



分散型元帳の実用に向けた開発現場の最前線

株式会社bitFlyer 代表取締役
加納 裕三



事業者としてのサービス紹介





会社紹介



株式会社bitFlyer

設立	2014年1月
資本金	8億3979万円（資本準備金含）
本社所在地	東京都港区赤坂
海外拠点	シンガポール、（ルクセンブルク：手続き中）
取引銀行	三井住友銀行
会計監査人	新日本有限責任監査法人
弁護士事務所	西村あさひ法律事務所、AZX総合法律事務所、創法律事務所
税理士法人	EY税理士法人
従業員	23人



投資家（一部掲載）



chainFlyer (ビットコイン・ブロックチェーン)



**bitFlyerならではのビットコイン・ブロックチェーン技術を可視化したツール
トランザクション、アドレス、ブロックの概念が理解できる**

chainFlyer (トランザクション)

トランザクション

e0eeda83b37e5d6c1626154fb9fabea257239246c1d7ecodaa09eba388ba2e61

送付額

957 確認

受信日時 2015/11/26 18:13:53 JST

サイズ 467 bytes

送信額 0.03630000 ₿

手数料 0.0001 ₿

ブロックの高さ 385408

送付元アドレス

送付先アドレス

Input

31q7iya4jZusaYCCkJMssxbEsbKMj1xidX 0.0364 ₿

Output

1K4X0ggSQ5hJ191LvrTqJ7sZ6qGygiFMh2 0.0335 ₿

31q7iya4jZusaYCCkJMssxbEsbKMj1xidX 0.0028 ₿

Input Scripts

```
OP_0
OP_PUSHDATA: 3044022001ffea6dc4e10120811c6cc3bb0a7cf3f0f5faa65a5e
a231d6286406a562043b022029d4cf7ae2245a3c673995e8d5a1fcc9df84565d
015d3a86aebac273cab9f1901
OP_PUSHDATA: 304402200308c42afa010813e2915c57cdecf766eeddd158c4a4
e897ebfc35d768e8455302207aff71bcd63926cbd1628b2b01ce8dd30a101d9
8d5580132f630dcf8079374f01
OP_PUSHDATA1: 5241041c4ec78ec3bb6125bc96c7dca290550ffdcf3512c766d0
fcf41a7892e9bcb0b8ccf84d449bf4d0d445c44c0f02f7454ff28c6b70ec37540
e8eedb7c3998e355f41045e5c0fcf4a159615f3b74b0bc3a8eff5ba0cd97a64e
fbd4a1dd2e5666478786ec4957ebfecacc487aa6293ce8a82caeec766f3974079
2672a5de119e056025b4104c96d495bfd5ba4145e3e046fee45e84a8a48ad05b
d8dbb395c011a32cf9f880326dbd66c140b50257f9618173833b50b6e829b5cd0
4ffd0ba693b90be80435953ae
```

Output Scripts

```
OP_DUP
OP_HASH160
OP_PUSHDATA: c61ca2f4511718155129978d16e66a47c2099235
OP_EQUALVERIFY
OP_CHECKSIG
使用済
```

```
OP_HASH160
OP_PUSHDATA: 01882b7530c6ba31f88c99580710cbbbd5e22820
OP_EQUAL
未使用
```

親トランザクション

ブロックチェーンの中身を分かりやすく公開

ブロックチェーン研究所



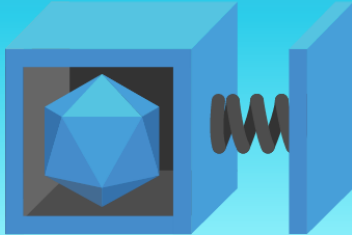
The screenshot shows the website for the Blockchain Research Institute. At the top, there is a logo consisting of a stylized 'b' with a colorful block inside, followed by the text 'ブロックチェーン研究所'. Below the logo is a search bar with the placeholder text 'ブロックチェーン検索' and a magnifying glass icon. Underneath the search bar is a paragraph of text: '当研究所ではブロックチェーンを活用した新サービスの研究開発をしています。bitFlyerの開発したブロックチェーンサービスを是非ご活用下さい。'. At the bottom of the page, there are four icons with corresponding labels: a magnifying glass over a group of people labeled 'ビットコイン監査ツール', a blue cube with a spring labeled 'バウンサー', a green pyramid and a pencil labeled 'ブロックチェーン・ライター', and an orange box with a smiley face labeled 'ブロックチェーン・ドキュメント'.

