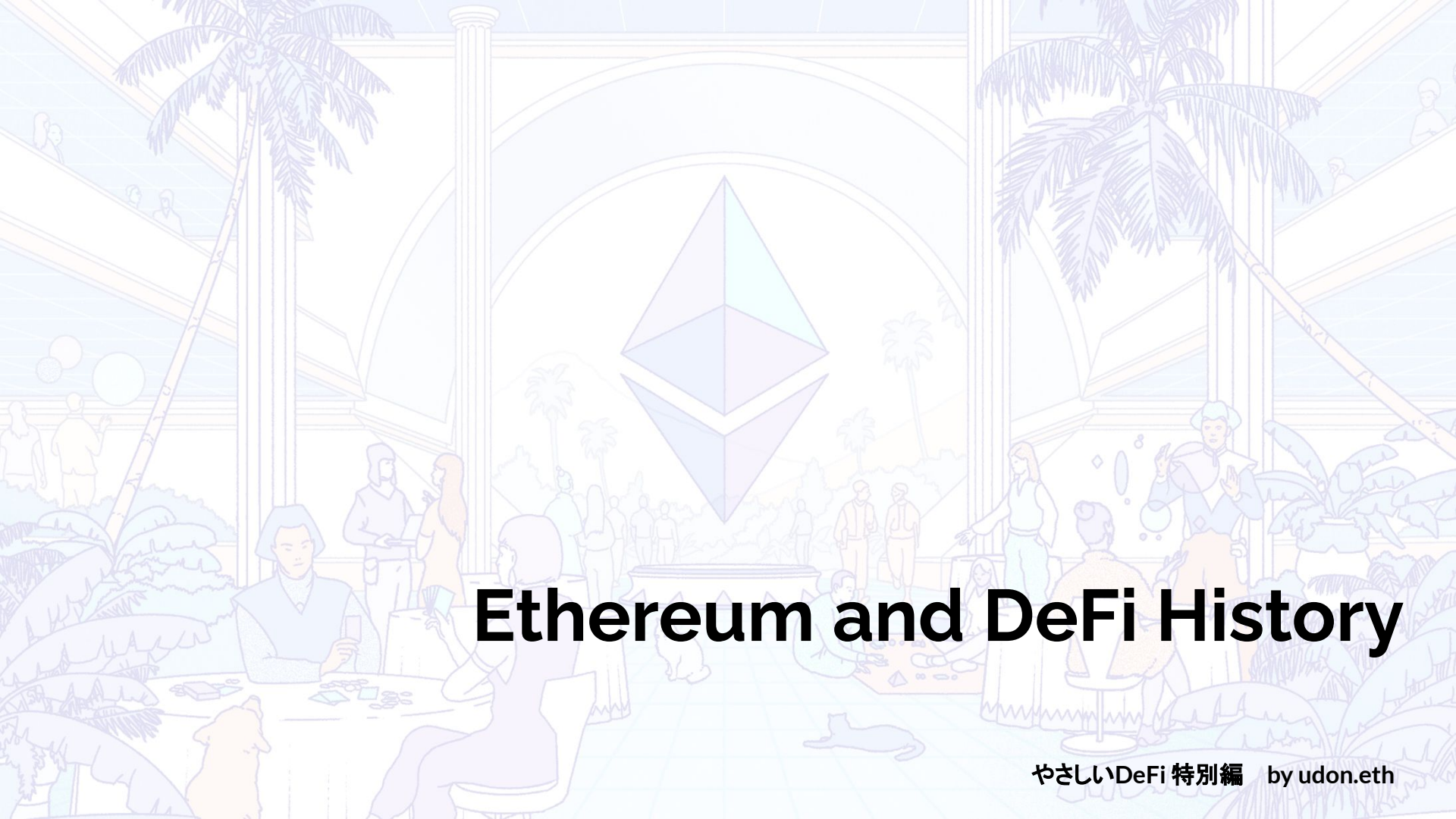


Ethereum and DeFi History

やさしいDeFi 特別編　by udon.eth

目的

EthereumやDeFiのあゆみを振り返り、

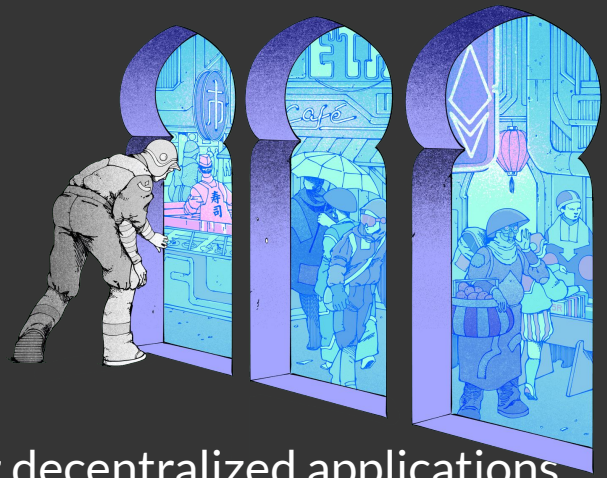
現在「なぜそのことが話し合われているのか？なぜスタンダードなのか」についてしる

Stats

Median Txs Per Block	200.50
Difficulty	2494892377415442
Gas Limit	12,372,021
Median Block Gas	12,377,104
Median Block Size	0.041 MB
Median Tx Gas Used/Limit	84.40%
Average Block Time	12 seconds
Market Cap (USD)	$35,556,676,663

Ethereumって何？

Ethereumとは



- 今回5歳の誕生日を迎えるクリプト
- “Ethereum is a global, open-source platform for decentralized applications. 直訳すると「EthereumとはDappsのためのグローバルでOSSなプラットフォーム。」
  - 何度も出てくる、Next-Generationとdecentralized applications
- みんなが自由にブロックチェーンアプリを作り、利用できる

