



ブロックチェーンで世界を簡単に。

CeFiから見たDeFiー革新性と課題

株式会社 bitFlyer Blockchain
株式会社bitFlyer
金光 碧

2020年11月12日



目次

1. DeFiとの出会いとCompoundの紹介

2. DeFiの定義、各種DeFiの紹介

3. CeFiとDeFi

4. DeFiと日本法

5. 暗号資産取引所とDeFi

6. DeFiの技術的課題

7. DeFiと金融規制（特にAMLCFT）



1. DeFiとの出会いとCompoundの紹介



自己紹介 - 前職でやっていた仕事、今やっている仕事など

数理統計勉強後、10年間外資系証券会社の投資銀行部門でデリバティブの設計に従事。2016年から仮想通貨/ブロックチェーン業界にいます。数学的仕組みもので今までできなかったことができるという事象が好きです

現在bitFlyer / bitFlyer Blockchainでやっている仕事など



本日お話しする内容は
個人の見解であり
所属組織の見解ではありません。

※DeFiの師匠：平野さん、信玄さん、堀さん、斎藤創先生
(DeFi最新情報等についてはそんなに詳しくないです)
※この資料では「仮想通貨」と呼んでいますが法的には「暗号資産」が正しい用語です

- 2006年から外資系証券会社の投資銀行部門資本市場のデリバティブ担当者（株式、為替、クレジットなど）
- 2016年1月からbitFlyerで勤務。CFO & PRという肩書でなんでも屋さんとして働く
 - 2017年9月の株式会社bitFlyerの仮想通貨交換業登録
 - 2018年以降の態勢整備
- 現在はbitFlyerのトレジャリー部長。担当範囲は以下
 - 分別管理
 - ウォレット管理
 - 自己資本規制比率管理
 - 在庫ポジション/リスク管理
 - 資金管理
- bitFlyer BlockchainではIR/IP（知財）担当の取締役

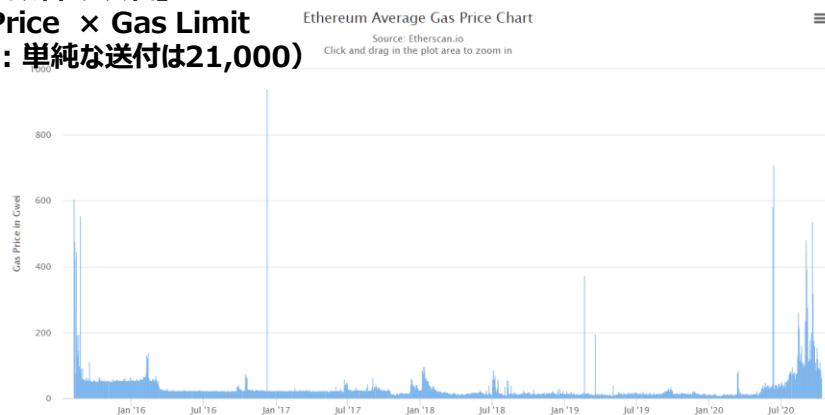


DeFiを調べ始めたきっかけ – Ethereumガス代の高騰

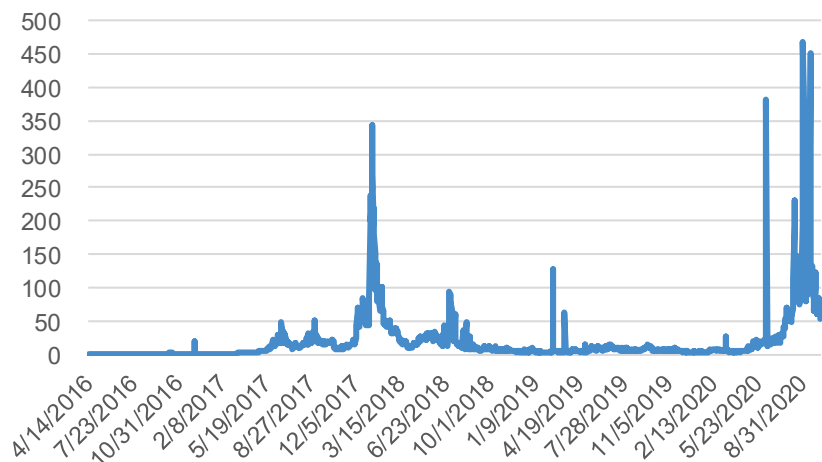
2020年6月頃からETHの送付手数料である「ガス代」が高騰。ETH、ERC20トークンの送付に時間がかかるようになり、当社が支払う手数料も高騰。暗号資産交換業者もDeFiに注目せざるを得ない状況に

ETHガス代の高騰

手数料「ガス代」
= Gas Price × Gas Limit
(GasLimit : 単純な送付は21,000)



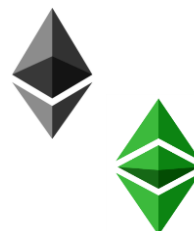
(円) GasLimit=21,000の際のガス代 (円換算)



ETH価格、マイナー手数料の推移



2020/6/16
COMPトークンの配布



ERC20 Tokens

Basic Attention Token (BAT)	Bread (BRD)	Civic (CVC)
EOS (EOS)	Funfair (FUN)	Golem (GNT)
Kyber Network (KNC)	Numeraire (NMR)	OmiseGo (OMG)
TenX (PAY)	Quantum Resistant Ledger (QRL)	Augur (REP)
0x (ZRX)		



“Compound”について

1. 借りたい人と貸したい人のモチベーション、株式市場における仕組み

Compoundは仮想通貨版日証金のようなもの。株式市場においては株式を貸したい人と借りたい人のモチベーションがそれぞれあり、証券会社、証券金融会社（東証が指定する証券金融会社が日証金）を通して信用取引、貸借取引が行われている

株を貸したいと借りたい人のモチベーション

株を貸したい人

- 長期のストラテジーを組んでいる機関投資家
- 大株主、オーナー



短期的な株価変動は気にせず長期で保有。保有期間中に貸し出して利回りを稼ぎたい！

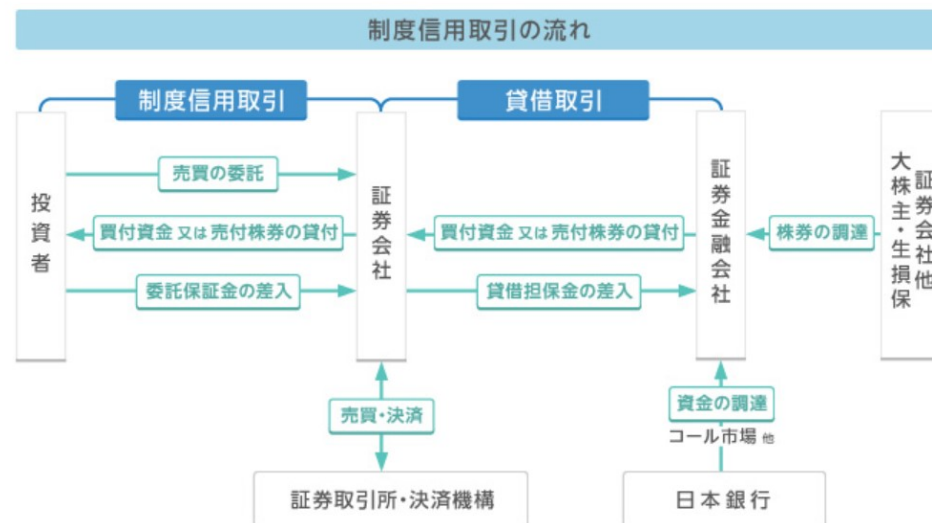
株を借りたい人

- 株価が下がっていると思っている機関投資家



今100円の株価が分析では70円まで下がる！
借りた株を売って、
株価が下がったところで
売って返そう！

株式市場におけるプラットフォーム



出所：東京証券取引所

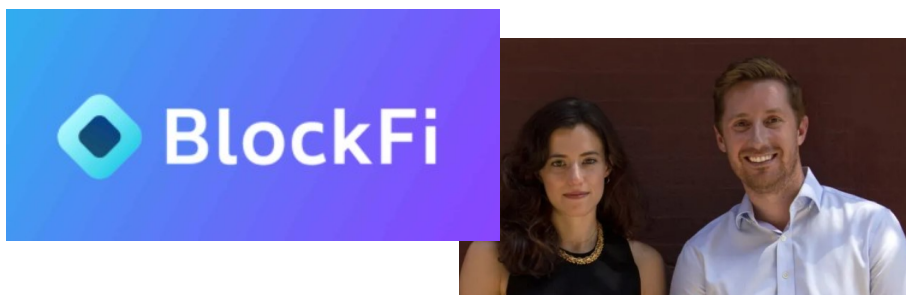


“Compound”について

2. 仮想通貨の貸し借りプラットフォームを運営する会社

仮想通貨のレンディングを行う会社はいくつか存在。米国ではBlockFi、Genesis、Anchorageなどが必要な規制に遵守して運営している。借り手は機関投資家等。Genesisでは一部会社による運用も実施（開示情報による）

—— 仮想通貨のレンディングを行うCeFi（Centralized Finance=普通の株式会社が運営するもの） ——



- 直近1年間でもモルガンクリークキャピタルなどから1億ドルを調達している未上場ベンチャー企業
- USにおいてライセンスを取得してレンディング、仮想通貨担保ローンを提供している（AMLCFT態勢も求められる）
- レンディングにおける借り手は自己勘定トレーダー、マーケットメーカーとされている

BlockFi Interest Account (BIA)

Annual Percentage Yield (APY)*

BlockFi Interest Account clients can deposit their crypto and earn interest. Paid out at the beginning of every month, the interest earned by account holders compounds, increasing the annual yield for our clients.

※APY = Annual Percentage Yield

Currency	Amount **	APY
BTC (Tier 1)	0 - 2.5	6%
BTC (Tier 2)	> 2.5	3.2%
ETH	> 0	5.25%
LTC	> 0	5.0%
USDC	> 0	8.6%
GUSD	> 0	8.6%
PAX	> 0	8.6%
PAXG	> 0	4%
USDT	> 0	7%

Licenses

State	License Type	Agency	License #
AL	Consumer Credit License	Alabama State Banking Department	100163229
AL	Money Transmitter License	Alabama Securities Commission	
CA	Finance Lender and Broker License	California Department of Business Oversight	60DBO 81955
CO	Supervised Lender's License	Colorado Department of Law	993426
CT	Money Transmitter License	State of Connecticut Department of Banking	
DC	Money Transmitter License	Government of the District of Columbia Department of Insurance Securities and Banking	MTR1873137
FL	Money Services Business License	Florida Office of Financial Regulation	FT230000280
GA	Seller of Payment Instructions	Georgia Department of Banking and Finance	69065
IL	Money Transmitter License	Illinois Department of Financial & Professional Regulation	MT.0000372
IL	Consumer Installment License Certificate	Illinois Department of Financial & Professional Regulation	CI.0004435-H
KS	Supervised Loan License	Kansas Office of the State Bank Commissioner	SL.0026692



“Compound”について

3. 仮想通貨の貸し借りプラットフォームを運営する会社、CREDのChapter11申請

仮想通貨のレンディングを行う会社の一つである米国のCREDが11月7日にChapter11（米国破産法の中の処理方法の一つで、日本の会社更生法と民事再生法の中間的な存在）を申請したことが報道された

CREDの会社概要とChapter11申請

Case 20-12837 Doc 1 Filed 11/07/20 Page 1 of 15

Fill in this information to identify the case:

United States Bankruptcy Court for the:
District of Delaware
(State)

Case number (if known): _____ Chapter 11

☐ Check if this is an amended filing

Official Form 201
Voluntary Petition for Non-Individuals Filing for Bankruptcy 04/20

If more space is needed, attach a separate sheet to this form. On the top of any additional pages, write the debtor's name and the case number (if known). For more information, a separate document, Instructions for Bankruptcy Forms for Non-Individuals, is available.

1. Debtor's Name Cred (US) LLC

2. All other names debtor used in the last 8 years
N/A
Include any assumed names, trade names, and doing business as names

3. Debtor's federal Employer Identification Number (EIN) 83-1785799

4. Debtor's address

Principal place of business		Mailing address, if different from principal place of business	
Number	Street	Number	Street
<u>3 East Third Avenue</u>			
<u>Suite 200</u>			
<u>San Mateo, California 94401</u>			
City	State Zip Code	City	State Zip Code
<u>San Mateo</u>			
County			

Location of principal assets, if different from principal place of business

5. Debtor's website (URL) https://mycred.io

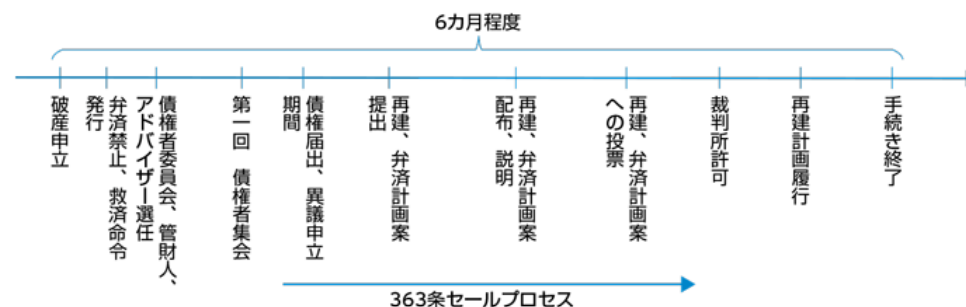
6. Type of debtor ☒ Corporation (inc) ☐ Partnership (ex) ☐ Other. Specify:

What is my current balance? What is my pre-petition balance?

 Written by Cristiane Ferreira
Updated this week

Cred cannot provide current balances outstanding at this point because it is in the process of reviewing all of its records and separating pre- and post-petition invoices. However, Cred will be filing a "Schedule of Assets and Liabilities." In this document, Cred will list balances it believes are owed to its creditors. If you have further questions about this, please contact your own legal and financial advisors.

