

RESEARCH INTERESTS	Applied cryptography, cryptographic currencies, distributed ledger technology, security engineering
EDUCATION	<p><b>Newcastle University</b>, Newcastle upon Tyne, Tyne &amp; Wear, UK</p> <p>Ph.D. Candidate, Bitcoin and Security Engineering, September 2013 (expected graduation date: March 2017)</p> <ul style="list-style-type: none"> <li>• Dissertation Topic: “Cryptocurrency: Payment Security and Applications of the Blockchain”</li> <li>• Advisor: Feng Hao.</li> </ul> <p>BSc (hons) Computer Science (with Industrial Placement at IBM UK), July, 2013.</p> <ul style="list-style-type: none"> <li>• Graduated 1<sup>st</sup> in my class with 89% overall.</li> </ul>
HONORS AND AWARDS	<p><b>Only Ph.D. Candidate</b> short listed for an ‘Impact in Progress Award’ across all departments at Newcastle University, 2015</p> <p><b>Winning team</b> at the Creative Cyber Security Hackathon 2015 sponsored by Newcastle University, Lancaster University, Raytheon &amp; the Department for Business and Innovation.</p> <p><b>Best overall performance</b> in Computer Science at Newcastle University, 2013.</p> <p><b>Scott Logic Excellence Award</b> for best overall performance for a second year student in Computer Science at Newcastle University, 2011.</p> <p>‘<b>Best Team award</b>’ for the Software Engineering Team Project in the undergraduate degree.</p> <p>‘<b>Excellence Scholarship</b>’ for over-achieving the entry requirements at Newcastle University.</p>
ACADEMIC EXPERIENCE	<p><b>Newcastle University</b>, Newcastle upon Tyne, Tyne &amp; Wear, UK</p> <p><i>Ph.D. Candidate</i> <span style="float: right;"><b>October 2013 - present</b></span></p> <p>Myself (alongside other academics) have discovered the following:</p> <ul style="list-style-type: none"> <li>• Bitcoin (and other crypto-currencies) provide the ideal infrastructure for command and control centers (C&amp;C) that allow ‘Botmasters’ to control thousands of infected machines,</li> <li>• A survey for Bitcoin-related crime, malware, theft and money laundering.</li> <li>• A post-payment protocol that allows two pseudonymous users to re-authenticate using the records stored in a distributed ledger,</li> <li>• A flaw in Bitcoin’s Payment Protocol standard (BIP70) that is used by more than 100,000 merchants. These flaws have been acknowledged by industry (Coinbase, BitPay and Bitt),</li> <li>• A survey for a new field of research ‘Bitcoin Payment Networks’ that is a potential scaling solution for distributed ledger technologies.</li> </ul> <p><i>Teaching Assistant</i> <span style="float: right;"><b>October 2013 - present</b></span></p> <p>I assist with teaching the following modules for both undergraduate and master students:</p> <ul style="list-style-type: none"> <li>• CSC8202 Information Security &amp; Trust - <i>Advising master students how to design encryption solutions and perform simulations using Markov chains,</i></li> <li>• CSC8002 Advanced Programming - <i>Advising master students how to create concurrent and event-driven Java programs,</i></li> <li>• CSC3621 Cryptography - <i>Advising undergraduate students during practical sessions how to break ciphers including text-book RSA, two-time pad and Vigeneres Cipher,</i></li> <li>• CSC2022 Software Engineering Team Project - <i>Supervising and technically advising undergraduate students to work as part of a team for large-scale software development,</i></li> </ul>
PUBLICATIONS	<b>P. McCorry</b> , M. Mö ser, S.F. Shahandashti, F. Hao. Towards Bitcoin Payment Networks (Invited Paper), 21st Australasian Conference on Information Security and Privacy (ACISP 2016)

**P. McCorry**, S.F. Shahandashti, F. Hao. Refund Attacks on Bitcoins Payment Protocol, 20th Financial Cryptography and Data Security (FC 2016).

**P. McCorry**, S.F. Shahandashti, D. Clarke, F. Hao. Authenticated Key Exchange over Bitcoin, 2nd Security Standardisation Research Conference (SSR 2015).

T. Ali, D. Clarke, **P. McCorry**, Bitcoin: Perils of an Unregulated Global P2P Currency, 23rd Security Protocol Workshop (SPW 2015).

T. Ali, **P. McCorry**, P. Lee, F. Hao, ZombieCoin: Powering Next-Generation Botnets with Bitcoin, 2nd Workshop on Bitcoin Research 2015 (co-located with FC 2015).

V. Vlachokyriakos, R. Comber, K. Ladha, N. Taylor, P. Dunphy, **P. McCorry**, PosterVote: expanding the action repertoire for local political activism. Designing Interactive Systems (DIS 2014)

PROFESSIONAL  
EXPERIENCE

**IBM UK, Hursley, Hampshire, UK.**

*Intern Software Developer for the CICS Portfolio*

**July, 2010 - September, 2011.**

I was an intern software developer in the CICS (Customer Information Control Systems) department. CICS is a transaction server that runs on zOS mainframes and the portfolio also includes CICSplex System Manager (CPSM) and CICS Explorer. This software is used by most banks in the world.

On the side, I taught primary school children ICT skills, organised induction events, instructed a '101 How To Code' series, and innovated a 'IBM Web Design Competition for Secondary School' which required local schools to build a website for 'IBM Smarter Planet'. The participants were invited to IBM to present their website in front of a panel of renowned judges to win a prize.

CONFERENCE AND  
WORKSHOP  
PRESENTATIONS

1. CryptoForma (Kent University) 2015
2. Workshop on Bitcoin Research (co-located with Financial Cryptography and Data Security) 2015
3. North East Fraud Forum 2015
4. European Symposium on Research in Computer Security 2015
5. CryptoForma (University of Strathclyde) 2015
6. Security Standardisation Research 2015
7. Bitcoin Summer School (Corfu) 2016
8. Australasian Conference on Information Security and Privacy 2016.