→アプリケーションって何？スマートコントラクトって何？

Ethereumとは

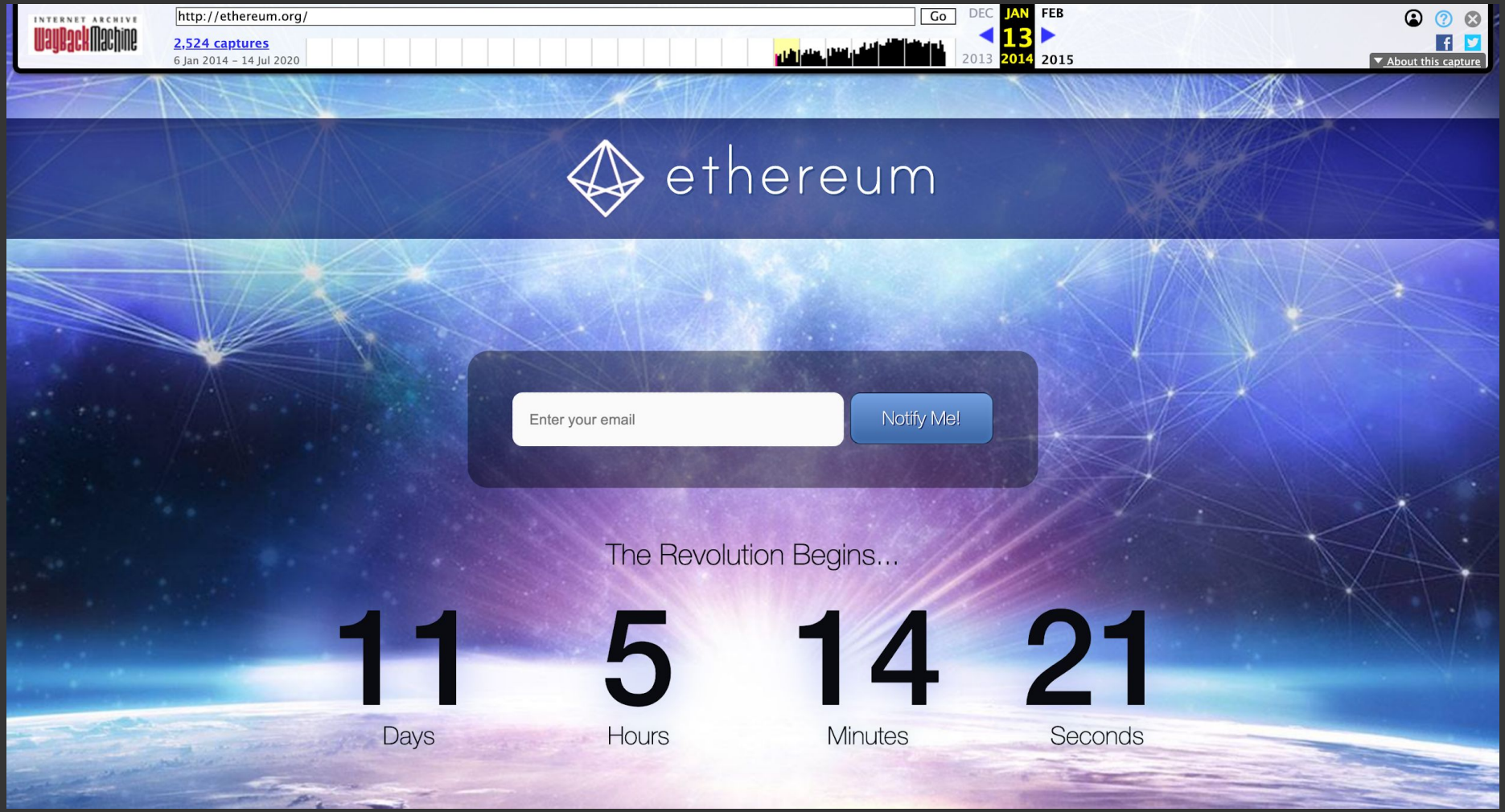
- ブロックチェーンの上で、プログラム(Script)を走らせること。（WebサイトをHostingしたり、なんかAWSの代わりに使うとかではないです。）
- パブリックブロックチェーンの特性(オープン、検閲耐性・改竄耐性やネイティブコインの存在、非対称暗号(署名)があるなど)を活用したアプリ
  - ex. Tokenの表現、DEX、DAO、金融派生商品の作成（合成資産など）、DNS的なものなど。
    そしてそれらの挙動は事前にプログラムでき、またさらに他のコントラクトを自由に利用・組み込みできるシステム