ブロックチェーンに関する研究開発成果の一部を公開しています

バウンサー

BOUNCER

1Bounce9TMxYae1W8jf3TgoZUsWzfqcGq4





Number of Transactions **71**

Bouncer will not bounce less than **0.00010546** ₿.

Estimated Balance
0.00121246 ₿

Confirmed Balance
0.00121246 ₿

6072a3da3acc57f6ddd0480f83af6816656a2c62e291f8c94ea2e49f156a3add
To ↓  1gjf7qakoSkGcp8nakJVeFdNGv4AZTfWe 2016/02/28 16:52:07 JST
- **0.00208900** ₿
Unconfirmed ▲

9f6f10b8ec5e87d774a10ed1842aeed644102968368ed054a24e1ff1ebff1d13
From ↑  1gjf7qakoSkGcp8nakJVeFdNGv4AZTfWe 2016/02/28 16:52:03 JST
+ **0.00208900** ₿
Unconfirmed ▲

ビットコインを送付すると送り主に戻ってきます
指定した金額（乱数）を送付することでPK（プライベートキー）を保有していることが証明できます
電子鍵などに応用できます

ブロックチェーン・ドキュメント

ブロックチェーン・ドキュメント



ブロックチェーンにファイルを残す

送り先アドレス

アップロードファイル

パスワード

パスワード（確認用）

※ファイルは一生残ります。削除、変更することは出来ません。ご注意ください。
※ファイルは20メガバイトまでです。
※同じアドレス宛のトランザクションに書き込む、ファイルを残せるのは10回までです。

送信

ブロックチェーンに残したファイルを探す

ファイルを選択

検索

**タイムスタンプ付きでファイルの存在証明ができます
改竄、削除が不可能なので、遺言、登記簿、契約書等に利用できます**



簡単なブロックチェーン紹介



電子署名されたメールのつながり

私は中本さんに100BTCをあげます。
その結果残高は400BTCとなりました。

ジョン

私はジョンさんから100BTCをもらいました。
私は佐藤さんに10BTCをあげます。

その結果残高は90BTCとなりました。

中本

私は中本さんから10BTCをもらいました。
私は黒川さんに10BTCをあげます。

その結果残高は0BTCとなりました。

佐藤

署名によりメールの内容が絶対に保証されており、過去のすべてのメールが保存されている。

メールをたどればすべての人の残高がわかる。

**ビットコインの世界では、
ブロックチェーンと呼ぶ**

ビットコイン・ブロックチェーンの実体

```
rw----- 1 1780320 Aug 18 10:32 rev00320.dat
drwx----- 2 4096 Aug 17 03:39 index
-rw----- 1 134113686 Aug 18 14:13 blk00321.dat
-rw----- 1 179268839 Aug 18 14:13 rev00321.dat
-rw----- 1 133452940 Aug 20 14:34 blk00322.dat
-rw----- 1 17781050 Aug 20 14:34 rev00322.dat
-rw----- 1 133882748 Aug 22 18:12 blk00323.dat
-rw----- 1 17841255 Aug 22 18:12 rev00323.dat
-rw----- 1 133695446 Aug 24 20:50 blk00324.dat
-rw----- 1 17813829 Aug 24 20:50 rev00324.dat
-rw----- 1 134205290 Aug 26 22:11 blk00325.dat
-rw----- 1 17929323 Aug 26 22:11 rev00325.dat
drwx----- 3 20480 Aug 26 22:11 .
-rw----- 1 16777216 Aug 26 23:39 blk00326.dat
-rw----- 1 1048576 Aug 26 23:39 rev00326.dat
drwxrwxr-x 5 4096 Aug 26 23:46 ..
: ~/.bitcoin/blocks$ bitls3
{
  "address" : "1oJcpLE6Y32LbjaPe1rBBT5Ycd",
  "account" : "",
  "amount" : 0.00000000,
  "confirmations" : 0,
  "txids" : [
  ]
}
ls0chl:~/bitcoin/blocks$
```

