Sound Marketization of User-Generated Content based on a Fair Micro-Billing Scheme

Masayuki Terada, Kozo Noaki, and Kimihiko Sekino
NTT DOCOMO, Inc., Yokosuka, Japan
Email: {teradam, noaki, sekino}@nttdocomo.com

***Abstract*— User-generated content (UGC) is one of the most promising services. Most UGC items are currently being distributed for free due to the lack of a suitable compensation system. This inability to compensate the creators stands in the way of UGC becoming a mature service with sustainable and sound growth. The current schemes used to charge for (professional) digital content are inadequate for UGC, since UGC is distributed through a different value-chain that dispenses with the selection processes of publishers and distributors found in the conventional value-chain for distributing professional works, and thus the quality of content is quite uneven. Such high quality unevenness greatly increases the user's risk of buying a pup, and turns the UGC market into a Akerlof's *lemon market*, where the quality of merchandise enters a death-spiral until the market collapses. This paper comprehensively examines the ability of monetization models to remunerate creators of UGC, and proposes a smartcard-based fair micro-billing scheme that will activate the UGC market. The proposed scheme enables users to pay for content in a "bit by bit" manner, and thus significantly reduces the user's content quality risk as well as the "freeride" risks for creators. This paper also shows that the proposed scheme can be implemented securely and feasibly by using current smartcards.**

***Index Terms*— user-generated content (UGC), lemon market, smartcard, micro-billing**

I. Introduction

A. Motivation

User-generated content (UGC), also known as user-created content (UCC) or consumer-generated media (CGM), has been rapidly proliferating due to the recent penetration of wired or wireless broadband Internet access. According to OECD surveys [1], [2], 26% of Internet users in the U.S. had published self-made "artwork, photos, stories or videos" as of 2006. eMarketer also reported that 82.5 million people (43% of Internet users in the U.S.) had published UGC (including blogs) as of 2008 and they estimate that this number will reach 114.5 million in 2013 [3], [4]. In Japan, many young people are enjoying UGC via the Internet as well as 3G mobile phone networks.

The utility and impact of UGC have lately attracted not only Internet users but also more traditional content holders; a few examples include the British Broadcasting Corporation (BBC), which is providing content under the Creative Commons (CC) license, and Kadokawa-shoten, which is acknowledging superior user-created secondary works (a.k.a. mash-ups) as "official" secondary works.

While UGC has the potential to become an influential service, most UGC creators[1] are unable to receive any remuneration for their creative efforts. The current situation, UGC is distributed for free, has attracted a wide audience, but it may prevent UGC from experiencing the sound and sustainable growth needed to become a mature service, and moreover, some critics [5], [6] warn that it will even damage the labor market.

To address these problems, some infrastructure that can provide adequate remuneration to UGC creators is needed; i.e., monetizing UGC and returning a fair share of the profits to the creators. Possible approaches can be roughly divided into two categories: indirect monetization models such as advertising-based models and monetizing the audience via online sales, and direct monetization models such as charging viewers for accessing UGC. Given the current situation of most UGC distribution sites, which adopt the advertising-based model but cannot cover even their basic operating costs, the indirect models appear unable to generate enough value to permit the creators to be remunerated.

Direct monetization models, such as promoting the "UGC store", look simple and natural, but are seen as risky because UGC is intrinsically a jumble of gems and stones; a user runs the risk of purchasing undesirable content. Such a market, which forces buyers into accepting high risks with regard to the quality of the merchandise, will turn into Akerlof's *lemon market* [7], where the quality of the merchandise enters a death-spiral until the market collapses. This is one of the characteristic problems in marketing UGC, which is widely distributed without any guarantee about its quality; professional works are distributed via conventional value-chains and the "brand names" of the creators and/or the distributors (e.g. record publishers) provide some implicit guarantee of quality. Sound growth of the UGC market, consequently, demands adequate measures that can reduce the user's risk.

This paper is based on "Smartcard-based Micro-Billing Scheme to Activate the Market for User-Generated Content" by M. Terada, K. Noaki, and K. Sekino, which appeared in the Proceedings of the 4th International Conference on Ubiquitous Information Management and Communication (ICUIMC 2010), Suwon, Korea, January 2010. © 2010 ACM.

[1] UGC creators are also "users" by definition (i.e., UGC stands for *user*-generated content), but this paper refers to users who created content as *creators* so as to avoid confusion.

doi:10.4304/jsw.8.3.507-519

B. Contributions

In this paper, we discuss the reason why sound marketization of UGC cannot be easily achieved, and propose a novel fair and secure client-side micro-billing scheme. Although UGC includes diverse media formats, e.g. texts, images, music, and videos, this paper mainly focuses upon UGC videos, which are a recent hot trend; however, the proposed scheme can also be easily adopted to support music and books.

We first give a definition of UGC and elucidate the intrinsic differences between UGC and professional works, and observe possible monetization models for UGC; their pros and cons are illustrated. Given the characteristics of the UGC value-chain, any monetizing scheme for UGC must provide a means to fairly remunerate many diverse creators, and to work soundly even if the quality of the content is highly uneven, however, the observation concludes that no currently deployed monetization model can meet these requirements.

We next propose a novel smartcard-based micro-billing scheme as a concrete solution that can satisfy the above requirements; the proposed scheme enables secure "bit by bit" charging even when viewing digital content offline, by enforcing the atomicity of (micro-)use of content and the corresponding payments. The proposed scheme can reduce the user's risk in a fair manner, and thus the creators of superior content are paid more than inferior creators. The security and feasibility of the proposed scheme are also discussed; the security of the proposed scheme is reducible into the security of several well-known cryptographic primitives (e.g. hash functions and digital signature schemes) given the tamper-resistance of smartcards, and the proposed scheme can be feasibly implemented using modern smartcards.

II. UGC and Monetization Models

A. User-Generated Content

There is no widely accepted definition of UGC, but this paper basically follows the definition in OECD reports [1], [2][2] as follows:

Definition 1 (User-generated content (UGC)): User-Generated Content is content that

1) is made publicly available over the Internet,
2) reflects a "certain amount of creative effort", and;
3) is "created outside of professional routines and practices".

While the first and second conditions simply exclude private (i.e. not publicized) content and non-creative works, the last condition, is the most important and distinguishing characteristic of UGC.

Here we do not restrict *professional works* to mean just the content created by professional artists, but any content that becomes available through "professional routines and practices" such as the selection and review processes performed by publishers, who are responsible for paying creators for their content and who guarantee the quality of published content to the buyers (users). This is realized by filtering out the content that is thought have little mass appeal (also called "long tail" content) and thus few sales. It is an intrinsic and important characteristic that UGC is published outside these conventional processes because the absence of such hurdles in the publication process of UGC offers much more diversity and lower distribution costs (Fig. 1). The key trade-off is, however, that the creators have difficulty in receiving fair remuneration for their creative efforts and users have no guarantees of content quality.

B. Monetizing UGC

To remunerate creators for their creative efforts, some monetizing scheme is indispensable. Given the characteristics of the UGC value-chain described before, any monetizing scheme for UGC must meet the following requirements: a) it must provide a means to fairly remunerate the many creators for their content, and b) it must work soundly to counter the uneven quality of the content.

