The Inescapable Escrow
Electronic playgrounds depend on trust

BROOKS MERSHON
Duke University
CS 342s
April 6, 2016

Escrows everywhere

One of the first papers [1] I read at the beginning of the course discussed a computational model for distributed electronic rights over distributed networks. I stumbled across this Google Research paper while searching for articles related to digital rights management. To my pleasant surprise, the authors explored the issue of *smart contracts*, or arrangements which must be carried out between mutually suspicious parties in an asynchronous computational model. We can think of the transfer of money as one obvious situation in which contracts come into play.

I spent many hours following the concrete examples that the paper provides of an extension that could be made to the JavaScript language to support secure execution of contracts. The concrete examples aimed at exploring the concept of trust in a real-world application were exciting for me because I have invested a significant amount of time in learning the intracies of a matured JavaScript. The JavaScript I happen to care about is one that is not only ubiquitous, but built tough for servers, built for modularity, and designed to remove the warts that have kept others from realizing its real potential in the past. In just 42 lines of code, the paper illustrates the details of an escrow exchange contract.

The concrete examples and code provide by the authors made me wonder about the deeper philosphical questions of trust, risk, and the need for a trusted third-party that arise in a wide variety of transactions. The need for trust in the form of an *escrow* seemed inescapable, and my interest in learning more about the way in which escrows pop up in various electronic applicaitons had been piqued.

Research project proposal

My goal for this research project is to examine several other articles from Google Research and elsewhere that do a good job of illustrating ways in which *the escrow* pops up in various applications. As I saw in the first paper I read on smart contracts, the best way for me to get a feel for the way *escrows* arise is by finding material that clearly explains concrete examples of the escrow in action. The exciting aspect of this project will be gaining an apprecition for the importance of the escrow through clearly articulated examples, code snippets, and diagrams that I will find in various papers I read.

So far, I have found the following potential papers:

1. Distributed Electronic Rights in Javascript [1]
2. Swapsies on the Internet: First Steps towards Reasoning about Risk and Trust in an Open World [2]
3. Reasoning about Risk and Trust in an Open World [3]
4. Failsafe Key Escrow (CSAIL)

References

1. Mark S. Miller, Tom Van Cutsem, and Bill Tulloh. Distributed electronic rights in javascript. In *ESOP'13 22nd European Symposium on Programming*, 2013.

2. Sophia Drossopoulou, James Noble, and Mark S. Miller. Swapsies on the internet: First steps towards reasoning about risk and trust in an open world. In *Tenth Workshop on Programming Languages and Analysis for Security (PLAS 2015)*, 2015.

3. Sophia Drossopoulou, James Noble, Toby Murray, and Mark S. Miller. Reasoning about risk and trust in an open world. Technical report, Victoria University of Wellington, 2015.