- CREDはライセンスを持ち183か国で顧客にサービスを提供する、仮想通貨レンディングを行う事業者。PayPal出身者が起業している
- 詐欺と不正があり、債務超過に陥ったことを認めた。資産US\$50 – 100mmに対して負債US\$100 – 500mm
- 仮想通貨の預け入れと引き出しを止めた上でChapter11を申請した
- 顧客が預けた仮想通貨の何割が弁済されるかは現時点では不明



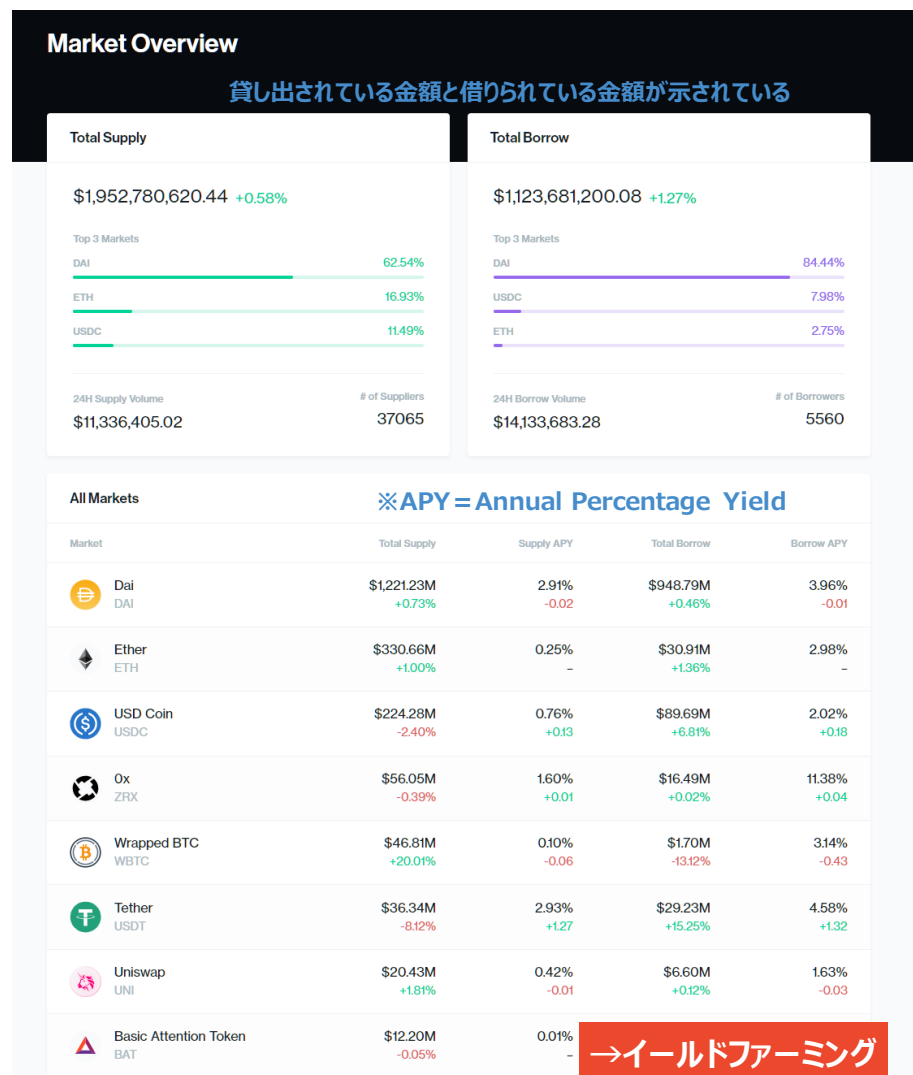


“Compound”について

4. 無人仮想通貨の貸し借りプラットフォーム（プログラムのみ） = Compound

Compoundはスマートコントラクト上で仮想通貨の貸し借りができるプラットフォーム。貸す人は仮想通貨を貸し出すことで利回りを得る。借りたい人は担保の範囲内で金利を支払って仮想通貨を借りる。清算の仕組みも設計されている

Compoundにおける 貸し手と借り手への金利



Compoundにおける 「超過担保」と清算の仕組み

- ユーザーはスマートコントラクトに仮想通貨をロックし、設定されたレートでcTokenを受け取る
- ユーザーはcTokenを保有することで利息を獲得できる
- ユーザーはcTokenを担保として預け入れることで暗号資産の借り入れが可能。担保に対する最大借入額の掛け目は預託した暗号資産によって決められる
- ユーザーの借り入れ残高が借り入れ能力を超えた場合、提供された担保はその時点の市場価格からの割引を行った上で清算される
- さらに、借り手が支払った金利のうち10 – 15%はSponsor Equityという名目で基金としてプールしていき今後万一貸し倒れが発生したとしてもこれを財源として賄うという仕組みになっている

おすすめの
記事

担保から考えるDeFiと既存金融 の違い



KanaGold Follow

Mar 13, 2019 · 9 min read



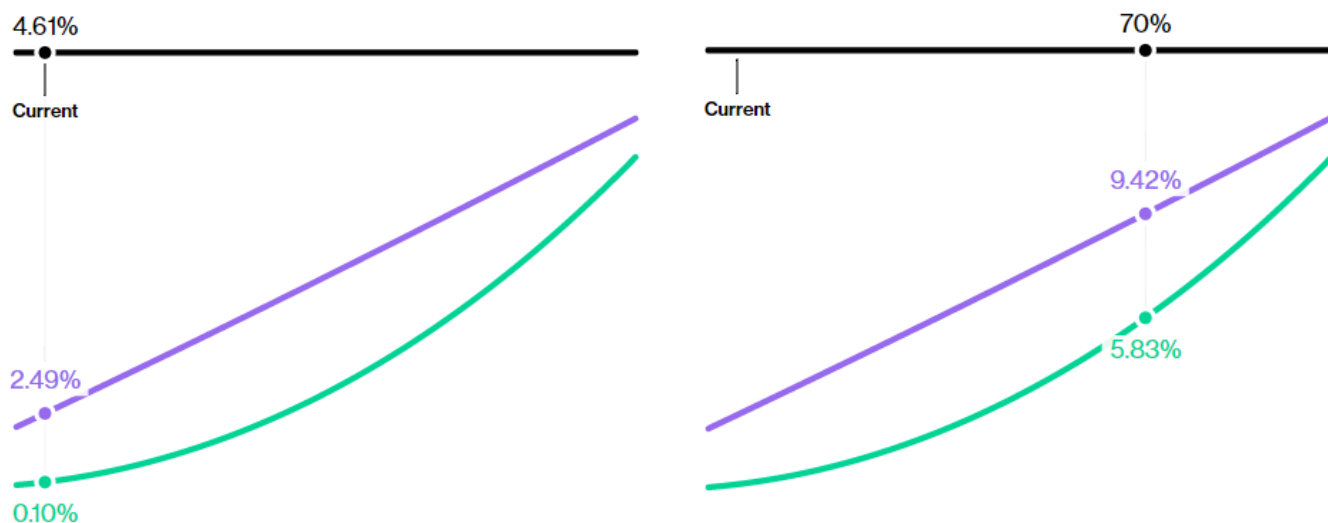


“Compound”について

5. 貸出金利、借入金利の決定方法

Compoundでは借入金利と貸出金利は需給によって決定するが、SUPPLYに対するBORROWの割合に応じて金利が事前に決まっており、Web上で公開されている。その他の要素も公開されており透明性が高い

Compoundにおける 貸出金利、借入金利の決定 (ETH)



- Compoundにおいては「SUPPLY」されている（＝貸し出されている）仮想通貨の何%が「BORROW」されている（＝借りられている）かによって貸出金利、借入金利が決定される。この割合と金利の関係はWebで公開されている
- 借入金利の何%がReserve Factorとなる（Sponsor Equityとしてプールされる）か、貸したETHの時価の何%の仮想通貨を借りることができるかも公開されている

Compoundにおける ETHの各種設定

Market Details

Price	\$459.74
Market Liquidity	1,099,513 ETH
# of Suppliers	32875
# of Borrowers	680
ETH Borrow Cap	No Limit
Interest Paid/Day	\$1,666.73
Reserves	95.27 ETH
Reserve Factor	10%
Collateral Factor	75%
cETH Minted	57,544,561
Exchange Rate	1 ETH = 49.92873907917052 cETH



“Compound”について

6. Compoundにおけるガバナンスとガバナンストークン

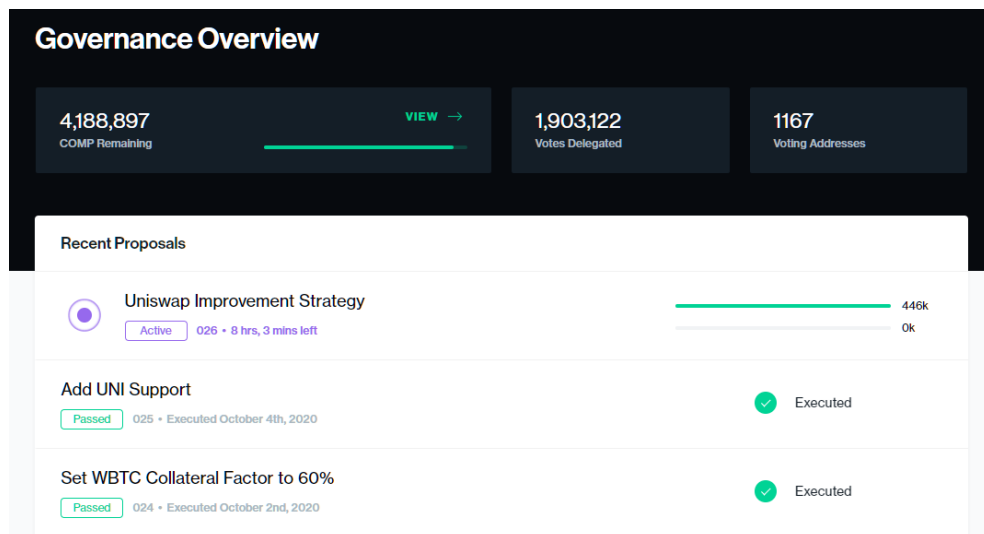
CompoundのプラットフォームはCOMPトークン保有者による投票で運営されている。当初は開発者グループのみが保有していたが、2020年6月16日以降ユーザーに配布。現在（11/12）「COMP」の時価総額は463億円相当

Compoundにおけるガバナンス

※COMP：ERC20トークン。Compoundプラットフォームにおける投票権

ガバナンスのプロセスとして、COMP保有者からの直接投票のほか、COMPを保有していないユーザー（当該ユーザーのアドレス）に委任することも可能。

COMPを保有するステークホルダーが会社の経営者になって、プロトコルの管理者となり、様々な提案を採決する仕組み。



→リクイディティ・マイニング

ガバナンストークン「COMP」



COMPはプラットフォームを利用するユーザーに配布する形で市場に放出。

2020年6月16日に初回の配布が行われて以降、毎日計2880COMPがCompound上の8つのレンディング市場に充てられる。

COMPをリアルタイムで受け取るのは、それぞれのレンディング市場で利息を貯めているユーザー（借主と貸主に50%ずつ）。8つのレンディング市場は、ETH、DAI、USDC、USDT、BAT、REP、WBTC、ZRXの銘柄の貸し仮想通貨マーケット。

今後4年間で計420万COMPを配布する予定で、COMPリザーブの42%に当たる。



2. DeFiの定義、各種DeFiの紹介



DeFiの定義

「DeFi」には明確な定義はありませんが、今日は「主にイーサリアムなどのスマートコントラクト上で稼働する分散型金融システム、アプリケーション」としてお話します

FSBによる 「分散金融技術」の定義

金融サービス提供における1つ以上の仲介者や中央集権化されたプロセスの必要性を低減または排除する可能性のある技術
FSB報告書“Decentralised financial technologies”

分散金融システム

分散型金融技術がもたらしうる（既存の中央集権型金融システムとは異なる）新たな金融システム

DeFi

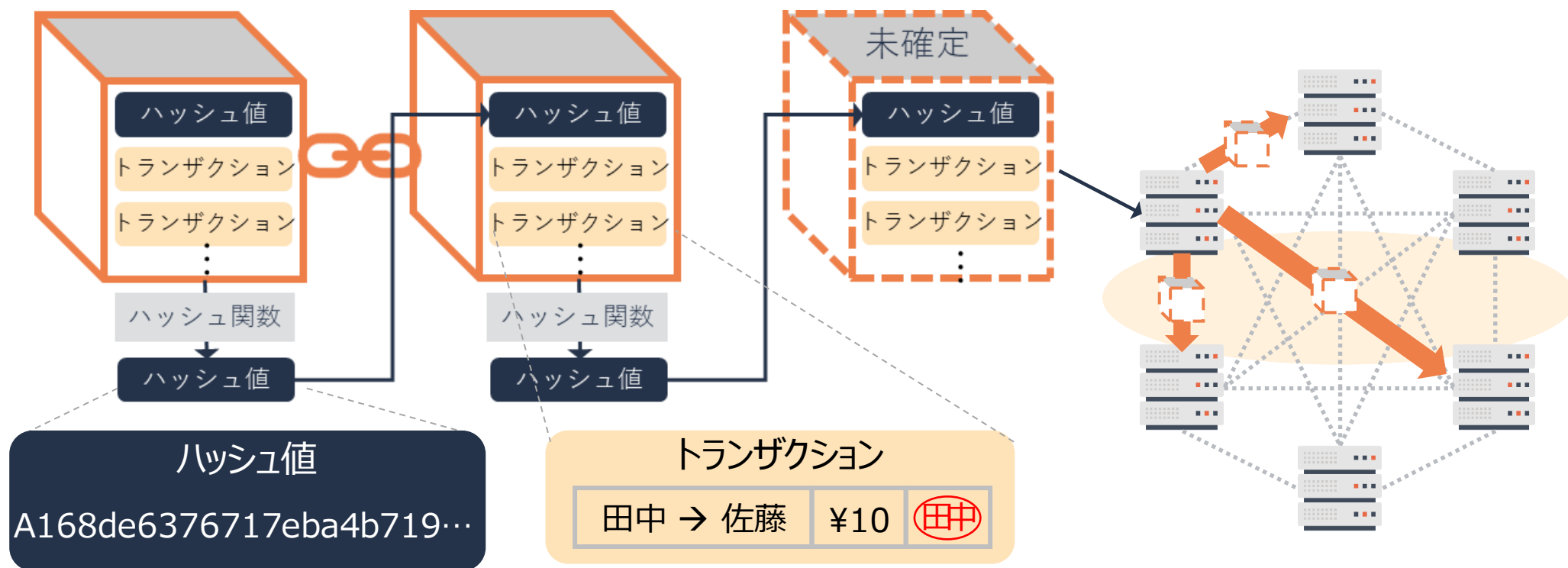
- 分散型金融システムの一部を構成するアプリケーション
- Uniswap, Compound, Maker etc.
- アプリケーションにより分散化の類型・程度は様々
- 完全分散型に近いユースケース（例：Bitcoin）と比較すると分散の程度は低いものもある





ブロックチェーンを構成する技術的要素

ブロックチェーンは様々な技術の組み合わせで出来ている。これらの技術から生まれる特徴により、参加者同士でデータを共有化するオープンな仕組みを作ることが可能となる



ハッシュチェーン

- 1つ前のブロックの情報からハッシュ関数を用いてランダムな文字列(ハッシュ値)を生成

電子署名

- 送信者が取引記録を作成し、秘密鍵でトランザクションに署名
- 他者は送信者の公開鍵で署名の検証が可能

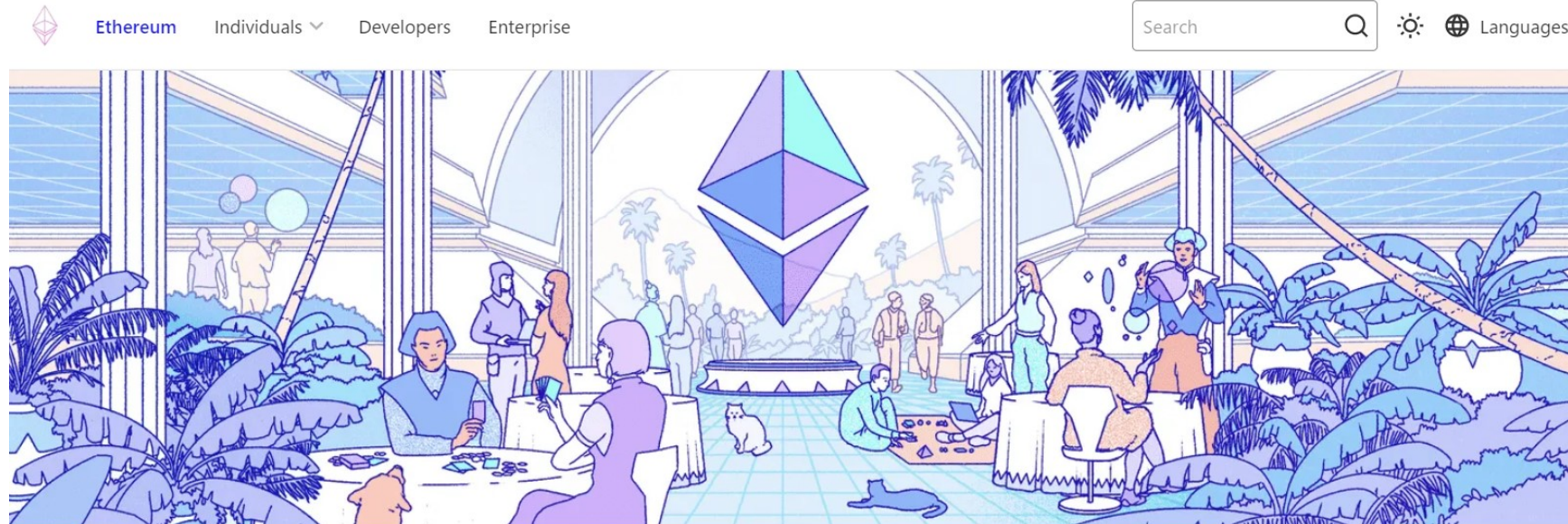
コンセンサス アルゴリズム

- 複数のノード間で取引の正当性を検証、永続化への合意
- P2P取引の実現



ビットコインとイーサリアム

イーサリアムは「ワールドコンピューター」を目指したもの。ビットコインは「送金」しかできないプロトコルだが、イーサリアムはあらゆることを処理できるようにすることを目指している



Ethereum is a global, open-source platform for decentralized applications.

