Physics > Physics and Society

An Analysis of Anonymity in the Bitcoin System

Fergal Reid, Martin Harrigan

(Submitted on 22 Jul 2011 (v1), last revised 7 May 2012 (this version, v2))

Anonymity in Bitcoin, a peer-to-peer electronic currency system, is a complicated issue. Within the system, users are identified by public-keys only. An attacker wishing to de-anonymize its users will attempt to construct the one-to-many mapping between users and public-keys and associate information external to the system with the users. Bitcoin tries to prevent this attack by storing the mapping of a user to his or her public-keys on that user's node only and by allowing each user to generate as many public-keys as required. In this chapter we consider the topological structure of two networks derived from Bitcoin's public transaction history. We show that the two networks have a non-trivial topological structure, provide complementary views of the Bitcoin system and have implications for anonymity. We combine these structures with external information and techniques such as context discovery and flow analysis to investigate an alleged theft of Bitcoins, which, at the time of the theft, had a market value of approximately half a million U.S. dollars.

Comments:	28 pages, 14 Figures. Updated with further related work, additional technical details. Format changed to author prepared book chapter preprint. Supporting code, additional discussion: this http URL
Subjects:	**Physics and Society (physics.soc-ph)**; Social and Information Networks (cs.SI)
Cite as:	**arXiv:1107.4524 [physics.soc-ph]**
	(or **arXiv:1107.4524v2 [physics.soc-ph]** for this version)

Submission history

From: Fergal Reid [view email]

[v1] Fri, 22 Jul 2011 14:29:34 GMT (2179kb,D)

[v2] Mon, 7 May 2012 17:23:31 GMT (2091kb,D)

Which authors of this paper are endorsers?