There are two approaches to monetize UGC: direct and indirect monetization. The former sells the content itself. The latter extracts payments through services related the content, e.g., charge users for content distribution and the sale of advertisements in UGC distribution sites. These monetizing models can be classified as follows:[3]

1) *Direct monetization models* where users pay for content, which is divided into the following subcategories according to when and how much users pay:
   a) *Charging for downloads*: the user pays to download content (similar to buying professional works),
   b) *Charging per view*: the user pays to view content (content is not retained),
   c) *Voluntary donation* the user voluntarily pays for content *after enjoying*: it, and
   d) *"Pay what you want" model*: the user pays what he wants *prior to downloading* the content;
2) *Indirect monetization models* where users or third-parties pay for related services; these models are subdivided below, according to who pays:
   a) *Subscription model*: the user subscribes to a service provided by UGC distributors, and
   b) *Third-party model*: the user is not charged at all and UGC distributors acquire payments from others such as advertisers.

[2] To be exact, these reports refer to UGC as UCC (user-created content).

[3] OECD [1], [2] gives a similar categorization that focuses more upon the indirect models; both *charging for downloads* and *charging per view* in this paper correspond to the"pay-per-item model" in their categorization, the *third-party model* is divided into three categories ("advertising-based model", "licensing of content and technologies to third parties", and "selling goods and services to community"), and there is no mention of the *pay-what-you-want model*.

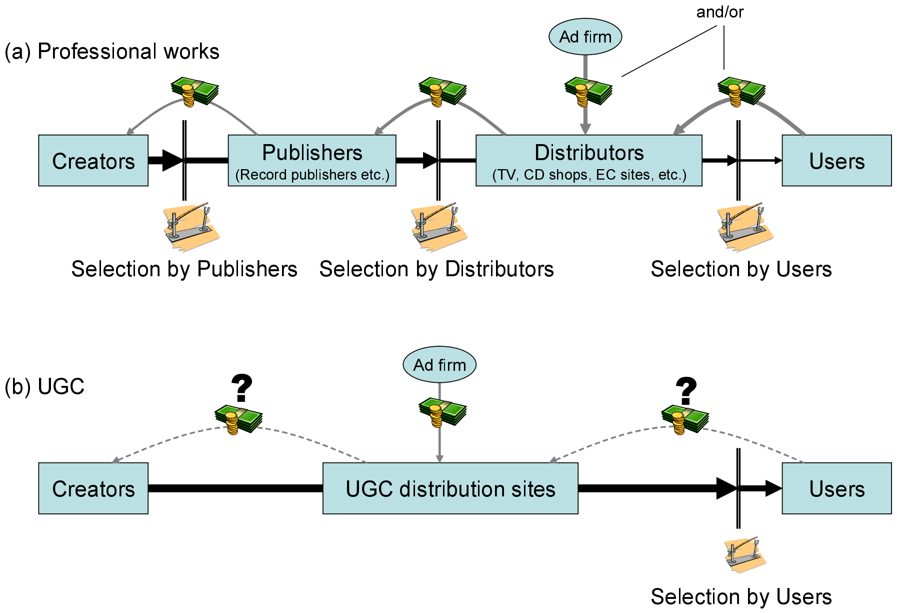

Figure 1. A comparison of (a) the conventional value-chain for professional works and (b) the value-chain for UGC.

Unfortunately, however, none of these models will satisfy the requirements stated above; roughly speaking, the direct monetization models fail to deal with the unevenness of content quality, and the indirect monetization models fail to support the fair remuneration of creators.

C. Indirect Monetization Models

Most sites currently distributing UGC take the indirect monetization approach while the direct models are much more popular for professional works, so we look first the indirect models here.

The unevenness of content matters only little in the indirect models since users pay nothing for each content; if the content being viewed is deemed to be worthless by the user, the user will simply drop the content at no charge to himself. However, at least currently, UGC creators[4] are rarely remunerated in the indirect models, for two main reasons: a) collected revenues from these models basically belong to the UGC distributors who provide the service (for which users or third-parties pay) and b) the revenues are not enough to share with content creators (in particular those of UGC video distribution sites, whose expenses are quite high to provide the bandwidth needed). Furthermore, even if the UGC distributors were willing to remunerate UGC creators for their creative efforts and they could earn enough to do so, it would be difficult to *fairly* share the profits to the creators. That is, high(low) payment for good(poor) content; this problem defeats the objective of fairly remunerating creators so as to facilitate the sound growth of UGC.

The following discussions focus on two indirect monetization models, the "subscription model" and the "third-party model".

1) Subscription model: In this model, the user subscribes to one or more services provided by a UGC distributor; the subscription gives the user the right to view content. This model is in place on many UGC distribution sites as well as paid-TV services. Most distributors offer a two-tier subscription approach: the "basic" account is free but there are limitations (e.g. bandwidth and/or resolution of the content), while the "premium" account has no such restriction. An example is most popular Japanese UGC video distribution site Nico-Nico-Douga [8], whose main revenue source is the subscription fees from the premium accounts. The site reported that its premium subscribers, each pays 500 Yen (about 5.5 dollars) subscription fee per month, reached 0.7 million in March 2010.

As noted before, however, the revenues from this monetizing model belong to the UGC distribution sites, and are rarely shared with UGC creators. The discussion below assumes that the distributors can make a profit and thus are willing to share their profits with UGC creators.

The uneven content quality is not a problem here, since the user does not pay to view individual content; the only risk is that the subscribed service is not worth the subscription fee. On the other hand, this model fails to offer fair remuneration because of the difficulty of determining content quality.

While direct monetization models basically use the market mechanism (or the so-called "invisible hand") to determine the remuneration, this model relies upon the UGC distributor to set the remuneration price. In the conventional value-chain for professional works, this price is determined through negotiation between the distributor and publisher as part of the "selection by the distributor" process (cf. Fig. 1), and basically the more is remunerated for the higher quality content. In the UGC value-chain, there are many diverse creators and

[4] Distributors often share their revenues with major content holders of professional works.

no publisher intermediates the distributor and them; it might be infeasible for the UGC distributor to check the quality of all works posted to the site and to price the remunerations according to the quality. Accordingly, remuneration must be determined automatically.

However, it is a hard problem to fairly create remunerations. For example, the simplest approach is to share profits equally among the creators, but this is obviously unfair and doesn't work properly since there is no incentive for creators to provide good works. A more reasonable approach is to share the profit according to content download frequency. Unfortunately, this is also unfair since the download frequency should not accurately reflect the value of content; e.g. a 2-hour movie will be downloaded much less often than a 1-minute short-short film, but usually the former is more valuable than the latter, if the skills of both creators are equivalent and they do their best. Such unfairness distorts the motivation to create good works, and accordingly would injure the creators' morality and the quality of their content.

2) Third-party model: This model secures payments from parties other than the user; the user is not required to pay anything. Examples include advertisements and licensing to third-parties. Advertising is the most workable means of collecting revenues from web services currently [9], and is quite popular for UGC distribution.

The distribution of UGC videos, however, makes it difficult to secure profits and thus creator remuneration[5]. The best example is YouTube [10], the Internet's largest UGC video distributor. YouTube continues to experience operating losses since the revenues from advertisements are insufficient. Ref. [11] introduces an analysis by Credit Suisse, which estimates that "the site (YouTube) will lose approximately $470 million in 2009, as the costs of the bandwidth and storage, to stream more than 5 billion clips a month far exceed the revenue YouTube earns from advertising". The following discussion thus makes the same profit assumption as the subscription model discussion.

The risks to users and creators are similar to those in the subscription model; there is obviously no users' risk (other than the side effects of advertisement-based monetization, see below) since they are charged nothing, and fair remuneration to creators is difficult to realize. The simple approach is to make remuneration proportional to advertising revenues. Relying upon this approach, however, might also distort the incentives and motivations of the creators. Ref. [9] identifies several side-effects created by advertisement-based monetization, e.g. spamming, product placement (or stealth marketing) and click-spoofing (or shilling). Monetizing from advertisements is, and will likely remain, one of the most important revenue resources supporting UGC, but it should be noted that excessive dependence on it could hinder the future sound growth of the UGC market.