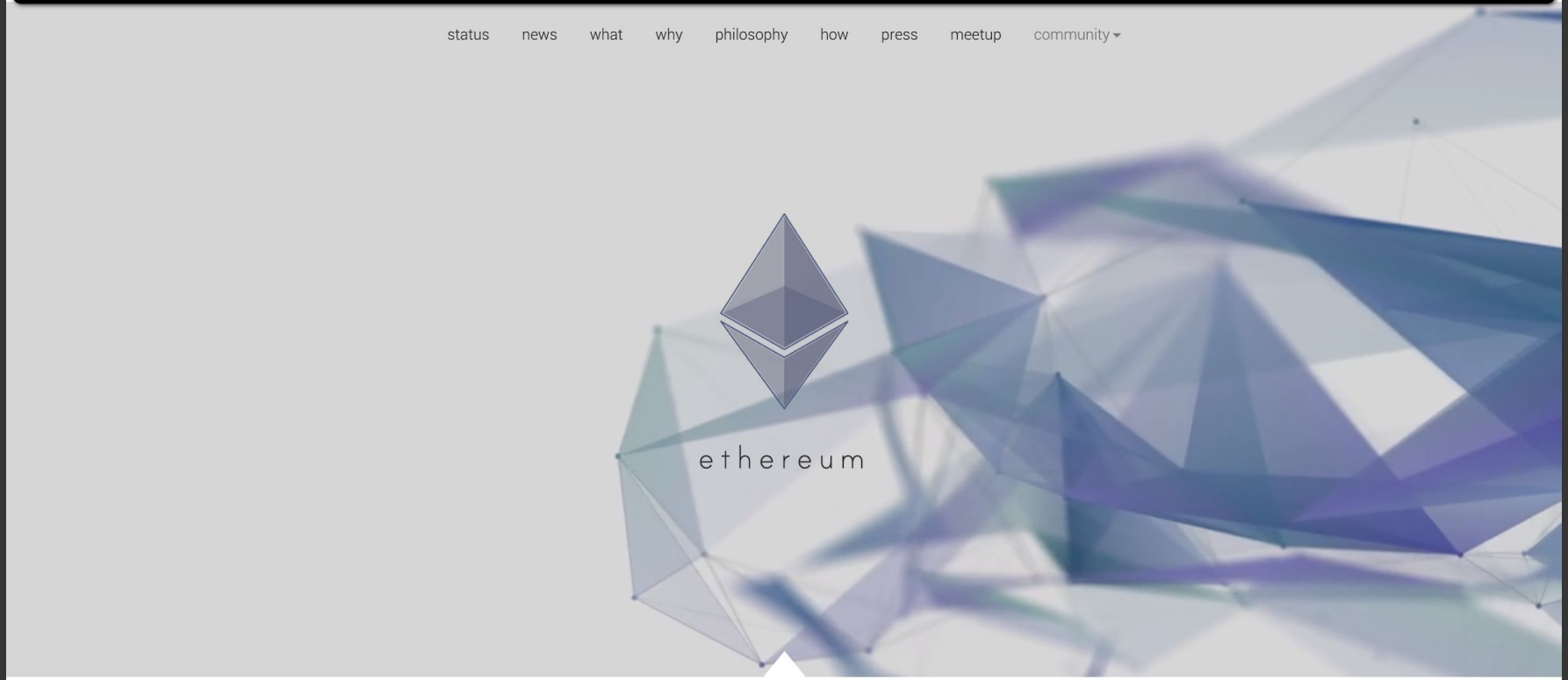
Ethereum初期のHP

Ethereum: The Ultimate Smart Contract And Decentralized Application Layer

Coming soon...

Google+


INTERNET ARCHIVE
WayBackMachine
http://ethereum.org/
Go
2,524 captures
6 Jan 2014 - 14 Jul 2020
DEC
JAN
FEB
13
2013
2014
2015
About this capture
ethereum
Enter your email
Notify Me!
The Revolution Begins...
11
Days
5
Hours
14
Minutes
21
Seconds



the ethereum ether sale has now concluded.

Philosophy

- simplicity: コントラクト開発者が開発しやすいようプロトコルはシンプルに
- Universally: Ethereumは何か特定の目的に特化しない。
- non-discrimination: Protocolは何か特定の”望ましくない”アプリを排除しない。手数料を支払ったなら、プロトコルに害を与えない範囲では自由にすべき
- modularity: プロトコルの各要素はモジュール化
- agility: より良い変更ができるならそうする(主に開発中だったため)

提唱してたもの

- Name Registrasion
- Metacoin（独自トークン）
- data feed
- ヘッジ契約
- DAO
- クラウドファンディング
- Shellingcoin


ETHEREUM
FRONTIER

Frontier  (2015/7/30~2016/3/14)

- 8893ものICO参加者が受け取る
- 超初期版のため、Admin Switch(Canary Contract)が存在
  - フォークした場合の正しいチェーンの宣言、ネットワーク停止権限、
- まともなGUIのウォレットがない (gethくらいしかない。MEWは2016/5くらい)
- 本当に開発者向けのベータ版くらい（言語もLLLとか色々あった）
- ERC20が2015/11/19くらいに提案された。ローンチ直後は独自規格のはあっても統一されておらず
- BlockRewardは5ETH、個人のPCでソロマイニングしても1日に一回くらい掘れた？CPUマイニングが最初。

Homestead 

(2016/3/14~2017/10/16)

- ERC20の規格も定まり、ICOもちょこちょこあった(記憶があるくらい)
  - その時はあるコントラクトアドレスにETHを送ると定められた数量のトークンが帰ってくる仕組み。今のDeFi?
- 大きかった出来事としてはThe DAOとそのHack。とても示唆に溢れているので次ページから特集します。