אתריום

On Ethereum, you can write code that controls digital value, runs exactly as programmed, and is accessible anywhere in the world.

- イーサリアムは、“Blockchain App Platform”、ブロックチェーン上に構築されるアプリケーションのプラットフォームとなることを目的として作られている
- イーサリアムは、ワールドコンピュータになることを目的としているため、ビットコインにはない「Turing Completeness（チューリング完全性）」という特徴を持っている
- チューリング完全性：あらゆる処理を実行できる計算能力を備えている性質
- ビットコインがチューリング完全性を備えていない理由は、ビットコインは通貨として利用されることを目的として Satoshi Nakamotoにより考案されているため、通貨としての利用に関係する処理だけを行うことができればよい



スマートコントラクトとは

イーサリアムの上に構築できる「スマートコントラクト」の特徴として、分散ネットワークに対してプログラムコードを第三者に検証可能な形でデプロイ・運用して自動執行できるという点がある

スマートコントラクトとは、一般的にブロックチェーン上にデプロイされるプログラムコードを指す。日本語では契約の自動執行と説明されることが多いが、この表現はスマートコントラクトの特性の一部のみを表している。分散ネットワークに対してプログラムコードを第三者に検証可能な形でデプロイ・運用して、かつ自動執行できる点にこそ新規性があると言える。

通常のプログラム



インプット

サーバーやハードウェアの
プログラムが処理

アウトプット

150円でコーラを買いたい。
500円をいれる。

在庫の確認・売上の計上・
お釣りの計算を行う。

コーラとおつりの350円
を出力する。

ユーザーや第三者からはどのようなプログラムが動いているかは分からない。閉じられたサーバー内やコンピュータでプログラムが実行される。この自動販売機はちゃんとコーラとおつりを返すだろう、という信用に基づいている。

スマートコントラクト



インプット

ブロックチェーン上の
プログラムが処理

アウトプット

150円でコーラを買いたい。
500円をいれる。

在庫の確認・売上の計上・
お釣りの計算を行う。

コーラとおつりの350円
を出力する。

どのようなプログラムが動いたかを第三者が検証可能である。この場合、150円でコーラを販売するプログラムであることや、お釣りを返すロジックも組み込まれていることが検証可能。不正ができず透明性があるプログラムが実現する。

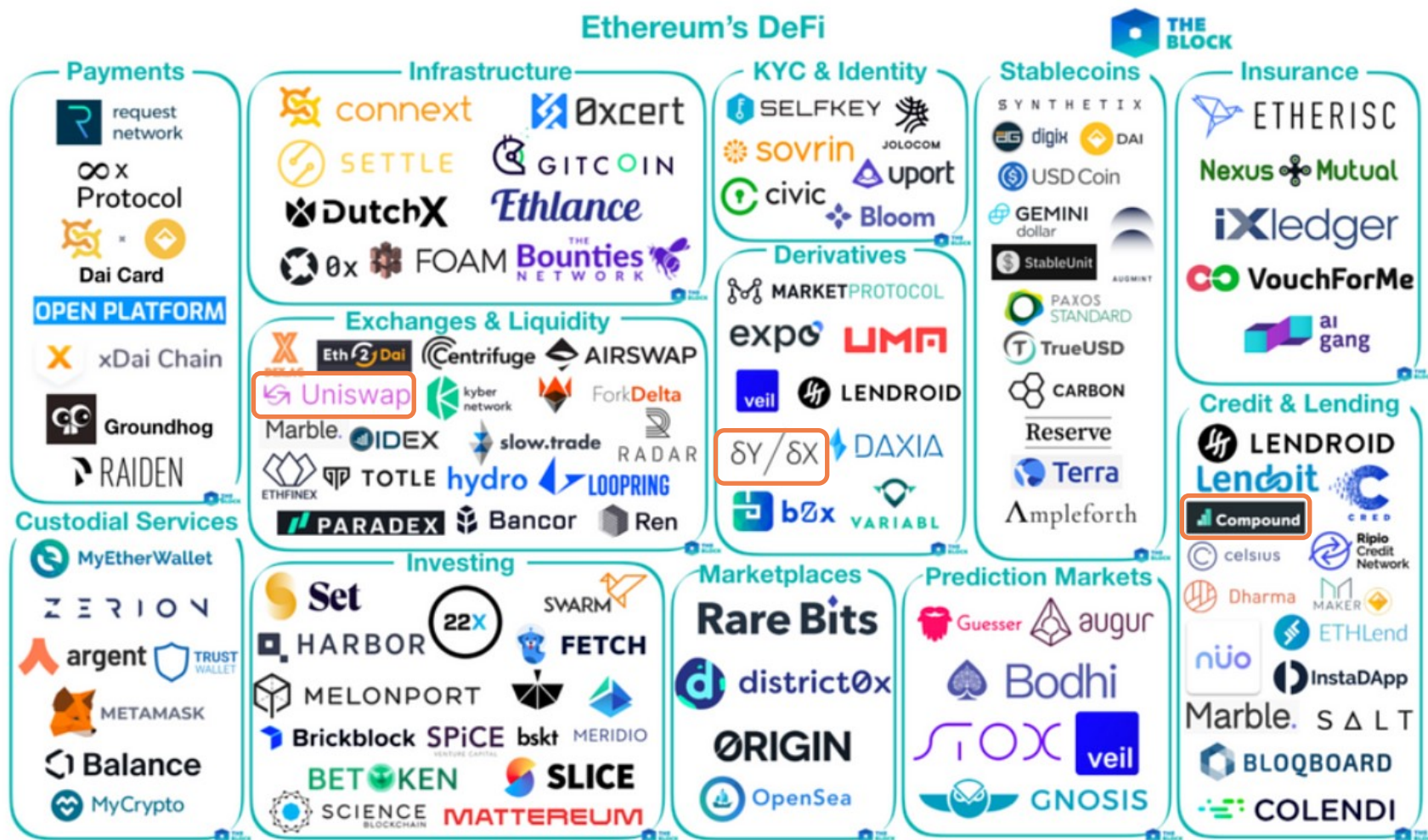
このページはHashhub平野さんの発表資料に基づきます



DeFiで実装される様々な金融機能

イーサリアムのスマートコントラクトを利用して様々な金融機能（取引所、デリバティブ、保険、レンディング、ペイメントなど）が実装されている

DeFiで実装されている金融機能（イーサリアム上のDeFi）





“Uniswap”について 無人仮想通貨取引所（プログラムのみ） = Uniswap

UniswapはAMM（Automatic Market Maker、自動マーケットメーカー）方式の暗号資産交換所機能。それまでの分散型取引所（DEX）は流動性が限定的で手数料が高い、不便なものだったがAMM方式になり改善

Uniswapにおける 売買画面

From

1

ETH ▾

To (estimated)

32.7491

BAL ▾

Price

0.0305352 ETH per BAL ↻

Connect Wallet

Minimum received ⓘ

32.58 BAL

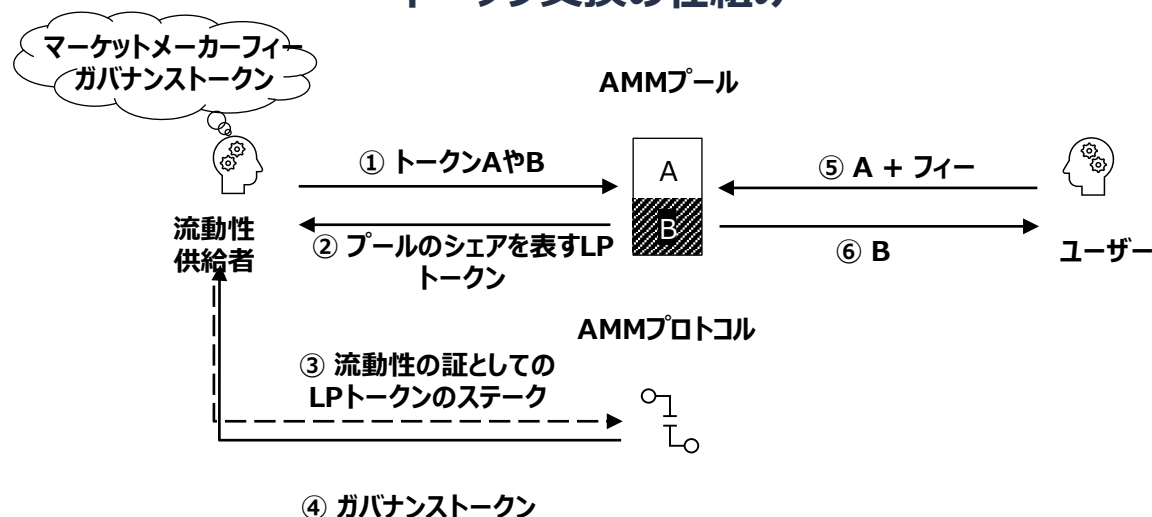
Price Impact ⓘ

0.15%

Liquidity Provider Fee ⓘ

0.003 ETH

Uniswap（AMM）における トークン交換の仕組み



既存DEXとUniswapの違い

	既存DEX（Kyber、0x等）	Uniswap（AMM）
流動性提供者	運営、提携先など	誰でも流動性提供可能
手数料収入	運営側で徴収	流動性提供者で分配
トークン上場	運営側で選定	自由に上場可能

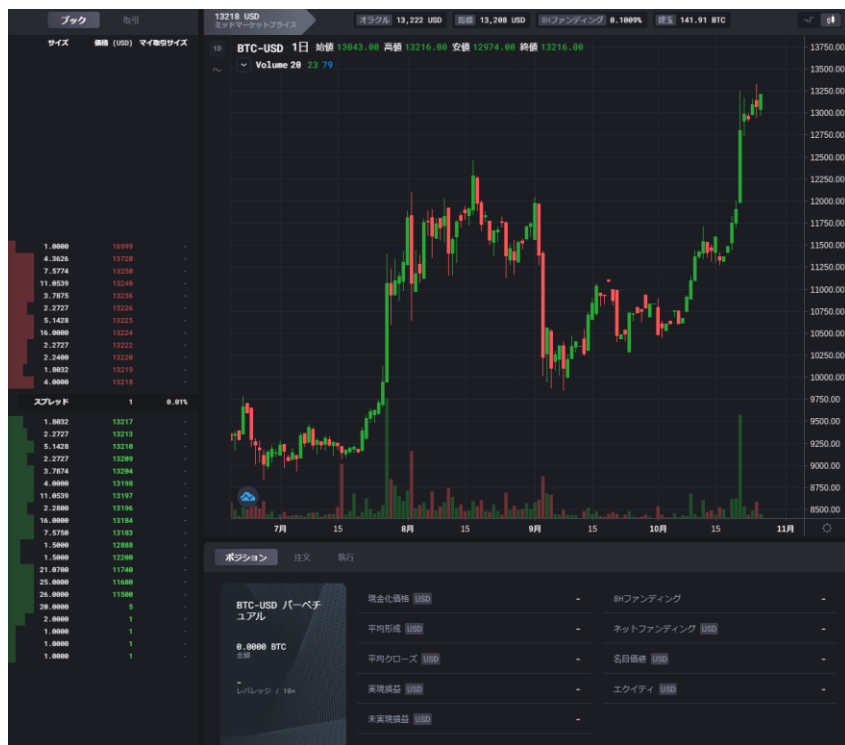


“dYdX”について

ほぼ無人仮想通貨デリバティブ取引所（オンチェーン+オフチェーン） = dYdX

dYdXはANDREESSEN HOROWITZ、BainCapital等から出資を受けているスタートアップ。仮想通貨のレバレッジ取引などを提供する。オーダーはオフチェーンで管理している

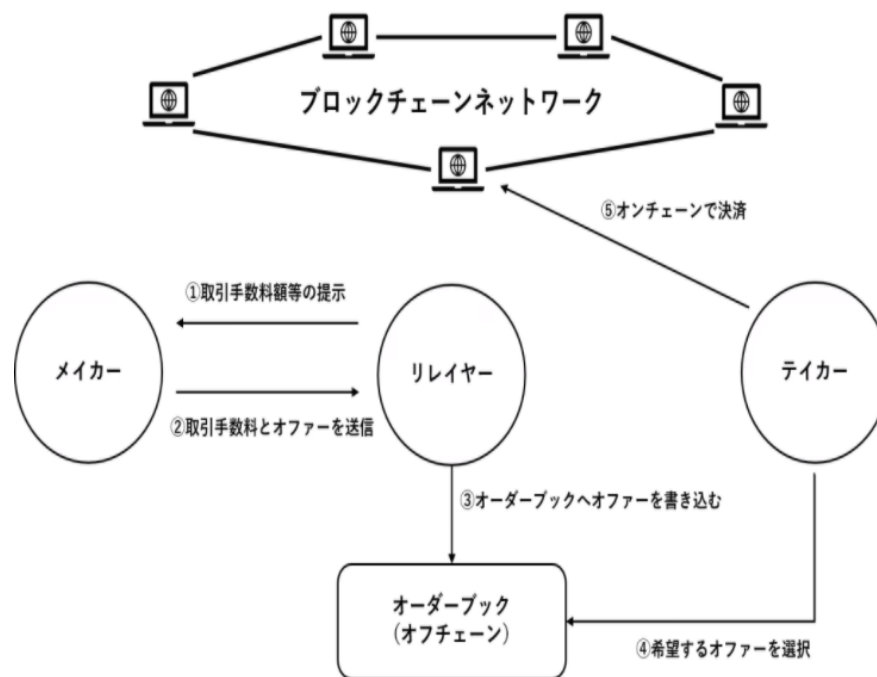
dYdXにおける トレーディングプラットフォーム



- ETH-DAI、ETH-USDC、DAI-USDCの現物取引、信用取引、貸出、借入及びBTC-USD、ETH-USD、LINK-USDのパーペチュアル・スワップ取引を提供（板方式）
- レバレッジは最高10倍

出所：dYdX、創・佐藤法律事務所

dYdXにおけるオンライン部分と オフライン部分



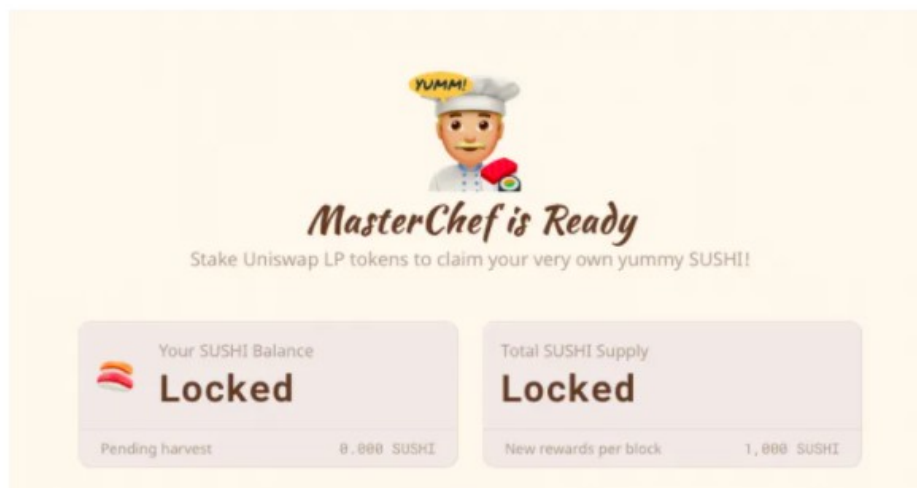
- 決済をオンチェーンで信用リスクをなくし、他方、注文をオフチェーンで行うことによりユーザーの手数料を抑え、処理スピードの向上を図る



【番外編】“Sushiswap”について 無人仮想通貨取引所Uniswapのコピー＝Sushiswap

ガス代の高騰に大きく影響したのがUniswapから派生したDEX(分散取引所)であるSushiswap。一時マネーゲーム的な様相を呈しランザクションが激増した

Sushiswapの概要



- SushiSwapでは、トークンのペアをプールしてくれるユーザーに対して、「Sushiトークン」というインセンティブを付与
- **Sushi**をもらうためのトークンペアを**SushiSwap**にプールする
→**Sushi**をもらい**Sushi**/ETHをプールする→さらに**Sushi**をもらい…
という行動をする人が増加。Transactionが激増

