A Derivative of Digital Objects and Estimation of Default Risks in Electronic Commerce

Kanta Matsuura
Institute of Industrial Science, University of Tokyo,
Komaba 4-6-1, Meguro-ku, Tokyo 153-8505, Japan
kanta@iis.u-tokyo.ac.jp

Abstract. In electronic commerce, traded digital objects are likely associated with several numerical values as well as their prices. These values may change unpredictably over time and bring risks both to the providers and to the consumers of the application. One possible strategy for hedging the risks is to introduce derivatives regarding the uncertain values. This paper shows a theoretical pricing equation of the derivatives when the underlying digital objects have systematic default or revocation risks. We can make use of this pricing to estimate the risks.

1 Introduction

With the help of applied cryptography, we are going to trade more and more digital objects over an open network. Since digital objects can keep their original bit strings virtually forever, one may expect that there would be no risk of change. This is, unfortunately, not always the case. Digital objects can have not only prices but also other important numerical values. For example, digital certificates may have confidence values or trust metrics \[1\]. Access-grant tickets may have priority numbers or QoS (Quality-of-Service) values \[2\] reserved. Digitally-watermarked images \[3\] may have innocence values about their origins in terms of copyright protection. Any product may be associated with some insurance contracts \[4\]. Reward points may be attached. Those additional values and their effectiveness may change unpredictably over time and cause risks. At the worst case, the values get into defaults (e.g. the corresponding certificate is revoked) and the holder may have a large financial damage.

A popular way for hedging such stochastic risks is to introduce derivatives or options written on underlying assets, typically regarding their prices. In financial theory, encouraged by the seminal paper by Black and Scholes \[5\], option-pricing theories have been developed a lot. Most of them use assumptions including divisibility of the underlying assets, which is not trivial in the case of the digital objects. Thus we are motivated to study option pricing with models and assumptions suitable for digital objects. The rest of this paper consists of modeling (Sect.\[2\]), pricing (Sect.\[3\]), discussion including an application (Sect.\[4\]), and conclusions (Sect.\[5\]).

© Springer-Verlag Berlin Heidelberg 2001
Fig. 1. A network commerce architecture where boxes with wider lines indicate that the entities inside are more trusted.

2 Objects with Default/Revocation Risks

Our model is based on an architecture illustrated in Fig. 1.

(Object Provider.) Copyright management and related technical maintenance are difficult and non-trivial tasks. So are management and maintenance of network-security infrastructure (e.g. public-key infrastructure). These tasks may require sufficient trustworthiness and reliability. We need specialized entities. They would be happier if the objects they provide are distributed and circulated more frequently in larger amounts; it would improve their reputation and/or make attached advertisement more profitable.

(Object Server.) Selling digital objects to untrusted customers through poor communication channels is difficult task, too. We need specialized entities.

(Customer.) We do not trust individuals in terms of (i) their own behaviour, (ii) their financial situation, and (iii) resources (for communication and computation) available to them.

In a network life, we would want to pay for digital objects in electronic cash. Such digital payment systems could be more efficient if the monetary value of each coin is less granular. Therefore, if we want to allow as wide variety of electronic cash systems as possible, highly discrete (i.e. very sparse) prices would be helpful. So we firstly assume an object whose price is fixed. For notational simplicity, we assign this fixed price as the unit of network currency. Also for simplicity, we assume each share of the object has a single value. This value is