Double Spending Protection for E-Cash Based on Risk Management

Patricia Everaere\textsuperscript{1}, Isabelle Simplot-Ryl\textsuperscript{1}, and Issa Traoré\textsuperscript{2}

\textsuperscript{1} Univ Lille Nord de France, USTL, CNRS UMR 8022 LIFL, France
\texttt{patricia.everaere@lifl.fr} \texttt{Isabelle.Ryl@inria.fr}

\textsuperscript{2} University of Victoria
Dep. of Electrical and Computer Engineering, Canada
\texttt{itraore@ece.uvic.ca}

Abstract. Electronic cash is an attempt to replace and reproduce paper cash in electronic transactions that faces competing challenges when used either online or offline. In effect, while effective protection against double spending for e-cash can be achieved in online payment environments through real-time detection, this comes at the expense of efficiency, the bank representing in such case a performance bottleneck and single point of failure. In contrast, in offline payment environments, while efficiency is improved, double spending can be detected only after the fact, which can be very costly. We propose in this paper a risk management approach for double spending protection which allows suitable tradeoffs between efficiency and effectiveness. This involves using the service of a trader, who is a trusted third party that will cover the risk involved in offline payment transactions, against some remuneration. The main goal is to provide full coverage to users against losses related to invalid coins while avoiding or minimizing interactions with the bank. Since the trader will incur some risk by guaranteeing coins while she cannot communicate with the bank, a winning strategy is devised for the trader to mitigate such risk.

1 Introduction

The last two decades have witnessed tremendous interest in electronic cash development from academia and industry. The main goal of these efforts is to go beyond the basic model of payment cards by introducing more flexibility and reducing the costs involved in carrying electronic payment transactions.

Electronic payment schemes are divided into two categories: offline schemes and online schemes \cite{1}. The key difference between these two categories is that online schemes involve communicating with a central authority during payment transactions, while offline ones do not have such requirement. In offline schemes, merchants are responsible for checking the validity of the coins on their own, which quite often can be difficult and costly, when double spending is involved. Most systems rely on detection of such kind of fraud later when the system is back
online. As a result double spending may lead to significant loss by merchants if catching the culprits later turns out to be impossible. In contrast in online systems, coins validity is checked by the bank during the transaction allowing double spending and forgery prevention. But this has the side effect of turning the bank into a performance bottleneck and single point of failure, limiting scalability as a result.

In such environment, the most widely used approach to combat multiple spending consists of maintaining at the bank a database of spent coins. This database must be consulted for each transaction to detect attempt of double-spending. Maintaining, however, a database of spent coins poses important system distribution challenges [2] related to location, scalability, performance and security. One of the key issues with such database is about its size that will grow with the time as more transactions take place and pose as a result significant storage and performance problems.

Some of the proposed solutions, to achieve the strength of each of these individual approaches, while limiting their downside consist of making a tradeoff by adopting an hybrid scheme that combines appropriately online and offline steps. With this approach, to improve efficiency, payments will by default be carried out offline, while to limit the impact of double-spending a subset of the payment transactions selected randomly will be checked online. Although this approach reduces the risk of double-spending, there still remains a residual risk that is inherent to randomized audit or probabilistic polling, and this can be significant for some of the merchants or consumers.

Other proposed solutions consist of redistributing the bank’s load so as to improve scalability and performance. In this case, the major challenge is about the difficulty of implementing such scheme. For instance, implementing publicly viewable coin binding list using existing distributed database technology means that the mechanisms used for data coherence and updates might introduce some delay that could create some windows of opportunity for successful double-spending. So like the previous solutions based on randomized audits, we are still faced with residual risk of double-spending that could be significant.

To eliminate or handle the impact of the residual risk while achieving better scalability and performance properties, we propose to combine risk management with redistributing the bank’s load onto smaller autonomous consumer groups or communities. Each of these communities will be managed by a trusted third-party referred to as a trader, who will oversee and guarantee payment transactions occurring locally within the network. The trader will manage and provide an insurance scheme to its membership against some fees proportional to the level of risk associated with each member that will cover any loss incurred due to double spending.

Trading within a community can be carried out using only trader certified coins, which are valid only locally. It is expected that initially members would purchase and hold bank certified coins. When joining a community, a member will exchange bank certified coins against trader certified coins that can safely be used in exchanges with other members in the community. At any time, a member