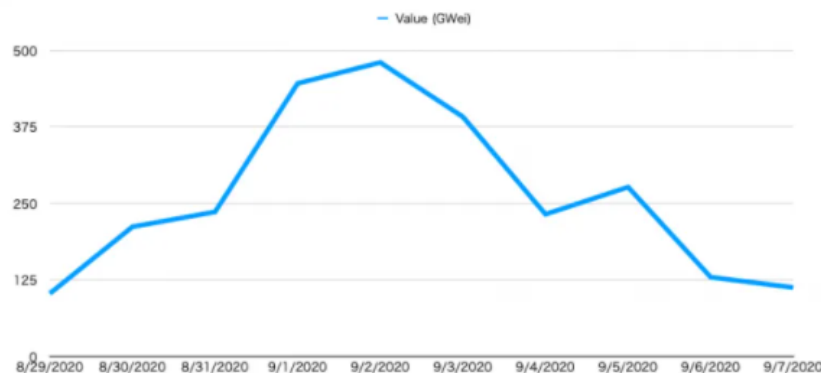
Sushiswap関連のイベント

- 8月29日：Sushiトークン配布開始
- 9月1日：SushiがFTXとBinanceに上場。先物取引も可能に
- 9月3日：Quantsstampのコード監査
- 9月5日：開発者NomiがSushiトークンを売却していたことを発表

SUSHIトークンの価格と ガス代の推移



Sushiのチャート（8月29日～9月7日）





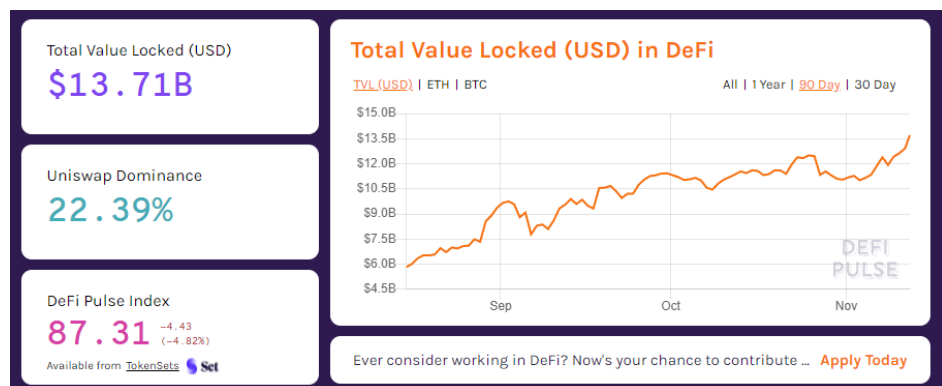
3. CeFiとDeFi



DeFiの市場規模

DeFiにロックされている金額は2020年6月以降急増し、足許では1.5兆円程度となっている。仮想通貨全体の時価総額が47兆円（そのうちビットコインが30兆円）であり、全体の3%程度

DeFiにロックされている金額の推移



DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
1.	Uniswap	Ethereum	DEXes	\$3.07B	3.77%
2.	Maker	Ethereum	Lending	\$2.27B	4.64%
3.	WBTC	Ethereum	Assets	\$1.95B	3.66%
4.	Compound	Ethereum	Lending	\$1.42B	6.05%
5.	Aave	Ethereum	Lending	\$1.21B	1.74%
6.	Harvest Finance	Ethereum	Assets	\$893.6M	86.98%
7.	Curve Finance	Ethereum	DEXes	\$870.0M	3.03%
8.	Syntheticx	Ethereum	Derivatives	\$682.5M	3.82%
9.	yearn.finance	Ethereum	Assets	\$371.6M	0.88%
10.	RenVM	Ethereum	Assets	\$348.3M	3.03%

仮想通貨の時価総額

Today's Cryptocurrency Prices by Market Cap
The global crypto market cap is ¥47677.77B, a **▲2.16%** increase over the last day. [Read more](#)

Bitcoin Casino.io **¥8000**

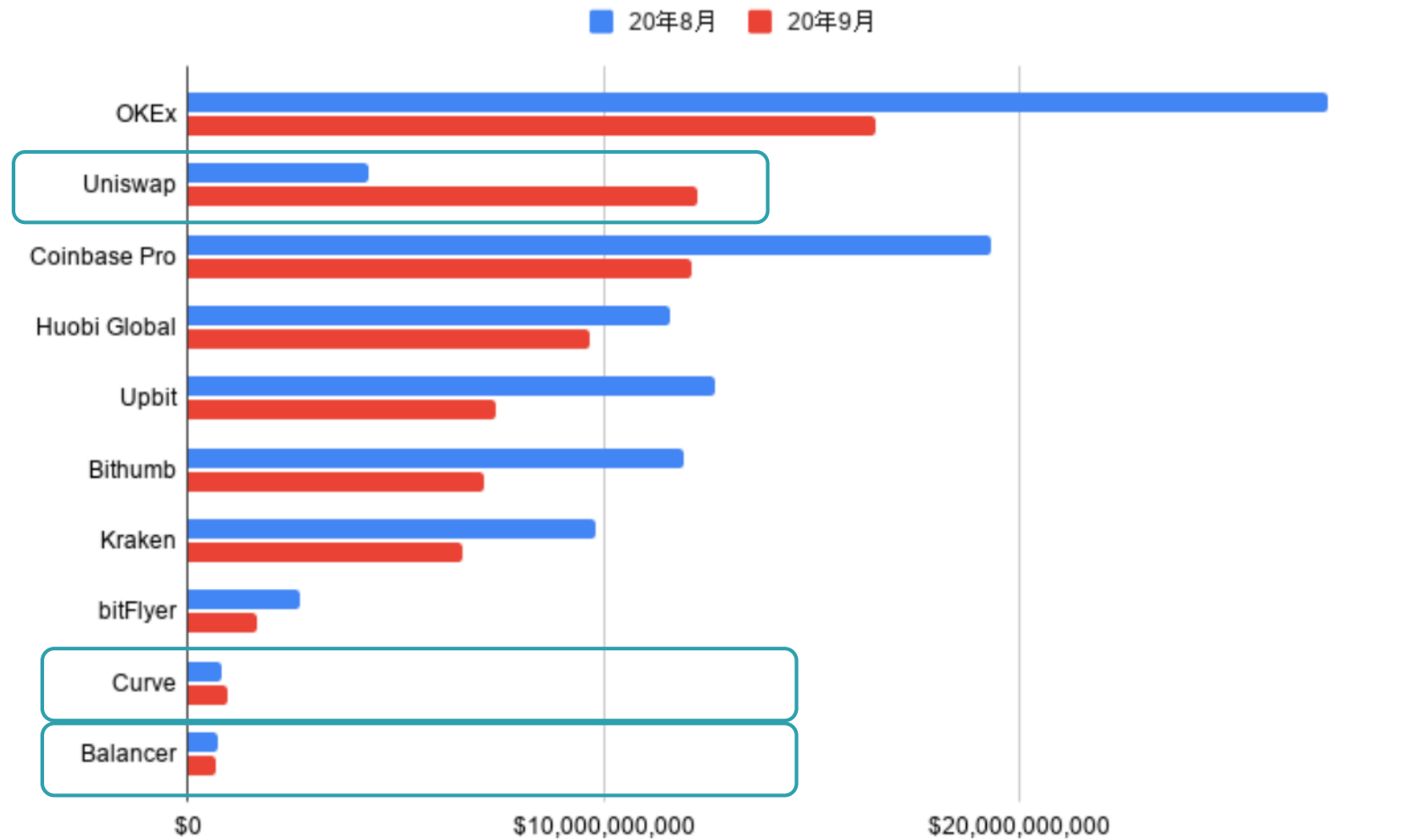
☆ウォッチリスト | 仮想通貨 | Derivatives | DeFi | Storage | Yield Farming

#▲	名前	値段	24時間	1週	時価総額①
☆ 1	Bitcoin BTC	¥1,653,435.98	▲2.47%	▲11.24%	¥30,652,004,594,152
☆ 2	Ethereum ETH	¥48,860.75	▲3.55%	▲14.98%	¥5,540,129,515,440
☆ 3	Tether USDT	¥105.52	▲0.02%	▲0.02%	¥1,841,974,425,892
☆ 4	XRP XRP	¥2710	▲0.39%	▲7.87%	¥1,228,043,345,663
☆ 5	Chainlink LINK	¥1,373.86	▼0.00%	▲23.13%	¥537,878,467,346
☆ 6	Bitcoin Cash BCH	¥27,381.70	▲0.98%	▲8.16%	¥508,464,805,351
☆ 7	Binance Coin BNB	¥2,959.92	▼0.35%	▲4.40%	¥427,432,403,112
☆ 8	Litecoin LTC	¥6,305.38	▲2.50%	▲9.88%	¥415,273,366,957
☆ 9	Polkadot DOT	¥472.77	▲2.02%	▲9.41%	¥414,761,465,931
☆ 10	Cardano ADA	¥11.21	▲0.81%	▲11.18%	¥348,861,821,692



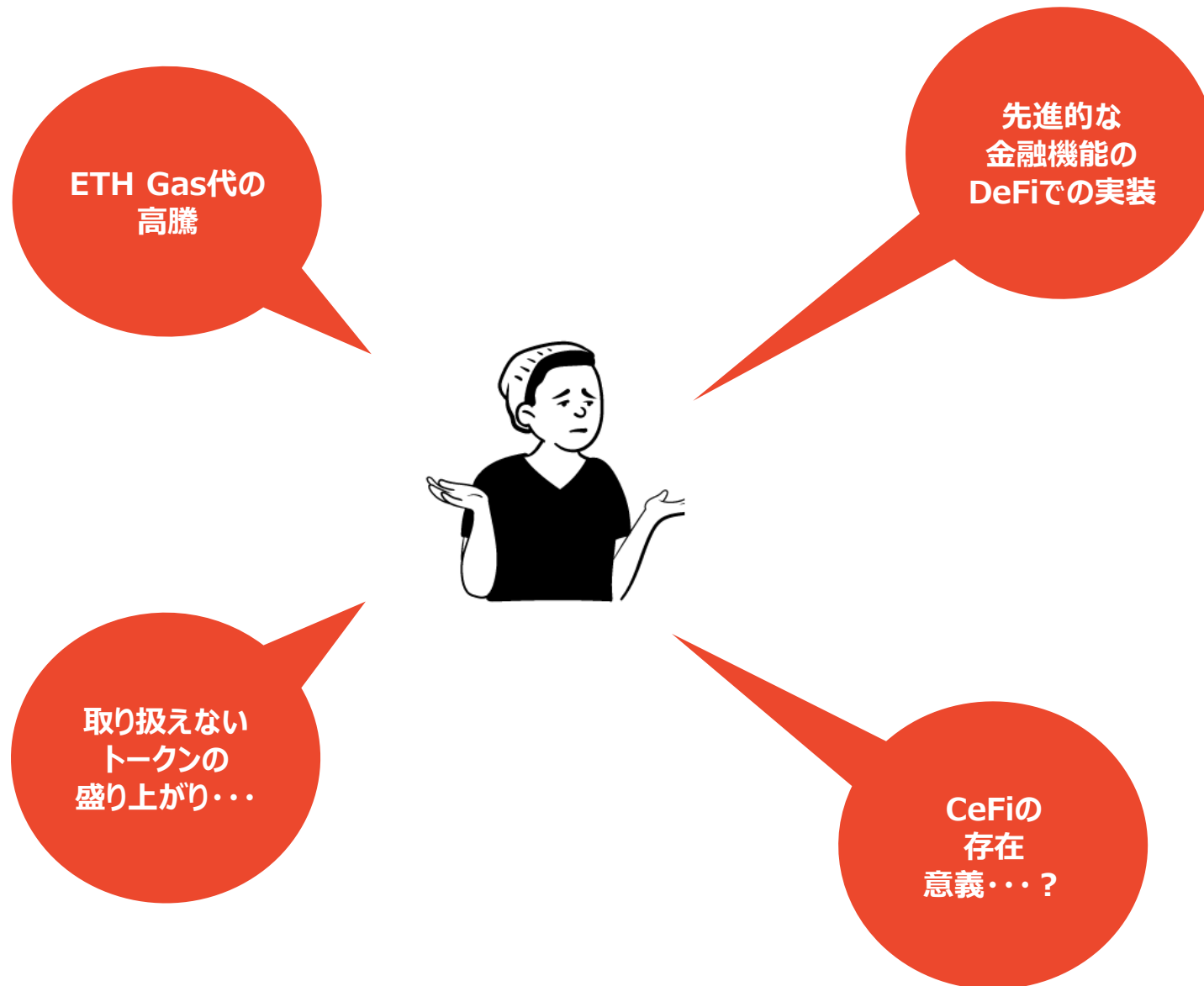
DEXの取引高推移

2020年8月→9月は市場全体でボラティリティが低下する中、9月のCeFiの暗号資産交換業者の取引高は8月のおよそ6割程度となったが、Uniswap、Curve、Balancerにおいては取引高が増加





日本の暗号資産交換業者としてDeFiで何かできるか？





4. DeFiと日本法



DeFiと日本法

ここからは創&佐藤法律事務所の発表資料に基づき資料を作成しています。

DEFIと日本法まとめ

DeFiに対する法律の適用を考える際は、一つ一つのコンポーネントに分けて日本法を分析する必要がある

- ① 日本法は運営主体や販売を規制する法体系。完全に非中央集権なプロジェクトは日本の規制に服さない
- ② 但し、中央集権的な部分が残っていると規制の可能性があり。例えば、DeFiデリバティブで決済はオンチェーンでやるが、デリバティブのマッチングには運営者がいる場合(dYdX)。DeFiのコインを取り扱う通常のExchangeも当然規制
- ③ 投資家側が規制に服することは通常はない

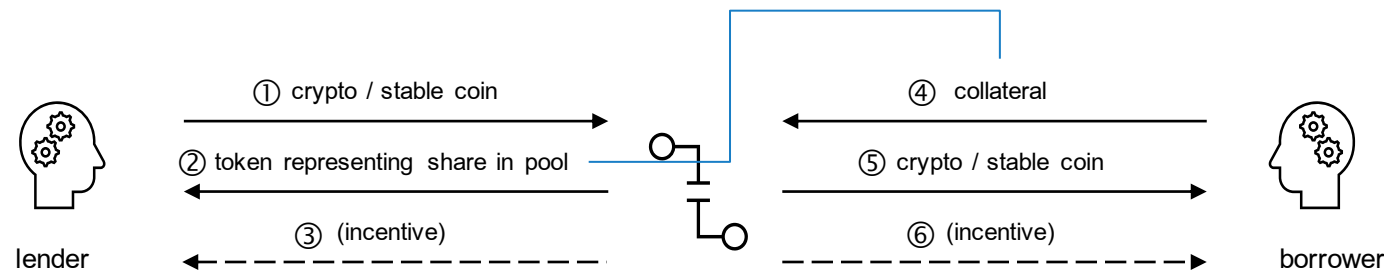




Compoundの仕組みと法律

Compoundの仕組みにがどのように日本法で解釈されるかを検討するため、要素を分解し、それぞれが貸金業、集団投資スキーム、暗号資産交換業（交換、カストディ）に該当するかを検討する