D. Direct Monetization Models

The direct monetization models appear more workable. Two of them, *charging for downloads* and *charging per view*, are used commonly to monetize professional works, however, these models are not so popular for monetizing UGC, at least currently. There are various reasons for this: e.g., advertisement-based monetization is much easier for a UGC distributor to set up, Internet culture of giving stimulates the voluntary creation and publication of content, and there was not easy payment scheme suitable for UGC. Focusing on the differences between UGC and professional works, the key reason is most likely the absence of the "professional routines and practices". This absence yields highly uneven content quality, and forces the buyer to run the risk of unacceptable quality.

Existing direct monetization models fail to address the content quality risks to the user. To summarize, *charging for downloads* and *charging per view*, popular approaches to the monetization of professional works, burden the UGC user with excessive quality risk and trigger the lemon effect which can demolish any market. The charging per view model offers a slightly better situation, but the improvement is not enough to avoid lemonization. In contrast, *voluntary donations* and the *"pay what you want" model* may completely liberate users from the quality risk, but both are quite unfair for creators, who will not receive fair remuneration. There is no intermediate course that is fair to both creators and users.

1) Charging for download: Professional works are widely sold in digital format by digital content distribution services for consumption on PCs, portable music/video players, and mobile phones; a few examples include iTunes Store for iPod portable players, Amazon MP3 for PCs, and "Chaku-uta" ring tone (incoming song) services for Japanese 3G mobile phones. In these services, users pay to acquire (download) content like purchasing physical media such as CDs or DVDs — a very simple and comprehensible monetizing model.

The UGC market in this model, however, burdens the users with too much risk with regard to the quality of the content bought as mentioned before. Different from professional works, whose quality is checked by publishers, the quality of UGC solely depends on the skill and motivation of the creator, these include anonymous professionals, rising indie producers, amateur creators, and maybe, malicious fraudsters. This inherent unevenness in UGC quality yields brilliant and unprecedented content, but users are forced to run the risk of paying for content not to his taste since they cannot judge the quality of the content beforehand; this is a quite unfair to the user.

Such an unfair market, where the quality of merchandise (i.e. content) is highly uneven and uncertain to the buyer (i.e. user) before making the purchase, is known to yield *adverse selection* by buyers and creates a *lemon market*. [7]

In such a market, the buyer has to estimate the quality of merchandise, but his best guess is the average of the

[5] Many blog owners earn profits from advertisements directly placed on their own sites, but UGC videos, on which this paper focuses, are rarely distributed directly from the creators' own sites.

merchandise because of the uncertainty of the quality. The average quality as estimated by users might be rather inferior in the UGC market, since the few brilliant works are surrounded by many more crude ones.

A user will, accordingly, tend to purchase cheap content to avoid the quality risk regardless of its real quality (adverse selection), and therefore superior (but rather expensive) content provided by "good" creators will disappear from the market. As a result, the market will be filled up by cheap but inferior content; i.e., the market becomes a market for lemons (Fig. 2).

This result is, ironically, contrary to the motivation of marketizing UGC, i.e. facilitating the sustainable and sound growth of UGC to create a mature service by appropriately compensating the creators.

2) Charging per view: This model, also known as pay-per-view (PPV) or pay-per-stream, charges users for viewing content, not for downloading it. The user in this model avoids the full purchase price and thus so not own the content.

This model is often employed by Pay-TV services and Internet streaming sites. Another notable example is the *superdistribution* architecture [12], where (usually encrypted) content[6] is freely distributed to users without restriction, and the users' devices enforce payment for viewing it. Several digital rights management (DRM) schemes including OMA DRM [13] and Windows Media Rights Manager [14], optionally support superdistribution-like content distribution models.

Compared to the charging for download model, the user risk should be somewhat relieved, because the theoretical price of viewing content is the same as the full purchase price divided by the number of expected views; a user who is not satisfied with the content has the option to stop subsequent views (and so avoid further payments).

In practice, however, since it is not usual for a user to view or listen to the same UGC frequently, "the expected number of views" will be a small number; so the price of content (relative to the user's risk) in this model may not significantly lower than that in the charging for download model — it remains unfair to the user and is likely to lead the lemon market.

3) Voluntary donations: In this model, content is available for free and a user voluntarily pays for content if the content is good enough; this model is just like that of street performers.

This model is rarely used for professional works, but is common in free-software distribution sites with a "donate" button. A user who enjoyed the content and decides to donate to the site owner pushes the button and pays the site owner for the content via an online P2P payment scheme such as PayPal.

A significant merit of this model is that the user can completely avoid any risk of paying for useless content since payment is made only if the user enjoys the content, however, this model intrinsically creates many "free riders" and is unfair for creators (and users who made donations).[7]

4) "Pay what you want" model: This model is similar to the voluntary donation model, but users who download content are asked to pay what they want *in exchange for downloading* the content, while users pay what they want *after playing* the content in the voluntary donations model; in this sense, this model is a hybrid of the voluntary donations and the charging for download model.

The risks of creators and users are also a mixture of those of the two models that yields a rather worse combination; creator's risk is almost same as that of the voluntary donation model because the payment amount is completely decided by the user, while the user's risk is higher because the user is uncertain about the quality of content when he is asked to pay.

A famous case of this approach is the album "In Rainbows" by English rock band Radiohead. It was first released on October 10, 2007 from the band's official website, and was downloadable from there until November 3, 2007. The consumers were asked to pay what they wanted to by credit card when downloading the album, and those who were not willing to pay were asked to give their email addresses.

This case is somewhat an extreme case, since the creator, Radiohead, was an established band that already had a very good brand reputation, and the album, which was released over four years after their previous album, was the one that their loyal fans had been eager for.

According to a study by comScore [15], however, 62% of the downloaders of the album from Radiohead's official website chose to pay *nothing* even for this album, and the average amount was no more than $2.26. Furthermore, there were many more freeloaders who used illegal downloads, even though they were allowed to legally download the album for free from the official site. Page and Garland [16] estimate that there were 2.3 million downloads via BitTorrent during the period that the album was officially downloadable, which far exceeds the estimated download total from the official site; thus the correct average price should be much lower.

Considering that even a well established band could receive too little from their brilliant work, we are pessimistic that the majority of UGC creators, most of whom are obscure, can receive fair compensation for their works in this model.

III. Approaches and Design Goals

Regarding the observations on the monetization models in Sect. II, two approaches can be considered: a) improving the indirect monetization models so as to fairly remunerate to creators, and b) improving the direct

[6] Although the superdistribution architecture mainly aims to distribute software products, it can also be applied to distribute digital content.

[7] Nevertheless, the voluntary donations (of time or money) made to support the *gift economy* (in contrast to market economy), which supported the early Internet and freeware (or open source software) movements for long time. However, the discussion about whether the gift economy or the market economy will provide a better future for UGC is beyond the scope of this paper, which focuses upon how a sound *market economy* for UGC can be constructed.

