schema; and 4) providing building blocks for a larger verification theory for the developing area of Bitcoin smart contracts. The verification of smart contracts, i.e. agreements built as transaction protocols, is a difficult to formalise and computationally demanding problem.

11:30-12:00 - What Blockchain Alternative Do You Need?

By Tommy Koens and Erik Poll (Radboud University, The Netherlands)

With billions of dollars spent on blockchain, there clearly is a need to determine if this technology should be used, as demonstrated by the many proposals for decision schemes. In this work we rigorously analyze 30 existing schemes. Our analysis demonstrates contradictions between these schemes - so clearly they cannot all be right - and also highlights what we feel is a more structural flaw of most of them, namely that they ignore alternatives to blockchain-based solutions. To remedy this, we propose an improved scheme that does take alternatives into account, which we argue is more useful in practice to decide an optimal solution for a particular use case.

12:00-12:30 - A Poisoning Attack against Crypto-currency Mining Pools.

By Mohiuddin Ahmed, Jinpeng Wei, Yongge Wang and Ehab Al-Shaer (University of North Caroline at Charlotte, USA)

This paper discusses a potentially serious attack against public crypto-currency mining pools. By deliberately introducing errors under benign miners' names, this attack can fool the mining pool administrator into punishing any innocent miner; when the top miners are punished, this attack can significantly slow down the overall production of the mining pool. We show that an attacker needs only a small fraction (e.g, one millionth) of the resources of a victim mining pool, which makes this attack scheme very affordable by a less powerful competing mining pool. We experimentally confirm the effectiveness of this attack scheme against a few well-known mining pools such as Minergate and Slush Pool.

12:30 – 14:00

Farewell & Lunch