Compoundのレンディングプロトコル

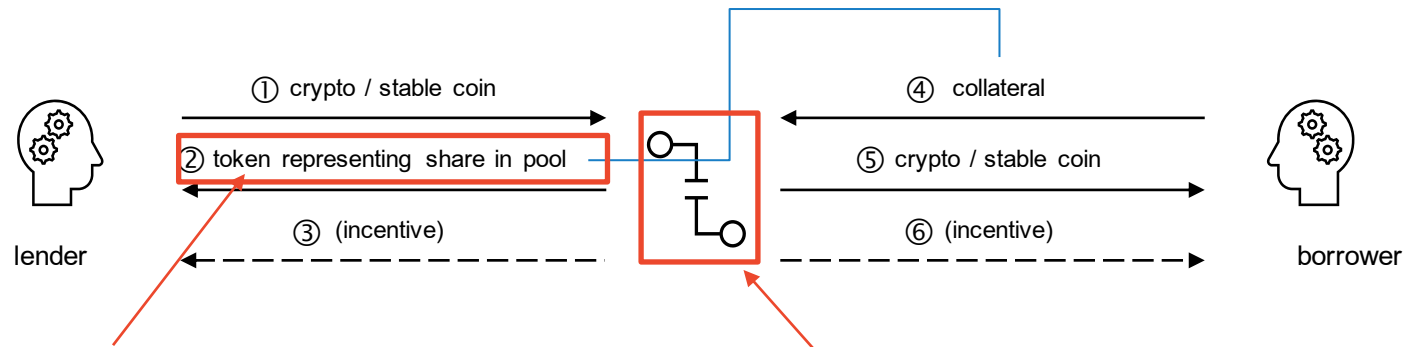


- ① ユーザーは、利息を得るため、スマートコントラクトに暗号資産やステーブルコインをロック
- ② ロックをした場合、事前に設定された為替レートでcTokenがユーザーに交付される。例えばEtherをロックした場合、cEtherが発行。ユーザーはcTokenを保有することにより利息を獲得できる。収益は、借手によって支払われる金利に依存。利率は、貸出と借入の需給に踏まえて決定され、日々常時変動している。
- ③ 上記の金利に加え、貸手はCOMPToken（ガバナンストークン）を受け取ることができる
- ④ cTokenを保有するユーザーはCompoundを担保として暗号資産やステーブルコインを借り入れることができる
- ⑤ 借入に際してユーザーはcTokenを担保として預け入れる。ユーザーが借り入れることができる最大額は、預託された資産に担保係数を乗じて計算される。ユーザーの借入残高が、未払いの利息の増大、担保価値の低下、借入資産の価格の上昇などにより借入能力を超えた場合、提供された担保はその時点市場価値から割引を行った上で清算される
- ⑥ 借手はCompoundプラットフォームを利用することによりCOMPTokenを報酬として受け取ることができる



Compoundの仕組みと法律

Compoundのレンディングプロトコルと法律



- トークンが「配当」を受け取れるものだと電子記録移転権利(有価証券)の可能性

- Compoundの c Tokenは配当ではなく利息？ そうだとすると暗号資産

- ①、②でクリプト又はステーブルコインを貸付、cTokenの発行を受けられる。④、⑤ではC tokenを担保に供することでクリプトやステーブルコインを受け取れる。

→ 貸「金」ではないので貸金業法は適用されない。

→ 所有権(類似の権利)を失う訳ではなく、通常の「売買」や「交換」とは異なり、交換業ではない？

- 貸付や担保で提供するのはカストディではないのでは？

- スマートコントラクト管理でユーザーしか動かせないのならカストディではない

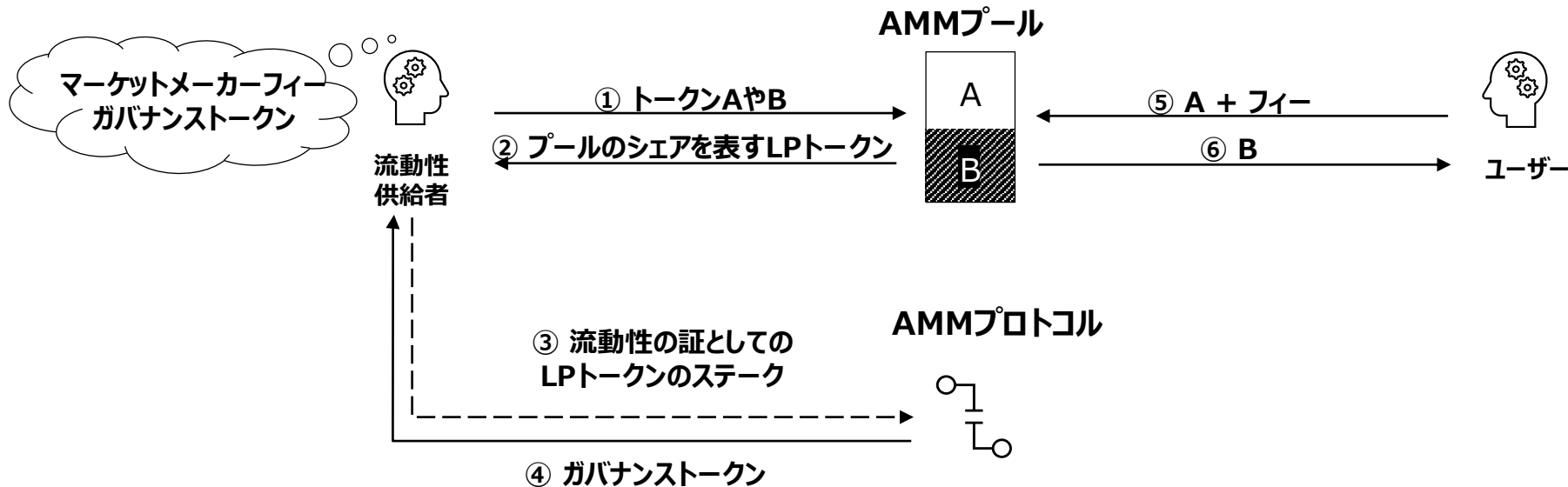
- COMP(ガバナンストークン)の発行がICOと類似するものとして暗号資産交換業になる？

→あくまでおまけとしての配布。ICOと異なり交換業ではないのでは



Uniswap (AMM) の仕組みと法律

Automated Market Makerの仕組み



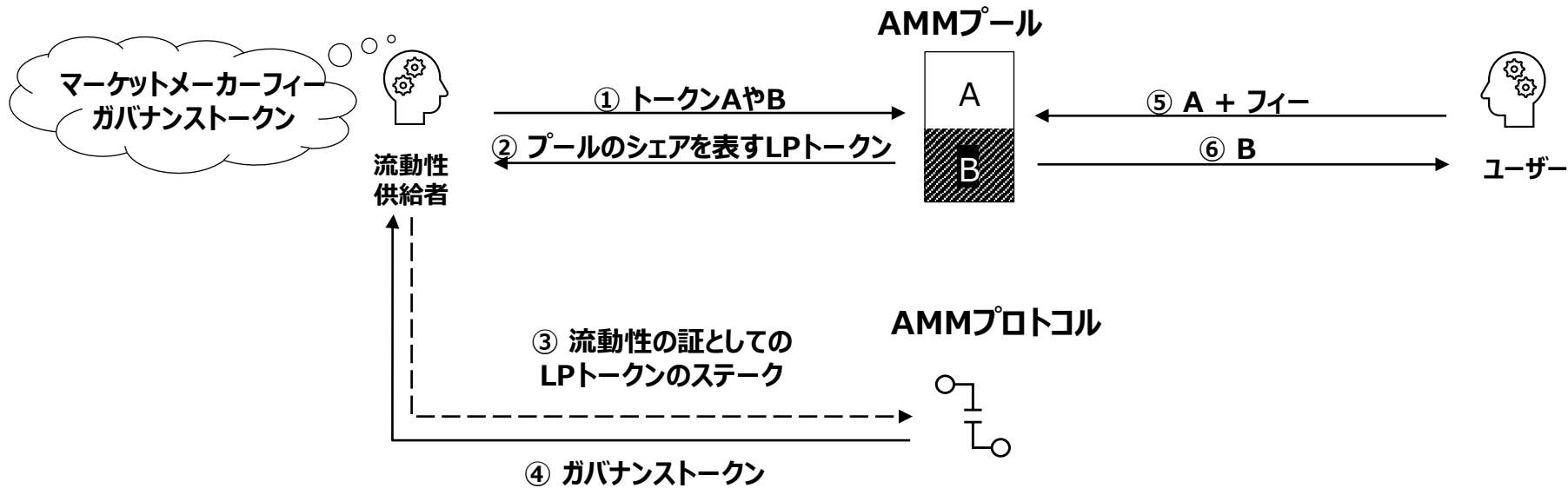
- AMM(Automated Market Maker) =DEX (分散型取引所)の一種。オーダーブックを持たず、代わりに1つ以上の暗号資産のペアで構成される流動性プールを使用
- 各暗号資産の価格は、プール内の他の資産に対して測定
- Uniswapは、プール内の各暗号資産の価格を決定するために以下の式を使用

$$x * y = k$$
 x と y はプール内の各トークンの数。 x と y は時間の経過とともに変化するが、 k は一定であり、AMMは任意の時点で各資産の価格を決定
- たとえば、ETH/DAIプールでETHをDAIに交換すると、DAIの価格はETHよりも割高に→プール内のETH価格が実際の市場価格から乖離している場合、裁定取引の機会が生じる。→トレーダーはプールにDAIを供給し、ETHを引き出す。→その結果、ETHの価格はリバランスされ、全体的な市場価格に合わせて調整
- 十分に X と Y の数が多い場合にはスリッページは僅少になる
- プールの流動性は流動性プロバイダー(LP)によって提供
- 流動性を提供することと引き換えに、LPはプールとのやりとりで請求される手数料に参加し、場合によっては追加のインセンティブとしてガバナンストークンを受け取る



Uniswap (AMM) の仕組みと法律

Automated Market Makerの仕組みと法律



- AMMであっても暗号資産交換業が問題となる。ただ、仕組み自体はコントラクトで動いており、運営者がいない
↓
暗号資産交換業ではない
- 「ガワ」を提供している人は交換業？ただガワがなくても動く仕組み
- LPトークンはセキュリティに該当するか？



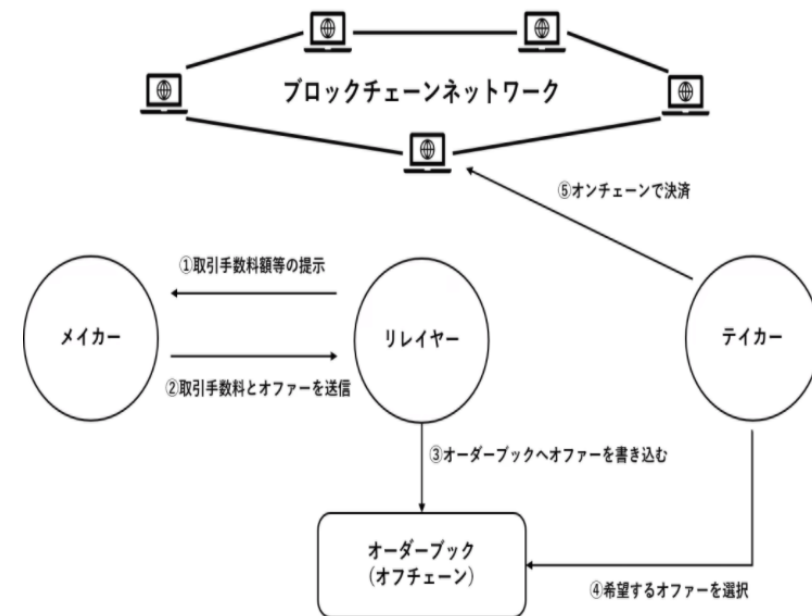
dYdX (DeFiデリバティブ) の仕組みと法律

dYdXはイーサリアムのスマートコントラクト上で実行される。決済をオンチェーンで行うことで信用リスクを無くし、注文をオフチェーンで行うことによりユーザーの手数料の削減、処理スピードの向上を図っている

dYdX (DeFiデリバティブ) の仕組み

dYdXにおける取引の具体的な仕組み

- ① リレイヤーがオファーを希望するユーザー(メイカー)に対して取引手数料と取引手数料を受け取るためのアドレスを提示。なお、リレイヤーの提示する取引手数料はリレイヤーが自由に設定でき、リレイヤー間での競争を促進し、取引手数料額の低価格化が図られている
- ② ユーザー(メイカー)は提示されたアドレスに取引手数料をセットし、秘密鍵で署名した購入オファーやローンオファーをリレイヤーに送信
- ③ リレイヤーはオファーを受け取り、それが有効であること、必要な取引手数料が提供されていることを確認し、有効なオファーをオフチェーンで管理されるオーダーブックに書き込み
- ④ 他のユーザー(テイカー)は、オーダーブック上でテイクを希望するオファーがある場合、秘密鍵で署名をしてテイク、ブロックチェーン上での決済を行う



dYdX (DeFiデリバティブ) の法律、規制面での整理

- ① 業としてデリバティブのカウンターパーティーとなり(例：ショートとロングのプライスを出し、プライスに同意するユーザーとデリバティブ取引をなす)、又は業としてデリバティブ取引の媒介をなす場合(例：デリバティブ取引の板を作成・運営する)には、原則として第一種金融商品取引業の登録が必要
- ② 完全に非中央集権であり、スマートコントラクトのみで動いているDeFiデリバティブの場合、業を行う「者」ではなく、登録は必要ないと思われる。但し、実際に「運営者」等がないかは慎重な判断を要する
- ③ dYdXでは、デリバティブのマッチング自体はオフチェーンで行われる。オフチェーンのマッチングシステムを提供する者は、日本居住者を顧客とする場合、第一種金融商品業の登録義務を負う



5. 暗号資産取引所とDeFi



海外取引所におけるDeFiトークンの取扱い

海外取引所はDeFiトークンの取扱いに非常に積極的。現在グローバルで取引高首位のOKEx、米国での規制下で運営する取引所の代表格Coinbaseでも取扱高ランキングの上位にDeFiトークンが登場する

海外取引所での取り扱い

US Dollar base markets at OKEx

BTC ADA ALGO ATOM BCH BSV DASH DOT EOS ETC ETH IOST IOTA KNC LINK LTC NEO ONT QTUM SUSHI
THETA TRX UNI XLM XMR XRP XTZ YFI YFII ZEC

is/are being traded as 30 market pairs with 1 base currencies of USD by the 24 hours volume 53,538 BTC at 1 exchanges of OKEx

This summarized statistics are based on the information of markets and exchanges registered at Coinhills. last updated: Wed, 11 Nov 2020 21:15:27 UTC

US Dollar base markets

BTC / USD Bitcoin / US Dollar	OKEx		15,712 USD +410.70 +2.68% ^	32,196 BTC 505,859,000 USD	+ Add to Dashboard Go to the Market
ETH / USD Ethereum Ether / US Dollar	OKEx		465.59 USD +15.3800 +3.42% ^	351,834 ETH 163,810,460 USD	+ Add to Dashboard Go to the Market
LINK / USD ChainLink / US Dollar	OKEx		13.0430 USD +0.05100000 +0.39% ^	2,230,940 LINK 29,098,150 USD	+ Add to Dashboard Go to the Market
YFI / USD yearn.finance / US Dollar	OKEx		16,362 USD -1,301.00 -7.37% v	1,322.84 YFI 21,644,290 USD	+ Add to Dashboard Go to the Market
LTC / USD LiteCoin / US Dollar	OKEx		59.7700 USD +1.7300 +2.98% ^	361,569 LTC 21,610,950 USD	+ Add to Dashboard Go to the Market
BCH / USD Bitcoin Cash / US Dollar	OKEx		259.03 USD +2.7200 +1.06% ^	54,135 BCH 14,022,470 USD	+ Add to Dashboard Go to the Market
EOS / USD EOS / US Dollar	OKEx		2.5110 USD +0.01100000 +0.44% ^	4,468,554 EOS 11,220,540 USD	+ Add to Dashboard Go to the Market
YFII / USD DeFi Money / US Dollar	OKEx		1,539.50 USD -130.00 -7.79% v	5,281.74 YFII 8,131,240 USD	+ Add to Dashboard Go to the Market

US Dollar base markets at Coinbase Pro

BTC ALGO ATOM BAND BCH DAI DASH EOS ETC ETH KNC LINK LRC LTC MKR NMR OMG OXT REN REP
UMA UNI XLM XRP XTZ YFI ZRX

is/are being traded as 27 market pairs with 1 base currencies of USD by the 24 hours volume 32,557 BTC at 1 exchanges of Coinbase Pro