REMEMBER THE DAO

THE DAOの概要と仕組み

- DAO(自律分散型組織)を実装したDAOの一つ
- EthereumをつかったSmart key StartupのSlock.itが作成
  - もともとICOやろうとしていたが、規制の関係上?投資ファンドDAOを作って、そこから出資してもらおうとした。
- 2016/4/30にローンチされ、28日間のICO?
- 当時”クラウドファンディング”としては世界最高の180億円を調達(ETHでなのでブレてる)
  - 扱いとしては、この頃は謎のチケットを配ってるクラウドファンディングと同じだった
  - ETH総発行量の14%がこのThe DAOに集まる

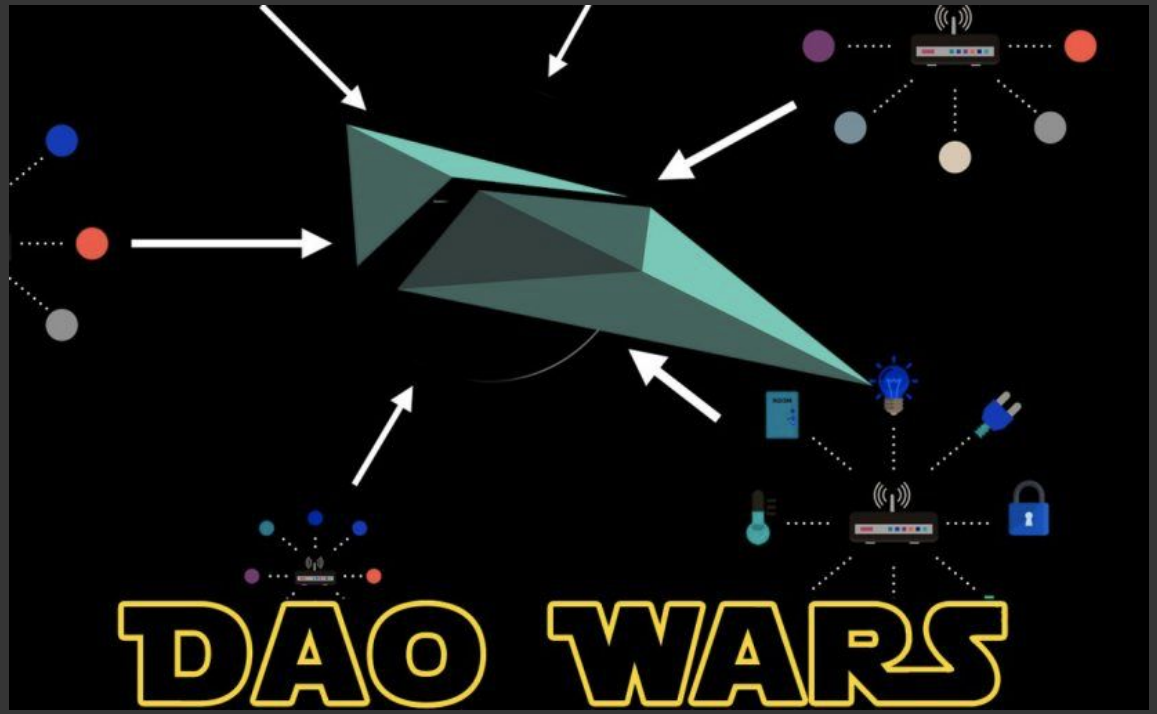
THE DAOの概要と仕組み

- The DAOホルダーは投票して、賛成した人がchildDAO（出資先のDAO）のトークンが受け取れる仕組み
- 最低投票数は20%（高めに設定してしまったため超えない→Proxy的なものがサードパーティーで提案中だった）
- Splitという機能を使えばReserveしていたETHを引き出すことが可能(投票してYesを出して出資した分のトークンについては償却されない）
  - 30日くらいたてば引き出せる状況
- The DAOの流出につながった脆弱性については5/27（ちょうど終了間際くらい？）くらいにVladさんとかEminさんが報告