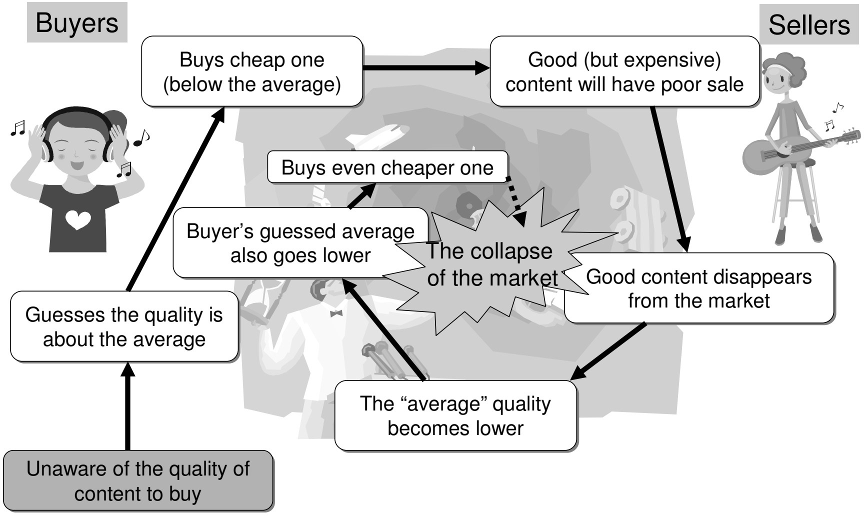
Buyers
Sellers
Buys cheap one (below the average)
Good (but expensive) content will have poor sale
Buys even cheaper one
Buyer's guessed average also goes lower
The collapse of the market
Good content disappears from the market
Guesses the quality is about the average
The "average" quality becomes lower
Unaware of the quality of content to buy

Figure 2. The death spiral of the lemon market.

monetization models so as to ease the risks of both creators and users.

This paper focuses upon the second approach, and introduces the "bit by bit" approach to address the lemon problem; i.e., dividing the content into a number of micro-blocks, each of which users can purchase and view gradually.

The idea behind this approach is similar to that of gradual exchange protocols, which are fair exchange protocols where two parties exchange information gradually. In these protocols, intuitively, when two parties Alice and Bob are willing to fairly exchange their information with each other, each divides his or her information into n of pieces[8], and both repeat the exchange of pieces n times. Since if Alice stops sending pieces, Bob can also stop, the unfairness for Bob is at most n-times less than exchanging information by simply sending the complete set of information to each other (and vice versa).

In our proposal, each content is divided into a number of micro-blocks, and a user pays per bit for using (viewing or listening) each micro-block; since a user can stop using the content at any time and is not liable for the unused portion of the content, his risk is greatly reduced so that adverse selection is avoided. Since brilliant works will be viewed to the end by many users, and so return a lot of profit to their authors, the motivation to provide better works and higher quality content will be significantly increased.

In addition, this approach should introduce another (good) side-effect since this "bit by bit" approach may be considered as equivalent to a series of "micro-trades". Such a process is known to encourage the trading parties to behave cooperatively (cooperative strategies become better than betrayals); creators will be further motivated to provide better content.

However, there is a problem in implementing this proposal; it seems infeasible to directly exchange a micro-block and the corresponding payment between the creator and the user.

A simple way to implement this scheme is to adopt an existing micro-payment system such as PayWord [17] and let the user (micro-)pay per each downloaded micro-block over the network.

Such an implementation of the micro-payment system, however, involves drawbacks that spoil feasibility. For example, the need to exchange micro-payment and content blocks means that stand-alone devices are not supported. Even if network access is provided, the replay quality of the content is likely to be degraded by intermittent disconnection or any increase in network latency, which is frequent in wireless networks; prefetch (or buffering) of the content data is the most popular and effective solution to prevent such degradation, but it is difficult to utilize the micro-payment approach because the prefetched micro-blocks must be paid for regardless of whether they are actually used or not.

Consequently, the billing (or payment) for micro-blocks should be performed autonomously in the user device with no reliance on network interaction. To realize this, a key issue is how to implement secure and feasible user-side enforcement to ensure the correspondence between micro-content access and micro-billing receipt, i.e., no content use without the corresponding payment and vice versa.

To summarize the above discussion, we set the following design goals for the micro-billing scheme for UGC:

1) *Fairness for content users.* The risk of paying for worthless or useless content must be acceptably low.
2) *Fairness for content creators.* The risk of failing to receive payment for the content used must be acceptably low. In addition, the creators' reputation is protected from being damaged by malicious acts

[8] To be more exact, each piece includes some cryptographic information that gradually increases the probability of restoring the original information to be exchanged.

like masquerading as a creator and then altering the other's works.

3) *Offline capability and feasible implementation.* The means to enforce the above requirements can be feasibly realized without remote access during content use.

IV. Proposed Micro-billing Scheme

To achieve the design goals described in the previous section, this paper proposes a new smartcard-based micro-billing scheme that securely realizes fair micro-billing for content use.

This section is constructed as follows: the proposed scheme is overviewed first, and the procedures to generate encapsulated content (including micro-blocks) for distribution (by the creator), to use the micro-blocks with the corresponding micro-billing (by a user), and to send the payment, which is the aggregation of the micro-billings, from the user to the creator, are then described.

A. Overview

Let H be the content creator (i.e. content holder) who generates encapsulated content c from (original) content m, and U be the content user that accesses (e.g. views or listens to) content c. Creator H possesses content generator device G_H and payment receiver device R_H, while user U has billing device B_U and content player device P_U.

Creator H generates encapsulated content c from m, e.g., video or music content encoded with a common encoding method such as MPEG4 and MP3, by using generator device G_H, which may be a program installed on a regular computer like a PC. Encapsulated content c consists of n encrypted micro-blocks, $\{c_1, c_2, ..., c_n\}$, and header c_0; i.e., $c = \{c_0, c_1, ..., c_n\}$). Header c_0 consists of divider information d_c including the correspondence between micro-blocks $\{c_1, c_2, ..., c_n\}$ and original content m, tariff information t_c to calculate the billing amount of each micro-block, authenticator a_c to prevent malicious alteration of the encapsulated content, and public key Pk_H, the public key of creator H; i.e., $c_0 = \{d_c, t_c, k_c, a_c, Pk_H\}$.

After its generation, encapsulated content c can be distributed by any means, including content distribution servers, P2P networks, and manually. Note that there is no restriction on the distribution means for c, e.g., it is copy-free and no enforcement for payment/billing or digital rights management (DRM) is needed, because the fee is not to possess (download) the content but to use its (the micro-blocks). In other words, this scheme can be considered as realizing *superdistribution* [12].

User U uses (plays) encapsulated content c by applying billing device B_U and player device P_U. Billing device B_U is a tamper-resistant device with electronic money functionality such as a smartcard or a mobile phone that offers electronic money. B_U receives block number i from player device P_U, and then decrypts corresponding micro-block c_i and charges fee (i.e. decreases the electronic money stored in B_U), which is calculated by tariff information t_c, for using c_i. The charged fee is recorded per creator so as to credit the creator as described below. Player device P_U is a content player device capable of replaying original content m, such as a portable player device or a PC with content player software. P_U sends block number i to B_U according to the instruction from user U, and plays the corresponding decrypted micro-block received from billing device B_U.

After finishing the use of content, or at specified intervals (e.g., every day or every month), the charged fees are transferred from the user's billing device B_U to creator's payment receiver device R_H, which is an electronic money account on a network banking server or a mobile phone with electronic money functionality. In the payment, B_U and R_H run a fair exchange protocol that exchanges the payment and its receipt in a fair manner.

B. Detailed Explanations

Each component of the proposed scheme proceeds as follows.

Let Pk_H and Sk_H be the public key and a secret key of creator H, respectively, both of which are stored in generator device G_H and payment receiver device R_H.

Pk_B and Sk_B are the public key pair of billing device B_U. Sk_B is common to all B_U and is renewed on a sufficiently frequent basis to provide continuous security. Note that billing device B_U is a tamper-resistant device; its secret key Sk_B or other secret information are not to be disclosed, and its behavior and stored data can not be illegally altered, even by its owner.