This summarized statistics are based on the information of markets and exchanges registered at Coinhills. last updated: Wed, 11 Nov 2020 21:14:06 UTC

US Dollar base markets

BTC / USD Bitcoin / US Dollar	Coinbase Pro		15,707 USD +410.14 +2.68% ^	14,801 BTC 232,471,158 USD	+ Add to Dashboard Go to the Market
ETH / USD Ethereum Ether / US Dollar	Coinbase Pro		464.87 USD +14.9900 +3.33% ^	195,297 ETH 90,787,507 USD	+ Add to Dashboard Go to the Market
YFI / USD yearn.finance / US Dollar	Coinbase Pro		16,273 USD -1,394.04 -7.89% v	2,543.82 YFI 41,396,359 USD	+ Add to Dashboard Go to the Market
LINK / USD ChainLink / US Dollar	Coinbase Pro		13.0087 USD +0.00480000 +0.04% ^	2,645,861 LINK 34,419,267 USD	+ Add to Dashboard Go to the Market
LRC / USD Loopring / US Dollar	Coinbase Pro		0.19260000 USD +0.01430000 +8.02% ^	112,082,275 LRC 21,587,046 USD	+ Add to Dashboard Go to the Market
LTC / USD LiteCoin / US Dollar	Coinbase Pro		59.6000 USD +1.6600 +2.87% ^	195,486 LTC 11,650,974 USD	+ Add to Dashboard Go to the Market
XRP / USD Ripple / US Dollar	Coinbase Pro		0.25670000 USD +0.00140000 +0.55% ^	41,310,689 XRP 10,604,454 USD	+ Add to Dashboard Go to the Market



日本における新規暗号資産取扱審査

暗号資産交換業協会（JVCEA）の自主規制規則の一つ「暗号資産の取り扱いに関する規則」において、新規暗号資産の取り扱いにあたって審査を行う事項について定められている

日本における新規銘柄取扱いに関する規則上のさだめ

第2条 会員は、取扱暗号資産の審査に関する社内規則を定めなければならない。

2 会員は、前項の社内規則の策定にあたっては、次の各号に掲げる事項（以下「必要審査項目」という。）を審査項目に含めなければならない。

(1) 取扱暗号資産に関する事項

イ 発行状況に関する事項

ロ 取引状況に関する事項

ハ 利用状況に関する事項

ニ 暗号資産の関係者に関する事項

ホ 暗号資産及び記録台帳の技術に関する事項

ヘ 対象プロジェクトに関する事項

(2) 会員の社内体制に関する事項

イ 暗号資産の安全管理体制に関する事項

ロ 暗号資産の技術対応能力に関する事項

ハ 自社の取引処理能力に関する事項

ニ 財務耐久性に関する事項

ホ 需要見込みに関する事項

ヘ 利用者との利益相反に関する事項

ト 取扱い開始時の価格決定方法及び取引条件に関する事項

チ 利用者への情報提供及び説明に関する事項

第3章 新規取扱（取扱いに慎重な判断を要する暗号資産）

第4条 会員は、取り扱おうとする暗号資産の特性に鑑み、次の各号のいずれかに該当すると認められる場合には、その適否を慎重に判断しなければならない。

(1) 法令又は公序良俗に違反する方法で利用されている又は利用されるおそれが高い暗号資産

(2) 犯罪に利用されている又は利用されるおそれが高い暗号資産

(3) マネー・ローンダリング及びテロ資金供与に利用されている又は利用されるおそれが高い暗号資産

2 会員は、取り扱おうとする暗号資産の特性及び会員自身の体制に鑑み、次の各号のいずれかに該当すると認められる場合には、当該暗号資産を取扱ってはならない。

(1) 移転・保有記録の更新・保持に重大な支障・懸念が認められる暗号資産

(2) 当該会員において、公認会計士又は監査法人による適切な監査が実施できない又は困難な暗号資産

(3) 当該会員において、システム上その他安全な管理及び出納ができない又は困難な暗号資産

(4) 前各号のほか、当該会員において資金決済法（以下、「法」という。）上の義務を適正かつ確実に履行できない又は困難な暗号資産

（協会への届出）

第5条 会員は、新たな暗号資産の取扱いを開始する場合には、協会に対して、次の各号に掲げる書類を事前に届出なければならない。

(1) 協会が別に作成する審査報告書

(2) 協会が別に作成する当該暗号資産の概要説明書（以下「概要説明書」という。）

(3) 当該暗号資産に関して利用者に開示・提供する資料等

(4) 当該暗号資産に係るホワイトペーパーその他当該暗号資産の内容を説明した資料

(5) 当該暗号資産の流通状況に関する資料（流通実績がある場合に限る。）

(6) 当該暗号資産に関連する事件・事故に関する資料

(7) 当該暗号資産の管理に関する社内規則や事務マニュアル等を記した書面

(8) 当該暗号資産の管理に関する社内検証を行った資料

(9) 当該暗号資産を取り扱う暗号資産の売買等の概要書

(10) 概要説明書を作成・管理する者の氏名、役職、所属部署、経歴、連絡方法を記した書面

(11) 当該暗号資産の管理者等の関係者の反社会的勢力との関係性その他マネー・ローンダリング及びテロ資金供与の関連性について社内検証を行った資料

(12) その他協会が提出を求める書面又は資料

日本における新規銘柄取扱いプロセス

社内の委員会
等による審査

取締役会での
決議

JVCEAでの
審査



DeFiアグリゲーター（プラットフォーム）

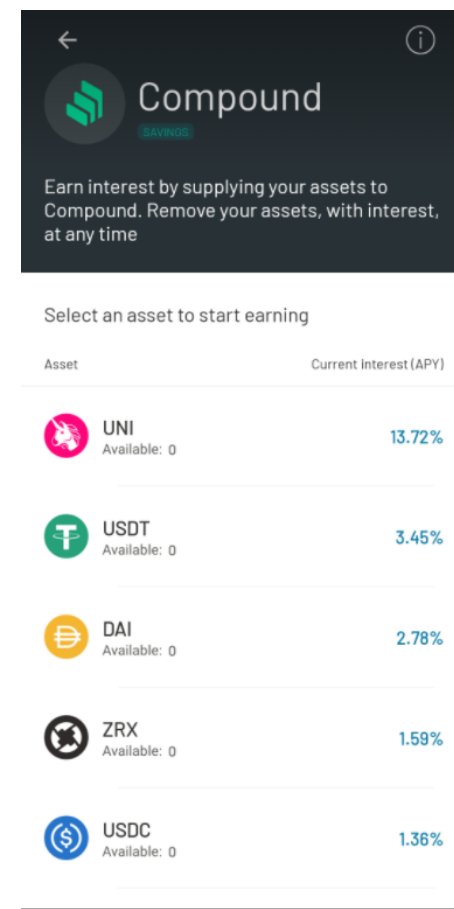
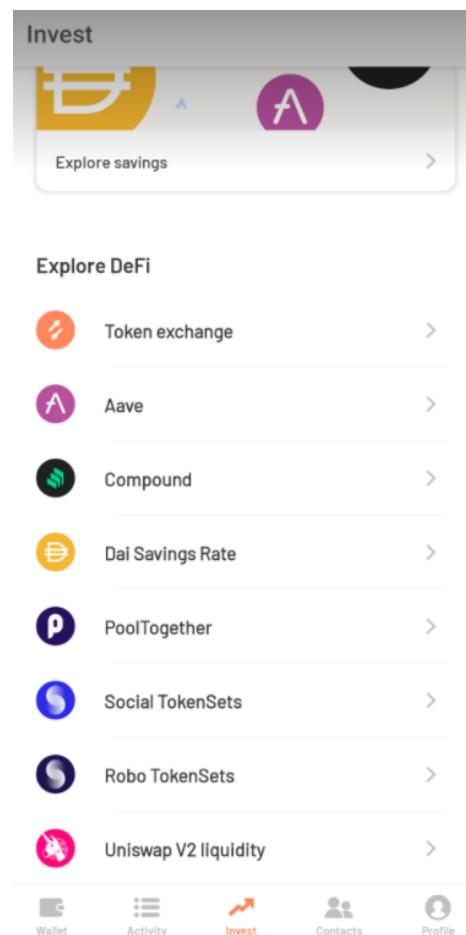
Compound等のDeFiプラットフォームに接続するためにはChrome等のブラウザを拡張してMetamaskなどのイーサリアムのウォレットをダウンロードし接続する必要がある。個別のDeFiプラットフォームにはそれぞれ接続が必要。アグリゲーターはスマートフォンで使え、様々なDeFiプラットフォームにアクセスが可能

Compoundを使う手順



- 基本的にPCでの操作となります
- ChromeにMetamaskをダウンロードし、ウォレットを作成
- ETHをMetamaskのアドレスに送付
- （取引所で買えないコインを預託したい場合はUniswapなどのDEXに接続して購入）
- Compoundに接続し保有するコインをSupply

「Argent Wallet」を使う場合





DeFiアグリゲーター（プラットフォーム）としての法的な建付け

そもそも各種金融機能をDeFiで行う場合に日本法ではどのように考えられるのか、各種DeFiに「つなぐ」アグリゲーターはどのような法律を気にすべきかについては斎藤先生が検討されている内容をベースに関係各所と協議する必要

DeFi及びDeFiアグリゲーターと日本法

レンディング： Compound

- 貸金業、集団投資スキーム、暗号資産交換業（交換、カストディ）には当たらないという整理が可能そう
- アグリゲーターとしてDeFiのレンディングプラットフォームにつなぐのは法的に問題ないと言えるのか

DEX： Uniswap

- 仕組み自体はスマートコントラクトであり、運営主体はいないため、「暗号資産交換業」にはあたらない？
- アグリゲーターとしてDEXにつなぐのは売買の媒介にあたらないか？

デリバティブ： dYdX

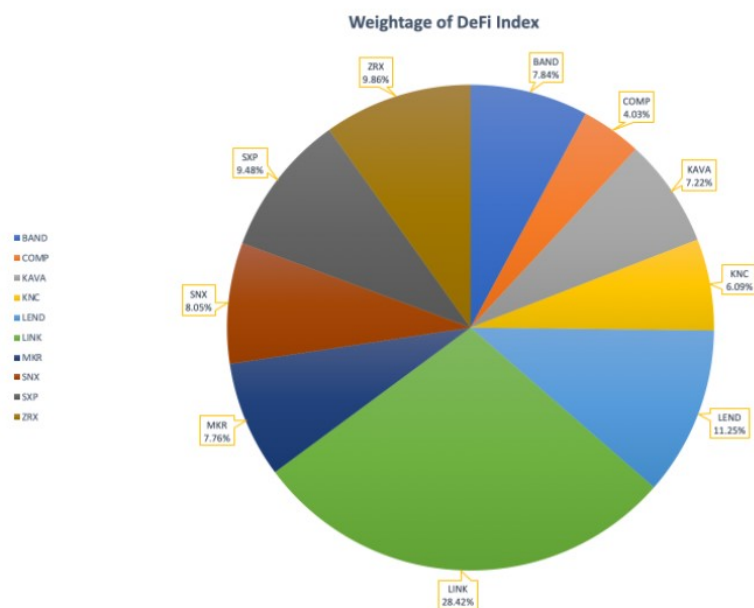
- スマートコントラクト上で動く部分については規制の対象外と言えるか。「運営主体」の有無については厳しく見られる可能性も。運営者がいる場合は第一種金融商品取引業登録が必要
- アグリゲーターとしてDeFiのデリバティブにつなぐ場合も要整理



DeFiファンド、DeFiデリバティブ

第一種金融商品取引業者としてDeFiデリバティブの提供、第二種金融商品取引業者としてDeFiファンドの組成などは現状の規制下でも可能と考えられる

海外取引所における DeFiインデックスの概要



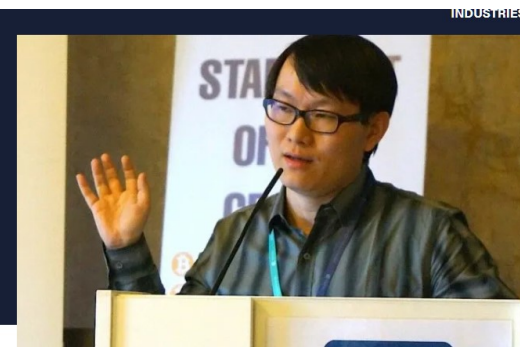
$$weighting\ factor_i = \frac{\sqrt{volume_i} + \sqrt{market\ cap_i}}{\sum_{i=1}^n (\sqrt{volume_i} + \sqrt{market\ cap_i})} \times 100\%$$

DeFi投資ファンド設立事例

フォビが投資ファンド 「DeFi Labs」を設立—— 投資ターゲットは分散型金 融

2020年 8月 5日 06:00 ・ 2020年 8月 5日 08:35 更新

🐦 f B!



暗号資産（仮想通貨）取引所を運営するフォビグループ（Huobi Group）は8月3日、新組織「Huobi DeFi Labs」の設立を発表した。新組織の目的は、DeFi（分散型金融）分野に数十億円規模の投資を行うためのファンドを運営することだ。

DeFi Labsは4人のスタッフで構成され、DeFi関連プロジェクトの調査・投資・インキュベーションに注力する。

同部門を率いるのは、最近同社に加わったチーフ・インベストメント・オフィサーのシャーリン・ウー（Sharlyn Wu）氏。

同氏は以前、中国大手銀行の一つ、招商銀行（CMB：China Merchants Bank）の海外戦略を担うチャイナ・マーチャント・バンク・インターナショナル（CMBI：China Merchants Bank International）でブロックチェーン投資部門の責任者を3年間務めた。

ウー氏の在任中、CMBIはウォレットスタートアップのBitpieやパブリックブロックチェーンプロジェクトのネルボス（Nervos）など、複数の暗号資産・ブロックチェーン関連企業に投資を行った。

「パーミッションレスエコノミーのパワーが世界規模で解き放たれる様子を見ることはエキサイティング。しかし、理論的・技術的なレベルで解決すべき問題はまだまだたくさんある」とウー氏は述べた。

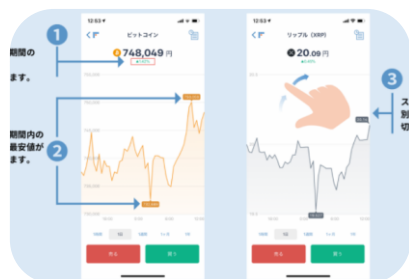
フォビグループ以外にも、暗号資産VCがDeFi関連プロジェクトに投資する動きは増えている。

先週、分散型取引所（DEX）のInjective Protocolはパンテラ・キャピタル（Pantera Capital）が主導する資金調達ラウンドで260万ドルを調達したと発表。他にも、ポリチェーン・キャピタル（Polychain Capital）とスリー・アローズ・キャピタル（Three Arrows Capital）は、DeFiサービスKeeperDAOの数百万ドル規模のシードラウンドに投資した。

CeFiが行ってきた仮想通貨をマス層に広げるための施策

現状アグリゲーターアプリであってもDeFiを使うことのハードルは極めて高い。多くの人に使ってもらうサービスになるためには言語含めたUI/UXの改善、マスマーケティング、カスタマーサポート、コンプライアンスが必要と考えられるが、スマートコントラクト上でこれらを実装することは現実的には難しい可能性

