



「そうだったのか！」ビットコインとブロックチェーン  
(有料セミナーのご案内)

プロファウンド・デザイン・テクノロジー株式会社

◆セミナーの目的

ブロックチェーン上で動く DApps(Decentralized Applications : 分散型アプリケーション)は、WWW(World Wide Web)以来の技術革新だと言われています。

DApps 技術を使えばプログラムあるいはプログラム中の変数やイベントをネットワーク上の各コンピュータで共有（保存）し、各コンピュータから変数の値を書き換えたり、イベントを検知して何か処理したりする、といったシステムをサーバーの設立になし簡単に開発することができます。

DApps ではプログラムやデータ（変数）はネットワーク上のブロックチェーンに半永久的に保存され、改ざんやネットワーク障害等に対して非常に堅牢です。またネットワーク上で半永久的にプログラムの実行を継続させるといったことも可能となります。

このような中、ブロックチェーンをビジネス上どのように利用するかについて検討する場合、まずはブロックチェーン技術について正しく理解することが不可欠です。ブロックチェーン技術に対する正しい理解がないと従来のサーバー・クライアント型で開発した方がよいケースに対してまでわざわざブロックチェーン技術を適用してしまう可能性があります。本セミナーではブロックチェーン技術の代表的な利用例である仮想通貨ビットコインを題材として、「なるほど、そうだったのか！」と納得できるようブロックチェーン技術の本質について解説します。

ビットコインやブロックチェーンの技術的な本質を理解すればその応用(例えば DApps)についても容易に理解できるようになります。これからブロックチェーン技術関連の調査をご検討されている方にとっても本セミナーは入門編として最適です。また、マイニングの主目的はデータ改ざんの防止だ、と勘違いしている方もぜひセミナーにご参加頂ければと思います。

なお本セミナーはビットコイン、ブロックチェーンを技術的な側面から解説することを目的としています。ビットコインへの投資を勧めるセミナーでは決してありません。

◆セミナー主催者

プロファウンド・デザイン・テクノロジー株式会社

◆対象受講者

以下のような方を対象としています。

- ・ビットコインとは何かについて知りたい方
- ・ビットコインやブロックチェーンについて調べたが結局多くの疑問が残っている方
- ・マイニングの主目的はデータ改ざんの防止だと勘違いしている方
- ・ブロックチェーンを自社ビジネスに利用できないかこれから検討される方

本セミナーはビットコインやブロックチェーンを技術的な側面から解説しますが、受講するにあたっては数学の知識やプログラミングに関する知識などは必要ありません。

◆セミナーの内容（1日：合計4時間）

<初級編>（2時間）

疑問はいろいろ残りますが、とりあえずビットコイン、ブロックチェーンの基本アイデアおよび全体像を把握します。

1. ビットコインの歴史
2. ビットコインは単なる送金台帳
  - 2.1 トランザクションとブロックチェーンの概要
3. みんなで送金台帳を管理
  - 3.1 ブロックチェーンへのトランザクション追加（マイニング）
  - 3.2 トランザクションの検証
  - 3.3 「合意（consensus）」という言葉の意味
  - 3.4 ブロックチェーンのフォーク（分岐）
4. 「仮想通貨」「ビットコイン」という単語

<中級編>（2時間）

初級編での疑問について明らかにするとともに、ビットコインにまつわるいくつかの事件について技術的な観点で解説します。

1. トランザクションの流れ
  - 1.1 ウォレット

秘密鍵と公開鍵

ビットコインアドレス

UTXO

1.2 トランザクションプール

1.3 ブロックのマイニング

2. フルノードと SPV ノード

2.1 ブルームフィルタ

2.2 マークルツリー

3. ハードフォークとソフトフォーク

4. 各種事件の詳細

4.1 Mt.Gox 事件

4.2 コインチェック事件

4.3 モナコイン事件

5. イーサリアムと DApps

<オプションで以下のセミナーも実施可能です（追加の受講料は不要です）> （1 時間）

マイニング用 ASIC 設計時の注意事項について説明します。

1. SHA-256

1.1 ブロックヘッダと difficulty

1.2 SHA-256 のアルゴリズムとハードウェア化対象

1.3 ソフトウェアとハードウェアの違い

2. マイニング用 ASIC 設計事例

2.1 LSI の消費電力とは

2.2 高位合成ツールを用いた設計

2.3 意外な結果

3. ビットコイン以外のマイニング

◆セミナー受講料

54,000 円/1 名（税込）（テキスト代込）

◆開催場所

プロファウンド・デザイン・テクノロジー(株)オフィス内会議室(JR 新横浜駅 徒歩 4 分)

◆開催日時

随時開催しています。

セミナー参加ご希望の方は下記までお問い合わせ下さい。

[seminar@profound-dt.co.jp](mailto:seminar@profound-dt.co.jp)

◆オンサイトセミナー

お客様ご指定の場所にお伺いしてセミナーを実施することも可能です。

最少催行人数は4名です。

◆問い合わせ先

[seminar@profound-dt.co.jp](mailto:seminar@profound-dt.co.jp)

◆セミナー講師

プロファウンド・デザイン・テクノロジー株式会社 代表取締役 塚本泰隆

(経歴)

株式会社リコー電子デバイス部門にてLSI設計用CADツールの開発および画像処理ASICの設計に従事したのち、2011年に独立しプロファウンド・デザイン・テクノロジー株式会社を設立。2015年にビットコイン・マイニング用ASICの設計に携る。現在は、SystemC および高位合成技術を用いたLSI設計を中心に事業を展開。また、DSM(ドメイン・スペシフィック・モデリング) 事業も展開中。