$\mathrm{Sign}_{Sk_X}(m)$ and $\mathrm{Verify}_{Pk_X}(m, s)$ (where s is a signature to be verified) denote signature generation and signature verification for message m by using public key pair Sk_X and Pk_X, respectively, while $Pk_X(m)$ denotes the public key encryption of m where Pk_X is the encryption key.

1) Generating encapsulated content: Creator H creates content m as usual, and decides how to divide the content into micro-blocks and how much to charge for each block. Content generator device G_H generates encapsulated content c from the information provided by H as follows:

1) According to the instructions from creator H, generate divider information d_c and tariff information t_c.

   Divider information d_c consists of n pieces of dividing position information d_i ($d_c = \{d_1, d_2, ..., d_n\}$), which indicates that micro-block c_i corresponds to the data from the $(d_{i-1}+1)$-th byte to the d_i-th byte of content m (referred as to m_i hereafter), where $d_0 = 0$ and $d_n = |m|$.

   Tariff information t_c defines the calculation rules (i.e. function) which map block number i and replay log l_c[9] to charge amount b_{i,l_c}, which is the fee for replaying c_i, and updated replay log l'_c ($t_c(i, l_c) \rightarrow$

[9] Described in Sect. IV-B.2.

$\{b_{i,l_c}, l'_c\}$). For the simplest example, if fee b is charged for every micro-block, t_c is a constant function that maps any value to constant b and an empty set ($t_c(\cdot,\cdot) \rightarrow \{b, \phi\}$).

2) Generate content key k_0 as a kl-bit random number ($k_0 \leftarrow \{0,1\}^{kl}$).

3) Generate key constructor k_c by encrypting k_0 with Pk_B, the public key of player devices ($k_c = Pk_B(k_0)$).

4) Generate $c_i (1 \leq i \leq n)$ from m_i and k_0 as follows:
   a) Generate block key i by encrypting block number i with k_0 ($k_i = k_0(i)$).
   b) Generate extended key e_i from k_i by using extender function $e : \{0,1\}^{kl} \rightarrow \{0,1\}^{|m_i|}$, which is a one-way function that generates secure pseudo-random number sequences ($e_i = e(k_i)$).
   c) Generate c_i as the exclusive-OR of m_i and e_i ($c_i = m_i \oplus e_i$).

5) Sign the concatenation of d_c, t_c, k_c and $h(c_{1,n} = c_1|c_2|...|c_n)$, and let authenticator a_c ($a_c = \text{Sign}_{Sk_H}$ $(d_c|t_c|k_c|h(c_{1,n}))$), where $h : \{0,1\}^* \rightarrow \{0,1\}^{hl}$ is a secure one-way hash function such as SHA-256.

6) Output encapsulated content $c = \{c_0, c_1, ..., c_n\}$, where $c_0 = \{d_c, t_c, k_c, a_c, Pk_H\}$.

The generated encapsulated content can be distributed by any means as mentioned in Sect. IV-A.

2) Playing and charging for encapsulated content: User U plays encapsulated content c by using billing device B_U and player device P_U; the process to play c consists of the *preparation* process, which is performed once at the beginning of every content play, and the *micro-play* process, which is performed for each use of a micro-block.

a) Preparation process: Before starting to play c, user U checks tariff information t_c to confirm if the fee for playing c is reasonable; e.g., the overall fee is not too high, and the transition in charge amounts is fair (i.e., the charge for early blocks is fair).

If U considers that the fee of c is adequate, U calculates hash value $h_c = h(c_{1,n})$, which is the hash value of the concatenation of the all micro-blocks included in c, and input h_c and c_0 (extracted from c) to billing device B_U to prepare for playing c.

The preparation is performed by B_U as follows:

1) Extract d_c, t_c, k_c, a_c, Pk_H from c_0, and verify that the micro-blocks and headers are not altered by the signature verification of a_c using public key Pk_H (Verify_{Pk_H} $(d_c|t_c|k_c|h_c, a_c) \overset{?}{=}$ success); if the verification fails, alert U to the alteration of c and abort the preparation.

2) Check that the debt (i.e. unpaid fee) to creator H (corresponding to Pk_H), namely b_H, does not exceed predetermined constant value $b_{\max}$; if exceeded, alert U to perform the payment process with H and abort the preparation.

3) Extract k_0 by decrypting k_c using B_U's secret key Sk_B ($k_0 = Sk_B(k_c)$), and notify user U that c is ready to be played.

b) Micro-play process: After preparation is completed, the micro-play process is performed as follows:

1) Player device P_U identifies block number i to be played by using dividing position information d_i, and sends i to billing device B_U ($P_U \rightarrow B_U : i$).

2) Billing device B_U charges for playing c_i corresponding to the provided block number i as follows:
   a) From tariff information t_c, calculate charge amount b_{i,l_c} and update replay log l'_c from i and (current) replay log l_c ($\{b_{i,l_c}, l'_c\} \leftarrow t_c(i, l_c)$), where l_c is recorded per content and if c has not been played (charged) by B_U before, the initial value is assumed to be an empty set ($l_c = \phi$).
   b) Deduct the electronic money stored in B_U (i.e. the balance of B_U) by b_{i,l_c} if the balance is enough; if this fails due to insufficient funds, alert user U and abort content play.
   c) After the successful deduction of the balance, add b_{i,l_c} to b_H, the payment due to creator H, which is recorded per creator.
   d) Update replay log l_c to l'_c ($l_c \leftarrow l'_c$).

3) B_U extracts k_i by decrypting i using k_0, which is extracted in the preparation process, as the decrypting key ($k_i = k_0(i)$), and sends k_i to P_U ($B_U \rightarrow P_U : k_i$).

4) P_U generates extended key e_i from k_i by using extender function e ($e_i = e(k_i)$).

5) P_U generates m_i by calculating the exclusive-OR of e_i and c_i ($m_i = e_i \oplus c_i$), and plays it.

3) Payment of charged fees: The payment of the fee from user U to creator H is performed between U's billing device B_U and H's payment receiver device R_H as follows:

1) Billing device B_U runs a fair exchange protocol [18], [19] to exchange payment b_H with corresponding receipt token d_{b_H}, which represents the acceptance that b_H has been transferred, with H's payment receiver device R_H. To prevent forgery of d_{b_H}, d_{b_H} includes a signature of Sk_H; for instance, $d_{b_H} = Sign_{Sk_H}(n_{b_H})$, where n_{b_H} is a unique nonce value bound to the fair exchange session.
   In the step of confirming the receipt of an item in the fair exchange protocol, B_U verifies the signature included in d_{b_H} by using H's public key Pk_H. If this fails, the exchange is aborted (R_H never receives b_H in this case because of the fairness property of the fair exchange protocols) [19], [20].

2) B_U clears b_H (let $b_H = 0$) upon receiving d_{b_H} by the (successful) completion of the fair exchange protocol; the fair exchange property also assures that B_U can always receive d_{b_H} if R_H receives b_H (unless U behaves dishonestly).

The reason why a fair exchange protocol is used here instead of just exchanging payment and receipt notices is to avoid the risk of double payment; if the fairness of exchanging b_H and its receipt d_{b_H} is not assured, it is possible that b_H will remain although the payment was completed successfully, and could be paid again at the next payment time.

V. EXAMPLE SCENARIOS

The proposed scheme is basically designed to achieve fairness in monetizing UGC by reducing the user's risk; from this point of view, it seems that only a fixed fee per block need by supported. Our scheme, however, involves tariff information t_c that enables creators to change the fee per block mainly because the "worth of a block" may vary depending on what the block contains (e.g., in a TV show, the show itself should be more valuable than the trailer and accompanying advertisements). The pricing flexibility of the proposed scheme enables diverse use-case scenarios and business models, such as combination with advertisement-based monetization.