マス向け取引所に必要な要素



アプリなどのUI/UX



マスマーケティング

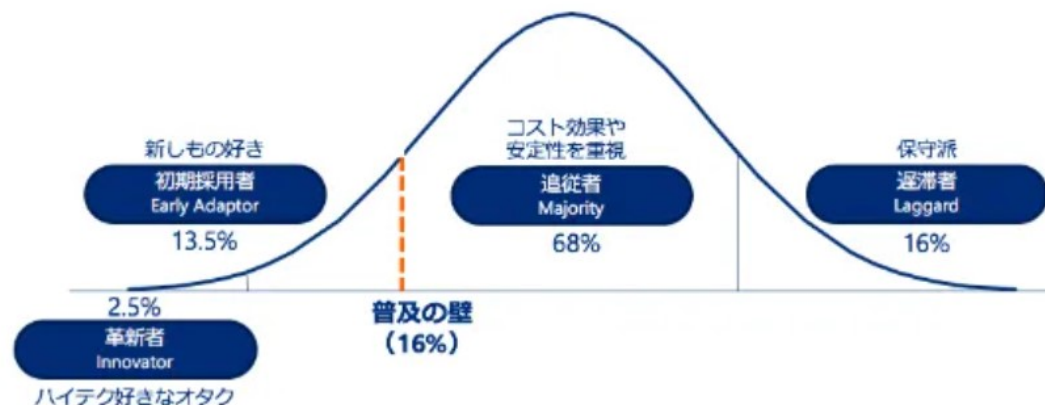


カスタマーサポート



コンプライアンス

「イノベーター理論」における位置づけ



- DeFiを実際に使っているのは「ハイテク好きのオタク」の中でもごく一部
- 仮想通貨を「聞いたことがある」のは90%、「使ってみたい」のは20%弱
- 一部の超コアユーザーがDeFiを使うようになる動きはあるが、このままではこれ以上広がるのは難しいか



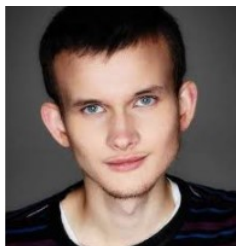
6. DeFiの技術的課題



イーサリアムのスケーリング問題 イーサリアム2.0とセカンドレイヤーソリューション

「並列処理」であるシャーディングを導入するイーサリアム2.0がスケーラビリティの問題を解決する可能性。セカンドレイヤーソリューションはDeFiの性質上ソリューションにならないと考えられている

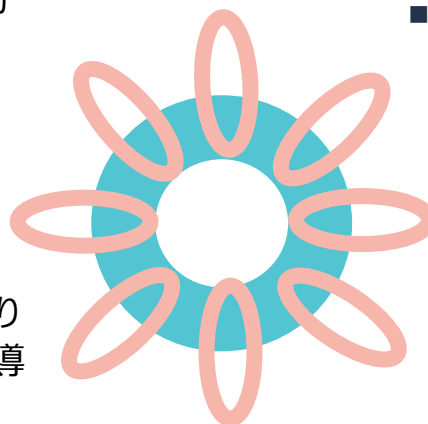
イーサリアムネットワークの混雑回避 技術的な方法



- イーサリアムのネットワークは過去はCryptoKittiesの影響、また足元はDeFiの流行を受けて混雑してきている
- ガス代は一時期よりは落ち着いたもののまだ割高な状態

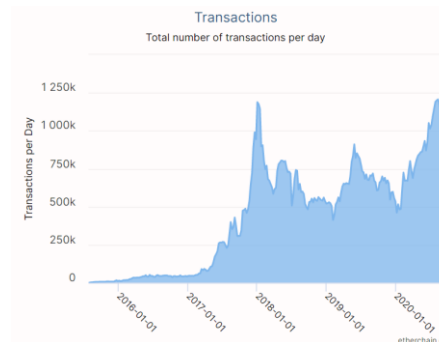
イーサリアム2.0（2020年11月・・・？）
PoWからPoSへ
シャーディングの導入

- シャーディングは元々データベースの分割手法の一つ。データベースへのリクエストを分散し全体の処理能力を上げる目的で利用されている
- イーサリアムにおいては、複数かつ別々のブロックチェーン（シャードチェーン）とそれらを取りまとめる一つのチェーン（フェーズ0で導入されるビーコンチェーン）という構成。PoWを採用している場合、シャーディングによってブロックチェーンが分割してしまうと競争率が下がり、51%攻撃がより簡単になってしまうため、PoSへの移行後にシャーディングを導入することが望ましい



セカンドレイヤー

- オフチェーンでの取引を行う
- イーサリアムの場合はDeFiにおいて必須な「誰のものでもない」状態をセカンドレイヤーでは表現できないという問題がある





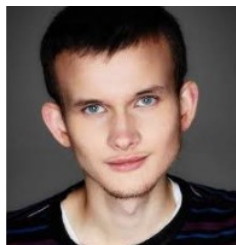
イーサリアムのスケーリング問題 イーサリアム2.0のロードマップ

スケーラビリティの問題は2014年ごろから認識されておりイーサリアム2.0の構想自体は2016年ごろから存在。現在、Phase3は2021年を予定しているがハードフォークになるためマイナーの同意が必要となる

イーサリアムネットワークの混雑回避 技術的な方法

What's in Ethereum 2.0?

- Proof of stake (Casper)
- Scalability (sharding)
- VM improvements (EVM)
- Improvements to cross-contract logic (eg. abstraction)
- Improvements to protocol economics



Expected phases

Phase 0: beacon
chain PoS

Phase 2: enable state
transitions (EVM)

Phase 1: shards as
data chains

Phase 3 and beyond:
iterate, improve, add tech



Polkadotへの注目ーイーサリアムキラー？

イーサリアムの共同創業者だったGavin WoodがWeb3 Foundationを創設し、Polkadotの開発を開始

Polkadotの概要とスケーラビリティ、AcalaNetwork



Gavin Wood

Founder,
Web3 Foundation

Co-Founder,
Parity Technologies

Profile

イーサリアムの共同創業者、元CTOとしてイエローペーパーの執筆から、初期の18-24ヶ月ほどの開発に携わる。

その間に、Solidity言語、Proof-of-AuthorityコンセンサスやWhisperなど、今日のブロックチェーン業界では当たり前になっている技術や概念を創出し、イーサリアムをメインネットローンチさせる。

“EthCore”として当初創業したイーサリアムに特化した開発チームは、100人規模のトップブロックチェーン開発陣が集うParity Technologiesとなり、現在も自身がリード開発者としてSubstrate, PolkadotおよびKusamaの開発を主導している。

2014年に「Web3.0」という概念を提唱し、Web3 Foundationを創設、プレジデントを務める。



Polkadotの概要

Polkadotはリレイチェーンとパラチェーンからなり、個々のブロックチェーンは「パラチェーン」としてリレイチェーンに接続する

Polkadotの概要とスケーラビリティ

Polkadot.

仕組み



ポルカドットのメインチェーンと呼ばれる「リレイチェーン」

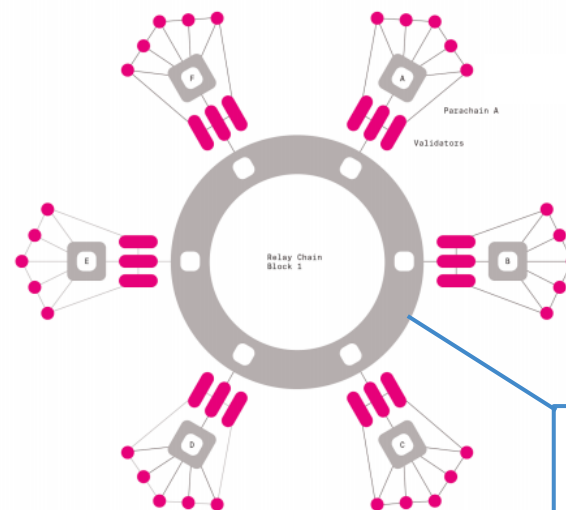
機能を削ぎ落としてチェーン間的高速通信と、バリデーターを集め共有セキュリティを維持するブロックチェーン



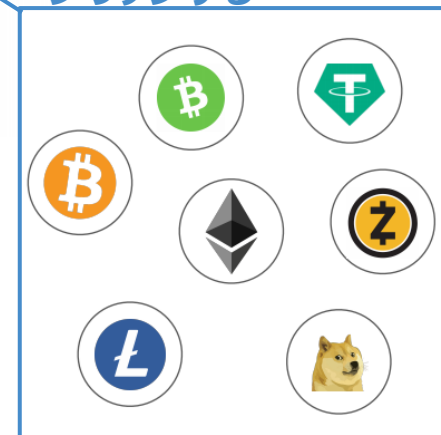
そこに接続される「パラチェーン」

一定のDOTトークンを期間指定で預けることで、ポルカドットのチェーンをまたいだ相互運用性、スケーラビリティ、セキュリティを享受しながら個々の用途やロジックで自由に運用されるチェーン

自前でチェーンのセキュリティを整備する必要がなく、非常に安価で短期間で構築できる



既存のブロックチェーンもブリッジする



理論上の基盤チェーンのスケーラビリティ

- $1,000\text{TPS} \times 100\text{パラチェーン} = 10\text{万TPS}$ が達成可能
- パラチェーンは当初は100上限、200程度まで拡張可能
- その他、データベースの最適化などで $5,000\text{TPS}/\text{parachain}$ 程度のベンチマークは達成可能

→この場合は $5,000\text{TPS} \times 200\text{パラチェーン} = 100\text{万TPS}$ も達成可能



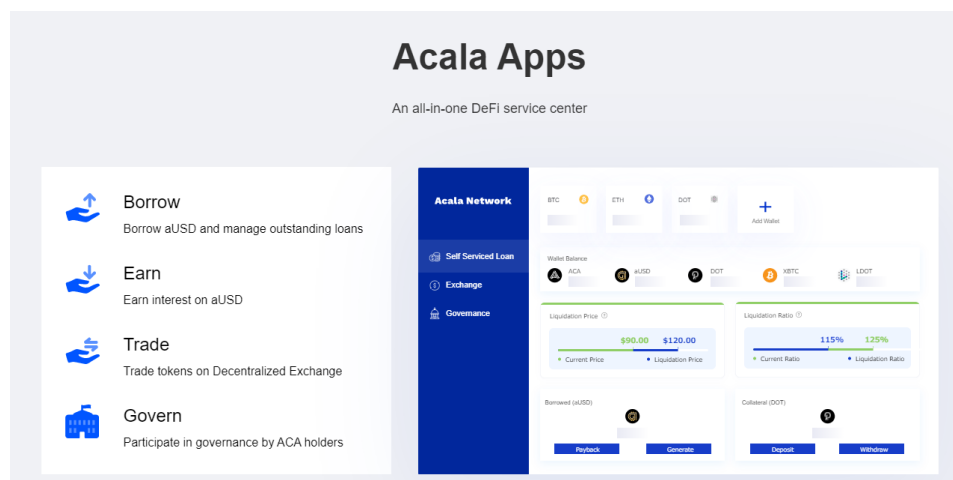
Polkadotのアップグレードの性質、ガバナンス、パラチェーン候補

イーサリアムの仕様変更マイナーのコンセンサスが必要であったが、Polkadotではフォーク無しで仕様を改善・進化していくことが可能

オンチェーンでの仕様変更

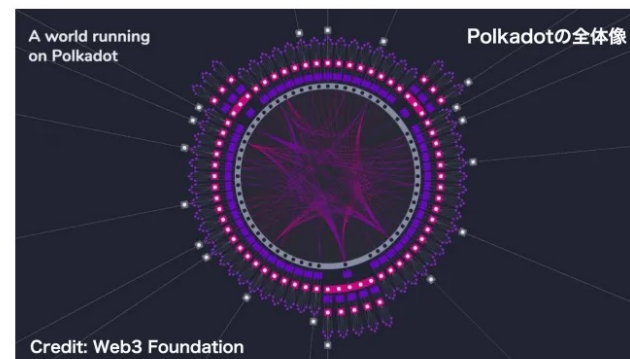
- Web-Assemblyベースの「メタプロトコル」
→チェーンロジックをオンチェーンにWasmを通して「データ」として記述できる
- ポルカドット内のチェーン全てに適用
- チェーン自体が、アップグレード性とオンチェーンガバナンスの仕組みを持つことで、未来の技術進化や環境変化に合わせフォークなしで自律的に、改善・進化していくことができる

パラチェーン候補の例



• Plasm Networkとは？

Plasm Networkは、ステイクの開発する日本発レイヤー1パブリックブロックチェーンです。Plasm Networkには、ブロックチェーンのスケーラビリティ問題を解決するために、レイヤー1のPlasm Network上にレイヤー2ソリューションが実装されています。そして、Web3財団、Parity Technologies社の開発するPolkadotというパブリックブロックチェーンに接続されることが見込まれています。Polkadotは、異なるブロックチェーンを接続するブロックチェーンであり、ブロックチェーンの課題の一つでもあるインターオペラビリティ（相互運用性）を解決します。、Plasm Networkは、スケーラビリティの問題をレイヤー2ソリューションを提供することによって解決し、Polkadotに接続することによってEthereumやBitcoinなど異なるブロックチェーンとのインターオペラビリティの担保をします。





7. DeFiと金融規制（特にAMLCFT）



KuCoinのハッキングに見るDeFiの課題

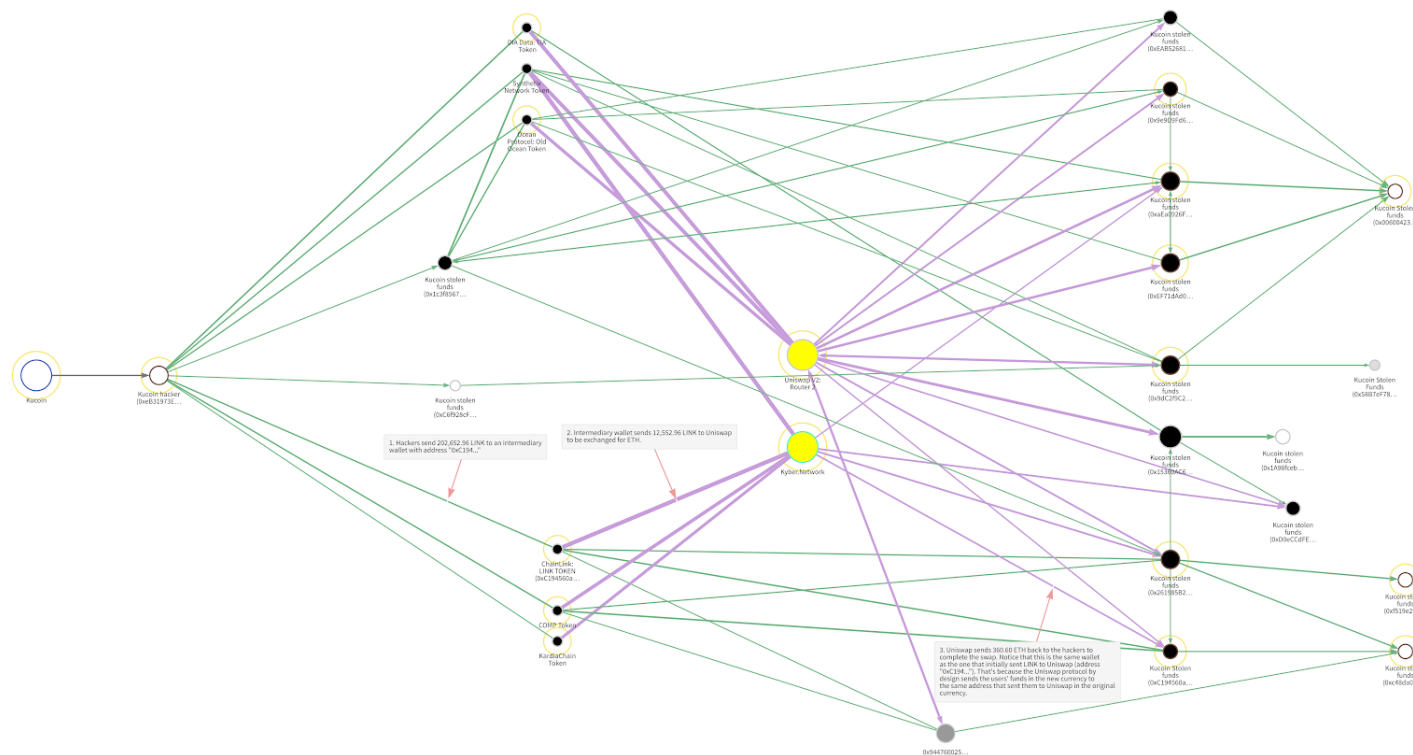
9月にKuCoinがハッキングを受け、\$275mil超の暗号資産が流出しました。流出した暗号資産にはETHやERC20トークンも含まれ、ミキシングの目的でKYCを行っていないDeFiが利用された

