Message Exploration in Bitcoin Blockchain

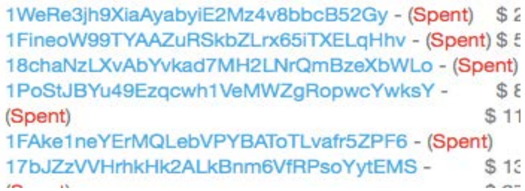
Department of Computer Science and Information Systems

Research Student
Sukhvinder Hara

Supervisors
David Weston
Trevor Fenner

Research Aims

The research will examine messages and communication data placed into the Bitcoin blockchain using one of four methods. There is evidence to suggest that users have placed messages to communicate with supporters and their network e.g. Wikileaks (see Figure 1). Which demonstrates how each transaction can convey single word message, and multiple messages can convey conversations.
https://blockchain.info/address/13LBgLZ24X55mr8LqKddy9DusJtba17NCC



1WeRe3jh9XiaAyabyiE2Mz4v8bbcB52Gy - (Spent) $ 2
1FineoW99TYAAZuRSkbZLrx65iTXELqHhv - (Spent) $ 5
18chaNzLXvAbYvkad7MH2LNrQmBzeXbWLo - (Spent)
1PoStJBYu49Ezqcwh1VeMWZgRopwcYwksY - $ 8
(Spent) $ 11
1FAke1neYErMQLebVPYBAToTLvafr5ZPF6 - (Spent)
17bJZzVVHrhkHk2ALkBnm6VfRPsoYytEMS - $ 13

Figure 1. Vanity messages placed in the blockchain by Julian Assange

The research also looks to find artefacts left on digital media from use of Bitcoin, using digital forensic techniques to establish a standard operating procedure (SOP). This will enable the research to establish whether recovery of artefacts enables investigators to link a user to transactions (messages) placed within the blockchain. It will examine whether these artefacts can reveal interactions with other users on the network.

Research Methodology

Initial experiments conducted using digital forensic frameworks, has demonstrated that different artefacts are recoverable dependent on the method used to image the digital media.

Using digital forensic software, the recovery of artefacts has been collected from user data, system files and application files enabling the cataloguing from various Bitcoin wallets.

Research Approach

Experimentation transactions (messages) will be sent, to demonstrate how messages are placed within the blockchain from a test machine. These will be sent from different wallets. At various stages this test machine will be imaged to forensically locate artefacts.

Upon completion of this, transactions will be parsed out of the blockchain. The point of this exercise is to determine the number of messages within the blockchain and network analysis. It will further be used for intelligence to discover identities where digital media evidence is available.

Submitted Publications

HEA National Conference for Learning and Teaching in Cyber Security

1. S. Hara 6th April 2017
   Developing Investigation Skills in DLT: Bitcoin

11th International Conference on Global Security, Safety & Sustainability 18th - 20th January 2017

2. Mitchell, T. Anandaraja, S. Hara, G. Hahzhinenov, & D. Neilson
   Deconstruct and Preserve (DaP): A method for the preservation of digital evidence on Solid State Drives (SSD) 11th International Conference, ICGS3 2017, January 18-20th,2017

3. Bitcoin Forensics: Practical Investigations (2016) D. Neilson, S. Hara, & I. Mitchell