This section introduces several example scenarios to show that the scheme is practical. To simplify the explanations, each content in the following scenarios is assumed to consist of 100 blocks.

A. Flat Charging

Tariff information t_c in this simplest scenario, where each block is equally charged, can be quite easily implemented as shown in the Algorithm 1.

Algorithm 1 t_c for flat charging

```
define $t_c(i, l_c)$:
  return ($\$0.01, \phi$)
```

t_c charges one cent for playing every block, and the user who plays the entire content (all 100 blocks) is charged $\$0.01 \times 100 = \$1$.

B. Charging only for the First Play

This scenario sets a flat charge for playing each block of content, but does not charge for the repeated plays of the content. Algorithm 2 gives tariff information t_c in this scenario.

Algorithm 2 t_c for charging only for the first play

```
define $t_c(i, l_c)$:
  if $i \notin l_c$ then
    return ($\$0.01, \{l_c, i\}$)   // charge 1¢, $l'_c \leftarrow \{l_c, i\}$.
  else
    return ($0, l_c$)   // do nothing for repeated plays.
  end if
```

t_c defined in Algorithm 2 also charges one cent for playing every block at each first play, where it holds $i \notin l_c$. However, different from Algorithm 1, once played, block i is stored in replay log l_c and so repeated plays of block i, where *not* hold $i \notin l_c$ holds, trigger no additional charges.

C. Quiz and Answers

In this scenario, content consists of pairs of a "quiz" section and an "answer" section. The quiz sections charge little (or nothing). If a user is interested in the quiz, the user plays the corresponding answer section, which charges more. t_c in this scenario is given as Algorithm 3.

Algorithm 3 t_c for the quiz-and-answer scenario

```
define $t_c(i, l_c)$:
  if $i \leq 40$ then
    return ($0, \phi$)   // Quiz #1
  else if $i \leq 50$ then
    return ($\$0.1, \phi$)   // Ans. #1
  else if $i \leq 90$ then
    return ($0, \phi$)   // Quiz #2
  else
    return ($\$0.1, \phi$)   // Ans. #2
  end if
```

t_c here allows users to play quiz sections #1 and #2 (block $1 \sim 40$ and $51 \sim 90$, respectively) for free. If the quiz does not look interesting, a user can refrain from playing the answer sections and is charged nothing. The user chooses to view the answers, each of which consists of 10 blocks (block $41 \sim 50$ and $91 \sim 100$), and is charged 10 cents per block and therefore \$1 is charged per answer.

D. Compensating Users for Viewing Advertisements

This scenario offers the user the option to choose whether he/she will play the content with advertisements for free, or skip the advertisements and pay for the content. Similar to the quiz-and-answer scenario, the content in this scenario consists of "main body" sections intervened with "advertisement" sections. The main body sections charge the user if viewed, while the advertisement sections credit the user if viewed; i.e., the charge is a minus value. t_c in this scenario is given as Algorithm 4.

Algorithm 4 t_c for compensating users for viewing ads.

```
define $t_c(i, l_c)$:
  if $i \leq 40$ then
    return ($\$0.1, \phi$)
  else if $i \leq 50$ then
    return ($\$-0.4, \phi$)   // refund.
  else if $i \leq 90$ then
    return ($0, \phi$)
  else
    return ($\$-0.4, \phi$)   // refund.
  end if
```

A user who plays the entire content is charged \$4 for playing each main section (block $1 \sim 40$ and $51 \sim 90$), and is credited with \$4 for viewing each advertisement section (block $41 \sim 50$ and $91 \sim 100$). Given the right balance, the user can play the content for free. On the other hand, without the advertisements the user is charged \$8 to play all blocks in the main body sections.

VI. Discussions

This section discusses the security and the feasibility of the micro-billing scheme proposed in the previous section.

A. Security for Users

The proposed scheme greatly reduces the user's risk. Three factors lie behind this risk: (a) the content is unsatisfactory, (b) the creator maliciously distributed worthless content (attacks by creators), and (c) someone has altered or forged the content (attacks by third-parties).

Regarding factor (a), this scheme reduces the risk of paying too much for unsatisfactory content by enabling users to pay in a bit by bit manner; if the content is unacceptable, the user will quit playing it. If the user plays only m of the n micro-blocks of the content, the total fee will be $\Sigma_{i=1}^{m} b_i$[10]. Since the fee for downloading the same content (i.e. the fee in the *charge for download* model) is not less than the sum of the charges for all micro-blocks, $\Sigma_{i=1}^{n} b_i$, the user's risk can be reduced by the ratio of these two sums: $\Sigma_{i=1}^{m} b_i / \Sigma_{i=1}^{n} b_i$.

If the initial micro-blocks are charged at an excessively high rate, e.g., the whole fee is assigned to the first block, the user is alerted and has the option of terminating content play with no charge, see Sect. IV-B.2.

The case of factor (b) is identical to that of factor (a); the user quits content play as the content is deemed unacceptable.

Some of the attacks associated with factor (c) are successfully countered by this scheme since alteration of the encapsulated content is prevented by the digital signature of authenticator a_c. d_c, t_c, k_c are directly included in the subject of the signature, and their alteration is detected by signature verification in the preparation process. Micro-blocks $c_1, c_2, ..., c_n$ are not directly included, but the hash value of their concatenation $h(c_{1,n})$ is protected by the signature; alteration of the micro-blocks also can be securely detected provided that hash function h is secure and user U behaves correctly.

Since misbehavior of the user himself is not considered here, security against the attacks by third-parties is reduced to the security of digital signature function Sign/Verify and hash function h.

B. Security for Creators

The risks faced by the creators are (d) content is used but not correctly charged, and (e) the charged fee is not transferred to the creator.

A malicious user, denoted by $\mathcal{A}$ hereafter, can avoid or (illegally) reduce the charge for playing encapsulated content c, if he can successfully alter tariff information t_c or can acquire (part of) original content m without reducing his money (i.e., bypassing the charge process (step 2) in the micro-play process described in Sect. IV-B.2).

Since the alteration of t_c is detected by the signature verification using authenticator a_c as mentioned before, this attack does not succeed unless the digital signature function is broken.

The attack to bypass the charge process succeeds if $\mathcal{A}$ successfully extracts m_i from c_i without running the micro-play process by inputting i. The discussion of this attack is divided into two game settings. In the first, $\mathcal{A}$ tries to obtain m_i with paying for c_i, and in the other, $\mathcal{A}$ reuses the information obtained in the past session that charged c_i properly (i.e. replay attack).

At first, we discuss the first game: $\mathcal{A}$ tries to obtain m_i without being charged for c_i (i.e., asking i to B_U to obtain k_i). In this game, $\mathcal{A}$ knows all information except m_i, e_i, k_i, k_0, Sk_B and is allowed to ask any block number except i to B_U so as to obtain $k_j (j \neq i)$. In the following, we briefly show a proof that $\mathcal{A}$ cannot win the game if the cryptographic primitives used in the scheme are secure.

Since micro-block c_i is an OTP (one time pad) generated by calculating $c_i = m_i \oplus e_i$, it is indistinguishable from a $|c_i|$-bit random number if e_i is random and its distribution is unknown to $\mathcal{A}$. e_i is output by secure pseudo-random number generator e whose initial seed value is k_i. Accordingly, the condition that $\mathcal{A}$ wins the game is reduced to the possibility that the sequence output from e can be distinguished from a random number (i.e. e is not a secure pseudo-random number generator), or $\mathcal{A}$ can obtain partial information of k_i.