blockchain data ←

bitcoin ←

```
2015-08-27 00:09:23 receive version message: /bitcoinj:0.13.2/Bitcoin Wallet:4.39/: version 70001, blocks=371113, us=127.0.0.1:8333, peer=126057
2015-08-27 00:09:23 Added time data, samples 200, offset +0 (+0 minutes)
2015-08-27 00:09:50 socket send error Broken pipe (32)
2015-08-27 00:10:04 ERROR: AcceptToMemoryPool : nonstandard transaction: dust
2015-08-27 00:10:04 receive version message: /BitcoinJ:0.11.1/MultiBit:0.5.17/: version 70001, blocks=371681, us=127.0.0.1:8333, peer=126058
2015-08-27 00:10:04 Added time data, samples 200, offset +1 (+0 minutes)
2015-08-27 00:12:55 receive version message: /bitcoinseeder:0.01/: version 60000, blocks=230000, us=23.99.99.226:8333, peer=126059
2015-08-27 00:14:04 ping timeout: 1200.006856s
2015-08-27 00:14:15 receive version message: /Snoopy:0.1/: version 60001, blocks=0, us=23.99.99.226:8333, peer=126060
2015-08-27 00:14:22 receive version message: /getaddr.bitnodes.io:0.1/: version 70002, blocks=371681, us=23.99.99.226:8333, peer=126061
2015-08-27 00:15:13 receive version message: /bitcoinseeder:0.01/: version 60000, blocks=230000, us=23.99.99.226:8333, peer=126062
2015-08-27 00:15:38 receive version message: /bitcoinseeder:0.01/: version 60000, blocks=230000, us=23.99.99.226:8333, peer=126063
2015-08-27 00:15:57 socket recv error Connection reset by peer (104)
2015-08-27 00:16:20 receive version message: /Bitaps:0.0.1/: version 70002, blocks=0, us=23.99.99.226:36128, peer=126064
2015-08-27 00:17:13 ERROR: AcceptToMemoryPool : nonstandard transaction: dust
2015-08-27 00:17:49 receive version message: /bitcoinj:0.13.2/Bitcoin Wallet:4.39/: version 70001, blocks=371456, us=127.0.0.1:8333, peer=126065
2015-08-27 00:17:49 Added time data, samples 200, offset +0 (+0 minutes)
2015-08-27 00:18:54 UpdateTip: new best=000000000000000007ac4fd8155c6c219329025bbe48d4fcadcc59c5d1577e32 height=371682 log2_work=83.264225 tx=81307696 date
=2015-08-27 00:18:11 progress=0.999999 cache=8814
2015-08-27 00:18:14 receive version message: /getaddr.bitnodes.io:0.1/: version 70002, blocks=371681, us=23.99.99.226:8333, peer=126066
```

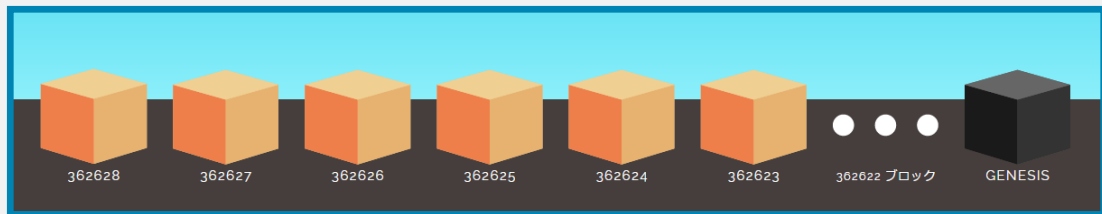
P2Pでそれぞれのコンピューター（Node）が情報を交換しています。

ビットコインは有体物ではなく、電磁的記録です。
ビットコイン・ブロックチェーンは普通のデータベースです。

データサイズは現在約50GB。P2Pで全世界の誰もが無料で共有できる（分散型）データベースです。
2009年1月からのすべての取引が記録されており、すべて公開されていることが特徴です。
稼働率は100%。システム開発、運用コストが10分の一にできる可能性を秘めた次世代のテクノロジーです。

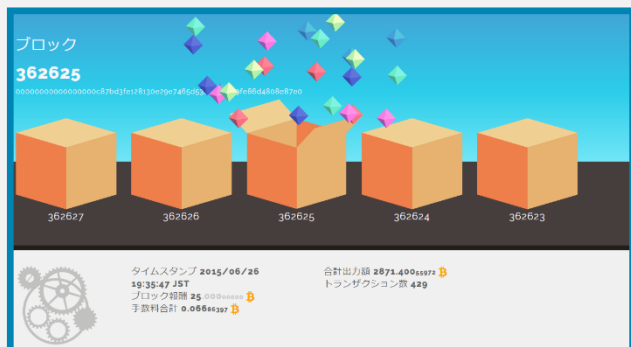
ビットコイン・ブロックチェーンの構成要素

ブロックチェーン：ビットコインの過去の全取引データ



一番右のGENESISブロックが歴史上最初にできたブロック
2009年1月4日 3時15分05秒 (JST)

