How blockchain could change Web-based content distribution

TPAC 2015 Breakout session on Oct. 28, 2015
Shigeru Fujimura, Hiroki Watanabe
(NTT Corporation)

IRC: #BCWCD
Background

- **Blockchain technology**: bitcoin’s core technology

- **Its most important feature**: enabling **decentralized, robust and tamper-proof** method for recording data in trustless network

- Robustness proven as bitcoin continues even today
  - **Applications other than cryptocurrency** garnering much attention
Blockchain Application

- Many types of applications based on blockchain technology
  - Cryptocurrency: first application
- One of the hottest area of emerging innovation
Main focus

• **Open discussion on:**
  - Acceptability of blockchain applications for Web-based content distribution
  - Possibility of standardizing in W3C
Agenda

13:30 - 13:35 : Brief introduction to session

13:35 - 13:45 : Blockchain technology details

13:45 - 14:00 : Concept of Web-based content distribution
  - How to apply blockchain tech. and what can be achieved
  - [DEMO] Example of direct license control

14:00 - 14:25 : Open discussion

14:25 - 14:30 : Wrap-up

by Hiroki Watanabe
Blockchain technology details
Blockchain technology

- **Blockchain**: something like database for specific use
  - Each of participants has blockchain
  - All blockchains become finally same by gradually synchronization

- **No master blockchain**: no centralized authority
  - Miners play very important role

**Blockchain network** (Overlay network on the Internet)

**BC**: Blockchain

**UA**: User Agent for blockchain network, ("wallet" in bitcoin)
Comparing to database

<table>
<thead>
<tr>
<th>In blockchain</th>
<th>In database</th>
<th>Additional explanation in terms of blockchain</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transaction</strong></td>
<td><strong>Insert query</strong></td>
<td><strong>Users can directly transact each other without needing intermediary</strong></td>
</tr>
<tr>
<td>Transaction: Tx1 (ex. 1btc From Alice to Bob)</td>
<td><strong>data</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Block** | (none) | **Made by miners**
| Block #N | verify and gather | **Excluding wrong transactions**
| Tx1 | Tx2 | Tx3 | Tx4 | **Connecting a new block needs difficult calculation**
| Tx5 | Tx6 | Tx7 | Tx8 |
| **Blockchain** | verify and form chain-like style | **(whole) Database** |
| Block #(N-1) | hash | **All history** |
| Block #N | hash | **Many participants have** |
| Block #(N+1) | hash | |
Data structure: transaction more detail

- All transfer history recorded by chain-like form
  - Proof of ownership (e.g. holding bitcoin)
- Only owner can issue new transaction because needing e-signature

Transaction: Alice -> Bob
- Bob’s address: pubkey
- Hash value of previous transaction
- Coin amount (in bitcoin)

Transaction: Bob -> Carol
- Carol’s address: pubkey
- Hash value of previous transaction
- Coin amount (in bitcoin)

Transaction: Carol -> Dave
- Dave’s address: pubkey
- Hash value of previous transaction
- Coin amount (in bitcoin)
Data structure: blockchain more detail

- Transactions are gathered as a block
- To approve as correct block, satisfying certain condition is needed
  - (In bitcoin,) First n digits of new block’s hash value must be zero
- Tamper-proof: every block after attacker’s target have to be regenerated

  - additional data to make first n digits of block’s hash value zero
  - Finding appropriate nonce is hard task (called **Proof-of-Work**)

(time-series data)
Summary of blockchain technology

• Blockchain has **high tamper-proof** feature
  - Chain-like form transaction and block
  - E-signature

• **Verification** at each stage increases security
  - Miners verify transactions and exclude wrong ones when making new block
  - Participants who have blockchain verify new block when synchronizing

• Blockchain technology is so simple that it can apply to various areas
How to apply blockchain technology and what can be achieved for Web-based content distribution
Motivation

- Sometimes, we must prove correctness of Web contents
  - Originality, permission and more...

- Conventional method of making a contract is taken time
  - Blockchain is suitable to record exchanges between two or more people
  - Enabling management by consortium style is consistent with Openness of the Web

Prove your originality!

Prove having permission!

I never agree your use!

My Boss

Me

Hmmm....

It’s pain...
Concept

- Metadata included in transaction can be used for agreements
  - This transaction becomes secure and transparent proof
- By using blockchain as timestamp, it helps to clarify originality
  - Existence of the content at certain time is proven

Transaction: Alice -> Bob
- Bob’s address: pubkey
- Hash value of previous transaction
- Agreements(License) as metadata

Alice’s e-signature
Use cases

- Proving correct use (i.e., having agreements)
- Proving contents originality
- [DEMO] Direct license control for contents creators
[DEMO]
Direct license control for content creators

In this demo, we use “BIG BUCK BUNNY”.
(c) copyright 2008, Blender Foundation / www.bigbuckbunny.org
Scenario

- System enabling control of encrypted content via blockchain
  - User gets encrypted content beforehand from internet
  - License and decrypt key requested to content owner
  - Blockchain works as public database to transfer license

Diagram:

- User requests encrypted content
- Owner grants license and decrypt key
- Blockchain network acts as a public database for transfer of许可 and key.

(bc = blockchain)
When transferring license and key

- **Secure transfer**
  - Blockchain open database, so anyone can get content key
  - Content key should be encrypted by user’s public key

- **Web-based interface by using MSE (Media Source Extensions) and Cryptography API**
Before open discussion
Our questions

1. What do you think about blockchain application for Web-based content distribution?
2. How about standardizing in W3C and What point?
   - BC Apps for Web-based content distribution itself?
   - Browser function (JS API) to access blockchain? (detail in next slide)

Blockchain technology

- Cryptocurrency (Payments)
- For Web-based content distribution
- IoT (smart contract)
- Certificate (Proof of Existence)
Our questions (cont.)

- Even if there are many types of blockchain application, common browsers functions might be needed.

1. Users access to UA by browser.

2. There is a possibility that user access local UA by using browser.

Blockchain network (Overlay network on the Internet)

- **UA**: User Agent for blockchain network, ("wallet" in bitcoin)
- **BC**: Blockchain

Centralized authority

Miners

User

UA (Local)

UA (Online)

User

User

User

Copyright©2015 NTT corp. All Rights Reserved.