To obtain partial information of k_i, which is generated by the symmetric encryption of i by using content key k_0 as the encryption key ($k_i = k_0(i)$), $\mathcal{A}$ has to know partial information of encryption key k_0, or it is possible for $\mathcal{A}$ to obtain partial information of k_i from $k_0(j) (j \neq i)$, which implies that the adopted symmetric encryption scheme is insecure.

Content key k_0 is a random number[11] generated per content by content generator device G_H, and its derivation is only $k_c = Pk_B(k_0)$ except for block keys $k_1, k_2, ..., k_n$ already mentioned above. $\mathcal{A}$ can know (partial information of) k_0 only when k_0 is distinguishable from a random number (the random number generator used by G_H is insecure), k_0 can be derived from k_c ($Pk_B()$ is insecure), or $\mathcal{A}$ can know Sk_B, which is assumed to be kept secret by the tamper-resistant feature of billing device B_U as stated in Sect. IV-B.

Consequently, $\mathcal{A}$ does not succeed in this attack if the following conditions about the security of the cryptographic primitives are satisfied:

1) Output from e is indistinguishable from a random number,
2) The symmetric encryption scheme used to generate k_i is secure,
3) Output from the random number generator used to generate k_0 is indistinguishable from a random

[10] More precisely, the charge amount should be denoted by b_{i,l_c} since it depends on the play history of content (l_c), but it is denoted by b_i in this section for simplicity.

[11] G_H may use a software-based secure pseudo-random number generator or a hardware-based random number generator that uses physical entropy for generating k_0.

number, and

4) The public key encryption scheme used to generate k_c is secure.

□

Next, we discuss the replay attack in which $\mathcal{A}$ tries to reuse the output of B_U from a past session. In this case, $\mathcal{A}$ succeeds in obtaining the information leading to win the game, i.e., k_i, e_i, m_i, by corrupting player device P_U[12] or eavesdropping the communication channel between B_U and P_U in the session of playing c_i. Accordingly, the security against this attack depends on the difficulty of corrupting P_U and the secrecy of the communication channel between B_U and P_U by $\mathcal{A}$, who is typically malicious user U himself.

The secrecy of the communication channel between B_U and P_U can be easily assured by encrypting the channel by an adequate key exchange protocol with authentication of P_U, unless P_U is corrupted. The difficulty of corrupting P_U, however, largely depends on the implementation of P_U; this is discussed in the next section.

Regarding the risk that the charged fees are not correctly paid, the proposed scheme has no mechanism to force the user to perform the payment except for the check of the debt in the preparation process for playing content by B_U; the theoretical maximum of a creator's uncollected revenue is accordingly estimated at $b_{\max} + \Sigma_{i=1}^{n} b_i$ per billing device.

However, this amount should be very low in practice; a user has no monetary incentive to dishonestly avoid the payment because the balance is reduced by playing the content, not performing the payment process. Avoiding the payment process is not a long-term strategy since the credit held by the user's device cannot be renewed until outstanding payments are made.

C. Implementation Feasibility

In the following, we discuss the feasibility of implementing the devices needed by the proposed scheme: G_H, B_U, and P_U[13]. The proposed scheme can be implemented with practical performance by using current smartcards as described below:

1) Content generator device G_H: Content generator device G_H can obviously be implemented easily since it is not required to be tamper-resistant and uses common cryptographic primitives like symmetric/asymmetric encryption schemes, a digital signature scheme, a secure hash function, and a secure pseudo-random number generator.

Regarding its performance, the computational cost of generating encapsulated content by G_H is linear to the size of original content m; there should be no concern given the performance of current PCs.

2) Billing device B_U: While content generator device G_H can be implemented by using common PCs, B_U must be implemented on a tamper-resistant device, which is most likely a smartcard since B_U should be inexpensive and handy enough to be possessed by every user in this scheme.

The computational performance of typical smartcards in handling cryptographic primitives is good thanks to the co-processor, but since I/O throughput is very poor [21], [22] attention must be paid to the I/O data size of B_U.

The input data size of B_U in the preparation process is $|c_0| + hl$, and the output is just the notification of success or failure; so we focus upon the input data.

The size of c_0 is $|c_0| = |d_c| + |t_c| + |k_c| + |a_c| + |Pk_B|$, where $|k_c|$, $|a_c|$, and $|Pk_B|$ are constant values determined by the adopted cryptographic schemes (should be less than 1K bytes). For the remaining data, the size of d_c is $|d_c| = n \cdot \log_2(|m_{\max}|/u)$ bits, where $|m_{\max}|$ is the maximum data size of the content and u is minimum micro-block size. For instance, if the maximum data size is 4G bytes ($|m_{\max}| = 2^{32+8}$ bits) and the minimum unit size is 1 byte ($u = 8$ bits), the size of d_c when dividing a 10 minute content whose bitrate is 1Mbps (content size is 600M bits = 75M bytes) every 10 seconds (divided into 60 micro-blocks) becomes $|d_c| = 60 \log_2(2^{32+8}/8) = 1920$ bits (240 bytes). The size of t_c depends on the complexity of the billing rules, but the size of the most likely rule, flat charge rate, i.e. the same fee for every block, will be very small.

Accordingly, the size of c_0 is likely to be less than 1K bytes, which should be feasibly for current smartcards whose effective I/O throughput is about 100Kbps.

The input data size of B_U for the micro-play process is $|i|$, and the output data size is $|k_i|$; they are obviously not bottlenecks in terms of performance. The computational cost of this process is also negligible: the read/update of replay log l_c, the application of tariff information t_c, the reduction from the balance, the addition to debt b_H, and symmetric encryption $k_0(i)$; none of them should be a burden to smartcards in practice.

The payment process consists of a fair exchange protocol between R_H and the clearance of b_H. Accordingly, the feasibility here depends on that of a fair exchange protocol involving smartcards, whose performance and practicality were confirmed in [21].

Consequently, B_U can be implemented feasibly on current smartcards.

3) Content player device P_U: Content player device P_U performs the following processes in the micro-play process: the generation of e_i by pseudo-random number generator, the extraction of m_i by computing exclusive-OR of e_i and c_i, and replaying m_i. They can obviously be implemented on a common PC or a media player appliance, however, implementing P_U requires attention to the possibility of the replay attack as mentioned in Sect. IV-B.

Solutions based on secure DRM systems can be also be used to deal with this problem, but similar difficulties

[12] P_U may be corrupted in this scheme since it is not assumed to be a trusted (tamper-resistant) device while billing device B_U cannot be corrupted because of its tamper-resistant feature.

[13] The feasibility of R_H, which runs a fair exchange protocol in the payment process, is not explicitly discussed in this paper since it depends on the feasibility of the fair exchange protocol; the feasibility of a fair exchange protocol involving smartcards is discussed in [21].

are raised. For instance, obfuscating the software program implementing P_U, will prevent casual attacks by ordinary users, but not veteran crackers. More strict solutions will require MAC (mandatory access control) mechanisms or dedicated hardware for P_U so as to prevent a user from maliciously accessing P_U.

VII. Related Works

Although this paper focuses upon monetizing models to avoid the lemon market effect, there are two other approaches that may be considered [7]: a) involves guaranteeing the quality of distributed content, b) providing means to inform the quality of the content to users.

The first approach, known as "screening", is equivalent to resurrecting the gatekeepers of the conventional value-chains for professional works; it may work, but it means that we have to give up content in the "long tail", which may include many striking and unusual contents that characterize UGC. The market based upon this approach should contradict the definition of UGC in Sect. II-A which makes it questionable that it can be called a "market for UGC".