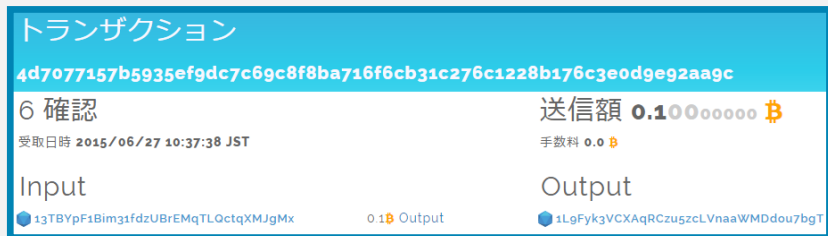
ブロック：約10分毎に取引をまとめたもの



アドレス：ビットコインの取引時に指定する口座番号



トランザクション（取引）：ビットコインの取引





金融機関を意識した活用例紹介

R3 CEV



- ・ NY本社のグローバル金融サービステクノロジー企業
- ・ 世界的大手金融機関42行とコンソーシアムを組成し、分散型元帳を活用した世界共通規格システムの研究開発を行う
- ・ 創業者であるDavid Rutter氏は2003年～2013年のICAP電子取引所運営部門のヘッド経験者

米NASDAQの動き

米ナスダック、未公開株式市場向けの基盤技術にブロックチェーンを導入

zakiyama 2015年5月12日 スタートアップ, ニュース, ビットコイン2.0, プロトコル, 企業, 取引所, 技術 0 Comments
 この記事の所要時間: 約3分

いいね! 16 ツイート 21 +1 3 Check LINEで送る Pocket




Hot Topics: ETFs | Retirement | Currencies | Online Broker Center

OUR COMPANY ▾
QUOTES ▾
MARKETS ▾
NEWS ▾
INVESTING ▾
ADVANCED INVESTING ▾

Search

マイナンバー制度対策が、必要なことをご存知ですか?

セキュリティ対策
社内研修・勉強会
マイナンバーの収集
安全管理実践

まずは、マイナンバーセルフチェックで、現況の確認を!

NTT 詳しくはこちら

US Market Closed Mar 1, 2016 CAC 40 4347.24 -85.59 ▼ -1.93% NIKKEI 225 16085.51 58.75 ▲ 0.37% FTSE100

Stock Market Activity

Index	Value	Change Net / %
NASDAQ	4689.60	131.65 ▲ 2.89%
NASDAQ-100 (NDX)	4333.61	132.49 ▲ 3.15%
Pre-Market (NDX)	4234.49	33.37 ▲ 0.79%
After Hours (NDX)	4334.43	0.82 ▲ 0.02%
DJIA	16865.08	348.58 ▲ 2.11%
S&P 500	1978.35	46.12 ▲ 2.39%
Russell 2000	1054.49	20.59 ▲ 1.99%

Data as of Mar 1, 2016 [View Major Indices](#)
 Try for Free: NASDAQ LiveQuotes Platform