KuCoinのハッキング概要、DeFiがどのように使われたか



- KuCoinは香港の仮想通貨取引所
- 2020年9月25日、2億7,500万ドルを超える暗号資産が流出。対象暗号資産は以下
 - BTC、ETH、USDT-ETH、XRP、LTC、USDT、XLM
 - ERC-20トークン（LINK、TIA、Old Ocean、COMP、KardiaChain）
- 犯人はETHやERC-20トークンをロンドリングするためにDeFi（Uniswap、Kyber）を利用

出所：Chainanalysisブログ



緑の線はETHやトークンの資金移動、紫の線はDEXのインタラクション

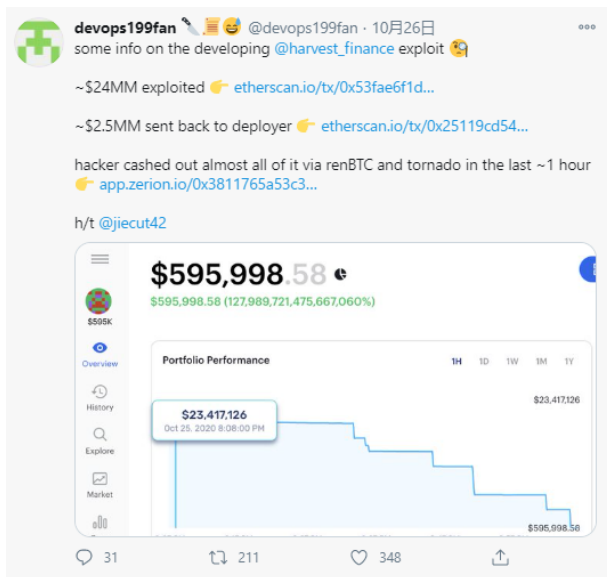
“DeFiによる複雑化にも関わらず捜査官はReactorを利用してほとんどの資金を追跡できています” Chainanalysis



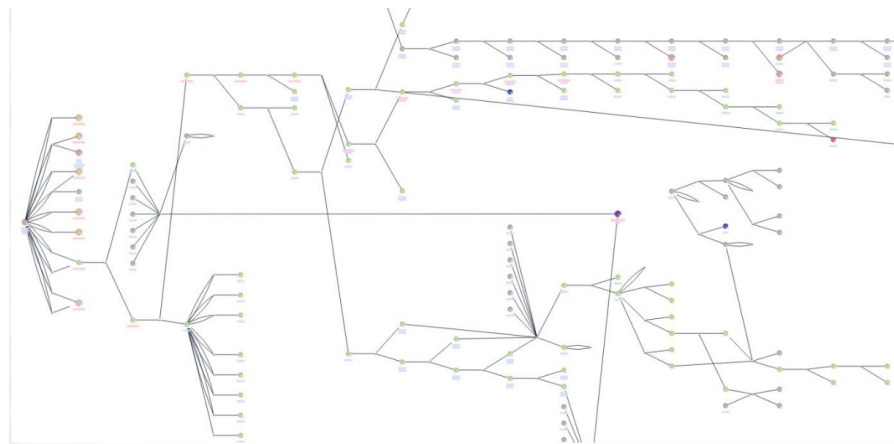
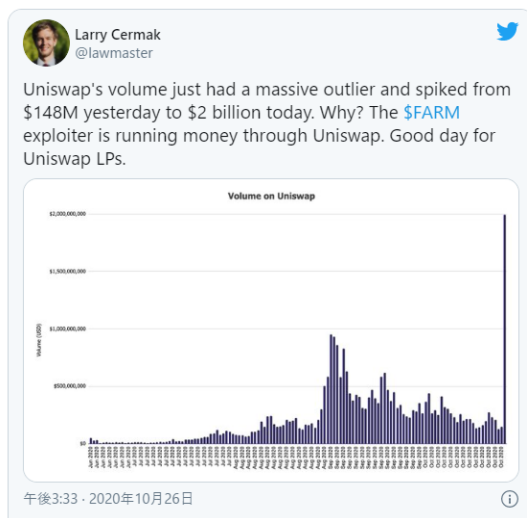
Harvest Financeからの不正流出に見るDeFiの課題

10月26日には、DeFiの利回り最適化プロトコル、Harvest Financeから2,400万ドル相当が不正流出した。流出後Uniswapでのトークン交換も行われていると見られている

Harvest Financeのハッキング概要、DeFiがどのように使われたか

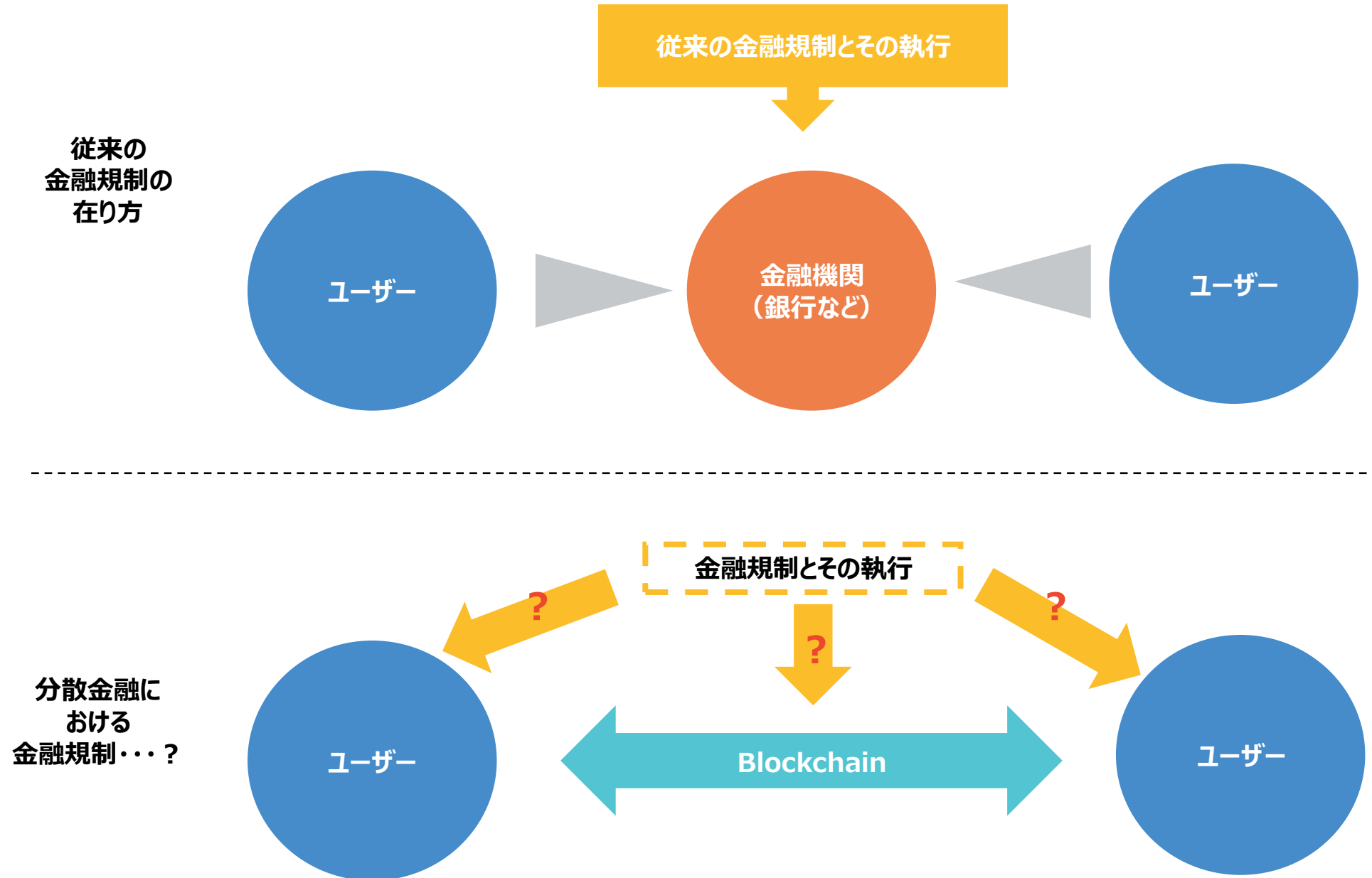


- 攻撃者は、無担保融資「フラッシュローン」の脆弱性を悪用し、DeFiのステーブルコイン取引プラットフォームであるCurveの「Yプール」にて、裁定取引による価格操作を行うことで、わずか7分足らずで不正に利益を引き出したとされる
- 流出したトークンの一部は、すでにERC-20基盤のBTCトークン「renBTC (rBTC)」と交換されたほか、トランザクションをミックスして匿名性を確保する難読化ツール「Tornado Cash (トルネード・キャッシュ)」を使用して、ステーブルコインUSDCやUSDTに変換された。
- 一方、分散型取引所「Uniswap」の取引高は、1日で1億4800万ドルから20億ドルまで急増した（流出したトークンがUniswapで交換されたとみられている）
- トラッキングツールによると、Flugsvamp3.0、Wm_cash、Coins.ph、Treddr、Kraken、Binance、Huobiを経由して移動している



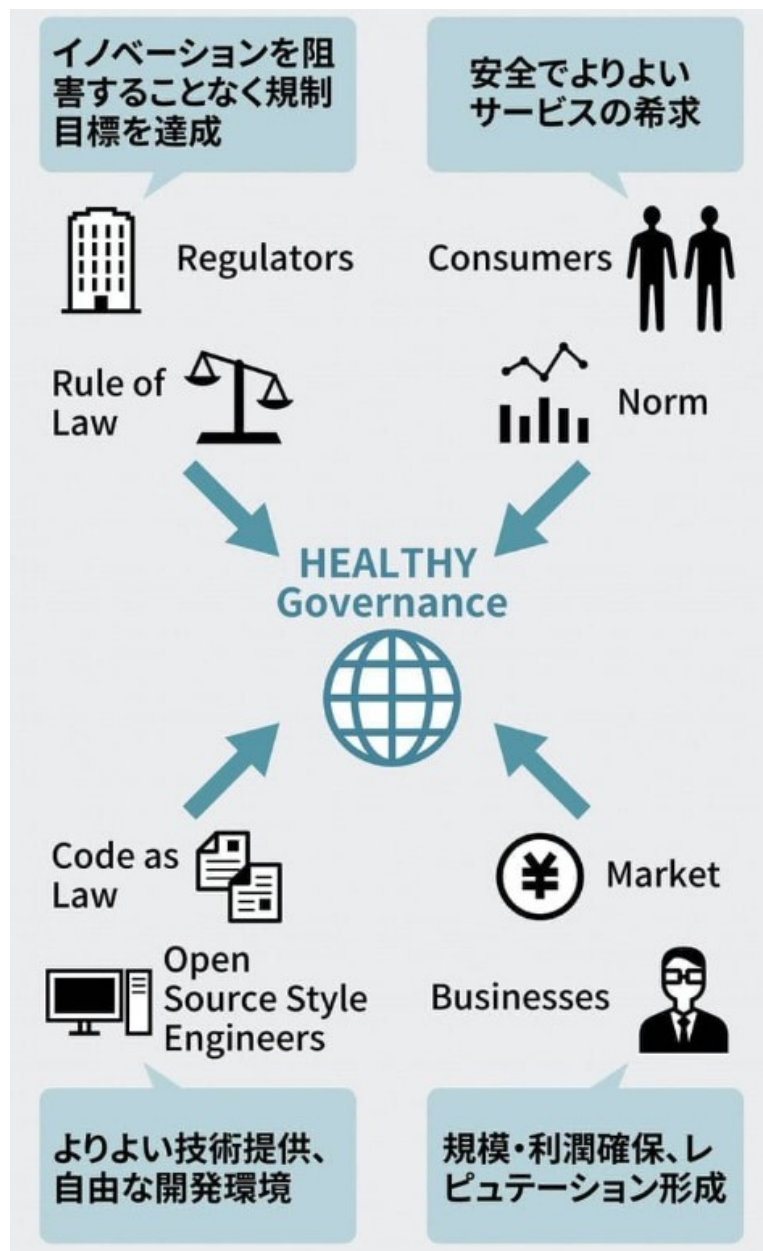


DeFiと金融規制





将来のブロックチェーンエコシステム（理想形）



分散型金融、官民でルール整備を フィンサム開幕

2020/8/25 20:30

保存 共有 印刷 印刷 ツイート その他

日本経済新聞社と金融庁の主催で、ブロックチェーン（分散型台帳）を使ったビジネスなどについて議論する「BG2C フィンサムBB」は25日、閉幕した。新たな仕組みによる取引の拡大を見据え、各国の規制当局だけでなく多様な参加者によるルール整備の重要性を確認した。

主要国の金融当局にとってブロックチェーンを基盤にした取引の広がりに対し、金融システムの安定をどう確保するかは大きな課題。従来の金融と異なり、ブロックチェーンの仕組みでは中央管理者が存在しないケースも想定されるためだ。

慶応大学大学院の鈴木茂哉特任教授はインターネット規制では「各国のルールに縛られず、参加者が一緒に問題解決に取り組んだ」と指摘し、ブロックチェーンにも応用すべきだと述べた。

金融庁で国際デジタル戦略を担当する高梨佑太氏は、金融規制だけでは限界があるとし「開発を担う技術者らと規制当局が共通の目的に向けて議論し、相互に理解することが欠かせない」と訴えた。米ストロングブロックのトーマス・コックス氏は金融システムを安定させるには「各国の法制度を調和させる必要がある」と強調した。

金融庁の氷見野良三長官も登壇し、新型コロナウイルス禍や格差問題などが世界の新常态（ニューノーマル）になったとし「いかに『信頼』を築くべきか」と問題提起。不特定多数で取引の正しさを承認するブロックチェーンの仕組みを生かせば金融に限らず「社会で協力できる分野は広がる」と期待を示した。



6. DeFiがAMLCFT、各種の観点からも問題なく運営されるためには・・・？



従来の「金融機関」がスマートコントラクト上の
「金融機能」となって動いているのは
画期的で素晴らしいこと！
(DXの観点からもよい方向に発展してほしい)

なので、
規制上も問題ない形にできないだろうか、
というのを考えてみました



①暗号資産取引所のガバナンス参加
免許を持っている取引所にて
KYCが終わったアカウントであるかを
判別するプログラムを
各DeFiのスマコンに組み込む。
また各取引所がガバナンストークンを
保有し改善提案等ができるようにする



②DID参照APIをスマコンに入れる
マイナンバー等を参照するプログラムを
各DeFiのスマコンに入れる。
KYCの観点をクリアすれば使っても
問題ない機能のみ、
コード監査の上アグリゲーターが纏めて
マーケティングする



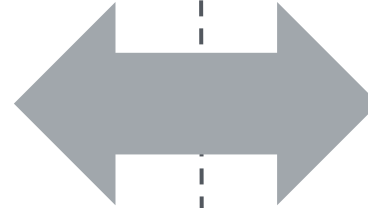
分散型金融の意義と今後の課題

分散型金融への期待、意義

- 金融安定化への貢献
- 金融取引における不確実性の低減
- 仲介業者への依存度低下（ソルベンシーリスク、流動性リスク低減）
- 可用性
- サイバーリスクに対する強靱性
- 金融サービスの利便性・多様性向上
- 信用ベースの既存金融システムとは異なる担保ベースのエコシステム
- 透明性の担保
- 顧客ニーズを満たす新たな金融サービス（マイクロペイメント等）
- 金融包摂

分散型金融の課題、リスク

- 金融安定化へのリスク
- 新たな集中リスク等
- 法的責任の曖昧化
- KYC/AML
- 消費者保護
- 既存の規制アプローチの限界



分散型技術のポテンシャルを最大限生かすためには、正しいリスク認識の下でリスク低減策を講じる必要

本件に関する弊社窓口



本日はありがとうございました。本件で当社に対してご質問やご相談がある場合は以下までご連絡ください。

■住所 〒107-6237 東京都港区赤坂9-7-1 ミッドタウン・タワー 37F

■連絡先 金光 碧
e-mail : midori.kanemitsu@bitflyer.com

Special thanks to 信玄さん、horyさん、平野さん、カナゴールド、斎藤創先生、牛田さん



ブロックチェーンで世界を簡単に。