The second approach, known as "signaling", includes free previews and reputation management systems[14]. Free previews, which are common in digital content shops, enable users to play partial content (typically the first 30sec.) for free, to allow users to assess if the content is valuable enough to justify purchase. It may ease the users' quality risk provided that the quality of the rest, the greater part of the content, matches the preview part, however, there is no one to guarantee this assumption in the UGC value-chain; in an extreme case, the rest of content could be just noise if its creator is malicious. The previews are certainly helpful for users, but fail to fully eliminate the quality risk. The reputation management systems collect comments from the users who have played the content, and provides a summary of them. The simplest examples, which are common in UGC distribution sites, are "rating by stars" representing the average numbers of "stars" given by previous viewers, and "posting comments" to enable viewers to post comments on the viewed content and show the posted comments along with the content. It is doubtful that these simple examples can sufficiently reduce the quality risk to users, but further studies on reputation management schemes may improve this situation. In particular, Yamagishi et al. [23] showed that providing reputation information of merchandise providers is effective in preventing the C2C market from being lemonized. Noaki et al. [24] proposed to apply this approach to the UGC market, where providers of reputations can also receive some profit so as to let them provide reputations honestly. These reputation-based approaches can be used together with the proposed scheme.

The implementation approach of the proposed scheme, enforcing the atomicity of block play and payment, is similar to the superdistribution architecture mentioned in Sect. II-D.2. The concept of superdistribution is stated in [12] as follows:

1) Software products are freely distributed without restriction. The user of a software product pays for that product, not for possessing it.
2) The vendor of a software product can set the terms and conditions of its use and the schedule of fees, if any, for its use.
3) Software products can be executed by any user having the proper equipment, provided only that the user adheres to the conditions of use set by the vendor and pays the fees charged by the vendor.
4) The proper operation of the superdistribution system, including the enforcement of the conditions set by the vendors, is ensured by tamper-resistant electronic devices as digitally protected modules.

This architecture has significant merit in that there is no restriction on the means of distributing the content (software products in the definition above); the content itself can be freely copied among users, e.g., by using P2P file sharing systems such as BitTorrent. Since the proposed scheme satisfies the above requirements in addition to enabling fair gradual payment for content use, the scheme might be considered to implement the superdistribution architecture, and can enjoy the same merit. This would drastically reduce the costs currently imposed by distributing UGC; current UGC video sites are troubled by extremely high bandwidth costs.

VIII. Conclusion

This paper first detailed the intrinsic difference between UGC and professional works: the absence of the "professional routines and practices" including review and selection performed by the publishers and the distributors in the conventional value-chains for professional works yields highly uneven content quality as well as making it difficult to fairly compensate the creators. We comprehensively assessed possible monetization models to remunerate UGC creators for their creative efforts. The importance of an fair balance between the creator's risk that users escape payment and the user's risk of paying for undesirable content is extracted as a result.

To achieve this balance, the paper proposed a smartcard-based micro-billing scheme that reduces the user's risk in a fair manner by providing secure "bit by bit" charging, analogous to gradual protocols in the fair exchange field. This scheme enables off-line digital content use by utilizing smartcards that enforce the atomicity of (micro-)use of content and the appropriate payment; this approach places no restriction on the distribution of content, i.e., the content can be distributed by any means including P2P file sharing systems such as BitTorrent, without compromising any security. In addition, the proposed scheme enables creators to flexibly vary the fee per block in their content. Several example scenarios were introduced along with descriptions of the tariff settings that support the scenarios.

[14] Branding is another well-known measure to provide signals, but it does not work well for creators or content in the long tail.

Our discussions on the security and feasibility of the scheme found that the proposed scheme is secure since its security is reducible into the security of several well-known cryptographic primitives (e.g. hash functions and digital signature schemes) and the tamper-resistance of the smartcard, and that the proposed scheme can be feasibly implemented on modern smartcards.

References

[1] S. Wunsch-Vincent and G. Vickery, "Participative web: User-created content," Committee for Information, Computer and Communications Policy, OECD, Tech. Rep. DSTI/ICCP/IE(2006)7/FINAL, Apr 2007.

[2] G. Vickery and S. Wunsch-Vincent, *Participative Web and User-Created Content: Web 2.0, Wikis and Social Networking*. OECD Publications, Oct 2007.

[3] P. Verna, "User-generated content: More popular than profitable," eMarketer Reports, Jan 2009.

[4] eMarketer, "Can user-generated content generate revenue?" Apr 2008.

[5] F. Kleemann, G. G. Voß, and K. Rieder, "Un(der)paid innovators: The commercial utilization of consumer work through crowdsourcing," *Science, Technology & Innovation Studies*, vol. 4, no. 1, pp. 5–26, Jul 2008.

[6] E. Morphy, "The dark side of crowdsourcing," LinuxInsider, Apr 2009.

[7] G. A. Akerlof, "The market for 'lemons': Quality uncertainty and the market mechanism," *Quarterly Journal of Economics*, vol. 84, no. 3, pp. 488–500, 1970.

[8] "Nico nico douga (9)," in Japanese. [Online]. Available: http://www.nicovideo.jp/

[9] P. Kangas, S. Toivonen, and A. Bäck, ""ads by Google" and other social media business models," VTT Technical Research Centre of Finland, Tech. Rep. VTT Research Notes 2384 (VTT-TIED-2384), Apr 2007.

[10] "YouTube – broadcast yourself." [Online]. Available: http://www.youtube.com/

[11] B. Stelter and M. Helft, "Deal brings TV shows and movies to YouTube," *The New York Times*, p. B1 of the New York edition on Apr 17, Apr 2009.

[12] R. Mori and M. Kawahara, "Superdistribution: The concept and the architecture," *Trans. of IEICE*, vol. E73, no. 7, pp. 1133–1146, 1990.

[13] Open Mobile Alliance, *DRM Specification V2.0*, Apr 2005.

[14] *Taking Advantage of Super Distribution*, Microsoft Corp., 2007, Windows Media Rights Manager 10.1.2 SDK Programming Guide.

[15] comScore, "For Radiohead fans, does "free" + "download" = "freeload"?" Nov 2007.

[16] W. Page and E. Garland, "In Rainbows, on Torrents," MCPS-PRS Alliance, Economic Insight 10, Sep 2008.

[17] R. L. Rivest and A. Shamir, "PayWord and MicroMint–two simple micropayment schemes," in *Proc. 1996 intl. workshop on Security Protocols*, ser. LNCS, no. 1189. Springer, 1996, pp. 69–87.

[18] H. Pagnia, H. Vogt, and F. C. Gärtner, "Fair exchange," *The Computer Journal*, vol. 46, no. 1, pp. 55–75, Jan. 2003.

[19] M. Terada, M. Iguchi, M. Hanadate, and K. Fujimura, "An optimistic fair exchange protocol for trading electronic rights," in *Proc. 6th Smart Card Research and Advanced Application IFIP Conference (CARDIS2004)*, ser. IFIP, vol. 153. Kluwer, Aug. 2004, pp. 255–270.

[20] N. Asokan, "Fairness in electronic commerce," Ph.D. dissertation, University of Waterloo, 1998.

[21] M. Terada, K. Mori, K. Ishii, S. Hongo, T. Usaka, N. Koshizuka, and K. Sakamura, "A framework for distributed inter-smartcard communication," *J. Information Processing Society, Japan*, vol. 47, no. 2, pp. 534–546, Feb. 2006.

[22] W. Rankl and W. Effing, *Smart Card Handbook*, 2nd ed. John Wiley & Sons, 2001.

[23] T. Yamagishi and M. Matsuda, "Improving the lemons market with a reputation system: An experimental study of internet auctioning," Hokkaido University, May 2002.

[24] K. Noaki, M. Terada, and K. Sekino, "Why the UGM market does not emerge?" in *Proc. Computer Security Symposium 2008*. IPSJ, Oct 2008, in Japanese.