NASDAQ Composite



Volume: 2 238 803 498

米NASDAQ は未公開株式市場向けのインフラテクノロジーとして、分散型元帳を導入することを最終目標とする分散型元帳技術イニシアティブを発足。

クレジットヒストリー

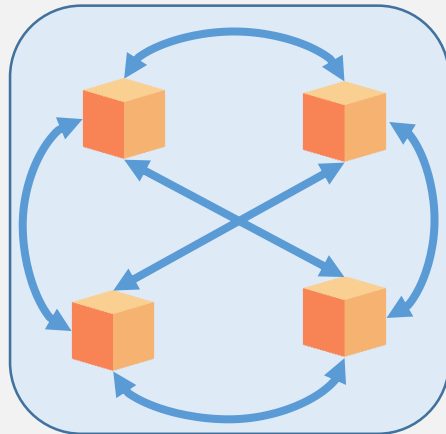
Bank



借入・返済履歴
売上・回収履歴
支払い履歴
決算情報
保有資産情報
担保設定情報等

・ 資金需要者の取引や資産の状態を記録します、信用情報のリアルタイム管理や履歴の確認ができます。

・ 事業者であれば特定の取引等によるクレジット悪化を捕捉でき、より実態に即した信用供与・融資審査に活用できます。



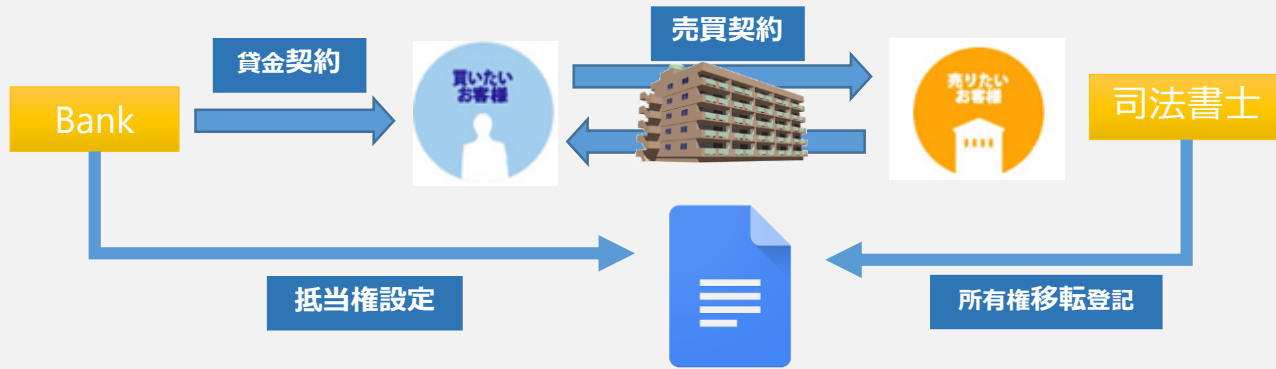
分散型元帳

運転履歴
事故履歴
購買履歴
SNS履歴
視聴履歴

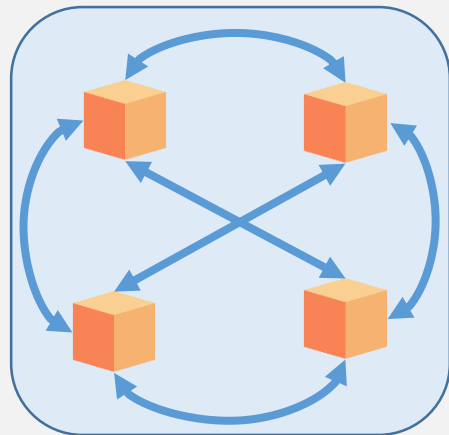
行動履歴

- ・ 個人情報はマスキングして供給
- ・ 情報提供者には仮想通貨で報酬が支払われる
- ・ 情報利用者は費用を負担する

不動産向貸出・売買・登記などへの分散型元帳活用



法務局



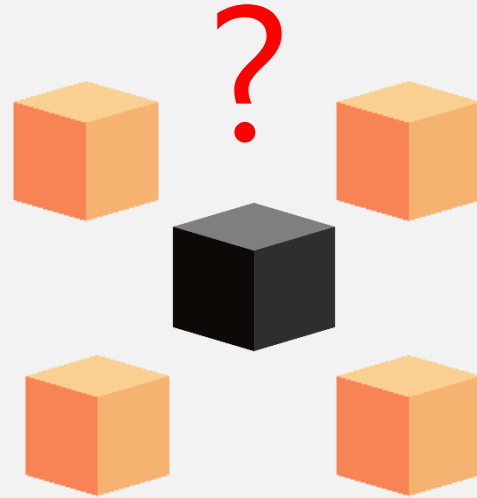
分散型元帳

・不動産売買契約は分散型元帳上で行われます。金銭支払いと所有権の移転、貸金契約・抵当権の設定が同時に行われます。金銭未払い、詐欺のリスクや第三者仲介等のコストが削減できます。

・情報は公開されており、誰にも改竄できません。法務局で所有権移転登記をする必要がなくなる日が来るかもしれません。

bitFlyer Blockchainのご紹介

次世代Fintech : BaaS (Blockchain as a Service)



- ・ 2年間のパブリックチェーン運用実績を元にブロックチェーンを再構築しました。
- ・ 複数のアプリケーションを一つのプラットフォームで実現します。
- ・ 高速にトランザクション処理が可能です。
- ・ 高可用性を実現し、開発・運用コストを大幅に低減することが可能です。

Q&A