THE DAO HACK

- Splitの再帰性攻撃（引き出し処理してDAOトークンの残高を書き換える前にもう一回引き出し処理をする）により、大量に引き出しが生じる
- それを検知したWhiteHackerが同じ手口を使ってThe DAOから資金を引き出す。1150万 Etherのうちの360万ETHがHackerに、残りがWhiteHackerに
- 即座に公式より、Ethereum NetworkにDDOS攻撃をしてくれという呼びかけ
- The DAOトークンは大暴落（無価値にはならず、五円くらいで反発、HardFork期待？）、Poloniexはサーバー落ち、公式アカウントはEtherとDAOトークンの入出金停止を呼びかけ

DAO WAR



DAO WAR

- 引き出しには28日間の猶予があったので、その間にソフトフォークを実行
- そのごHackをなかったことにするHardForkを実行する
- HardForkは大きな議論を呼ぶ
  - 一介のアプリケーションがハックされただけなのにロールバックを行うのは?(Code is lawはどこに?) 基準はどこに?（後々、ParityのMultisig凍結の際は特に実行されなかった）
- ハッカーを名乗るものが現れ、「プロトコル仕様に従って引出しただけであり合法である」といい、さらにHFに反対したマイナーにETHを送ると表明

Ethereum Classicの誕生

- 実際HF直後は、旧チェーンを使ったり取引できたりといったことは本当に細々とやっていたくらいだった
- 突如Poloniexが上場させ、Feverに（Barryさん推し）、一時対ETH建てで0.5ETHいく
- その時も、「Applicationはどちらに対応すべきか問題」が出る。多くは、様子見かETH側で、様子見が多かった。（現在ほどアプリケーションが乗ったら...?）

ICO 2016後半~2017年

- ICO、ICO、ICO、ICO
- The DAO以降、「集め過ぎはよくない」ということでCapを設けるICOが一般的に（3〜6億円くらい。10億だと多め？@2016年）
- 希少性が生じ、ICOで買って即座に市場で売れば数倍になるというフィーバー状態
- ICOでは、プロBuyer（Gasを1000GWeiに設定して、ブロックが指定の数字になったら即送金）が買い占めることが多発。BraveのICOではほんの十人以下くらいがほとんどを買う。→規制の流れもあり、KYCと個人のCapを設けるように。
- ほとんどのProjectは消えましたが、結構残ったものもある（BNBとかLInkも2017年）

DeFiの芽（2017〜2018）

- AMMという概念の登場：Bancor Protocol（2017/7）とICO
  - その時はReserve（準備金）といってたのでわかりずらかったのかも
- EtherDelta（2016~2017頭から流行ってたOn-Chainの板取引所）
- 0x v1（2017/7）
- MakerDAOのLaunch（2017/12）
- Kyber Network Launch(2018/2)
- Compound v1 Launch（2018/9）
- DeFi.network、DeFIという言葉が生まれた（2018/10/15）
- dydxのExpo（2018/10）、板は2019/4
- Uniswap Launch（2018/11）

2019-2020 DeFi Growth

- 0x v3
- compound v2
- Uniswap v2
- MakerDAO MCD
- dydx perp swap
- DXDao、Omen、Gnosis Protocol
- loopring
- AAVE
- Augur
- Curve.fi
- New Project、New Project、New Project!!!

DEFI PULSE

Rari Capital – A Yield-Maximizing Robo-Advisor that Takes Risk Management Se... Read on the DeFi Pulse Blog ▸

Total Value Locked (USD)

$3.81B

Maker Dominance

27.81%

Total Value Locked (USD) in DeFi

TVL (USD) | ETH | BTC | DAI All | 1 Year | 90 Day | 30 Day

Earn the highest returns from a variety of trusted DeFi protocols with Rari Capital. Start earning today

DeFi Pulse Farmer

Be the first to read Newsletter #1!
- Fresh yield farming plays
- Insight on big governance decisions

ALL | LENDING | DEXES | DERIVATIVES | PAYMENTS | ASSETS

DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
🏆 1.	Maker	Ethereum	Lending	$1.06B	-0.03%
🥈 2.	Compound	Ethereum	Lending	$784.1M	-0.56%

DeBank
Your DeFi Wallet

- Dashboard
- Portfolio
- Interest Rates
- Token Swap
- DeFi List
- Ranking

- About

English/中文

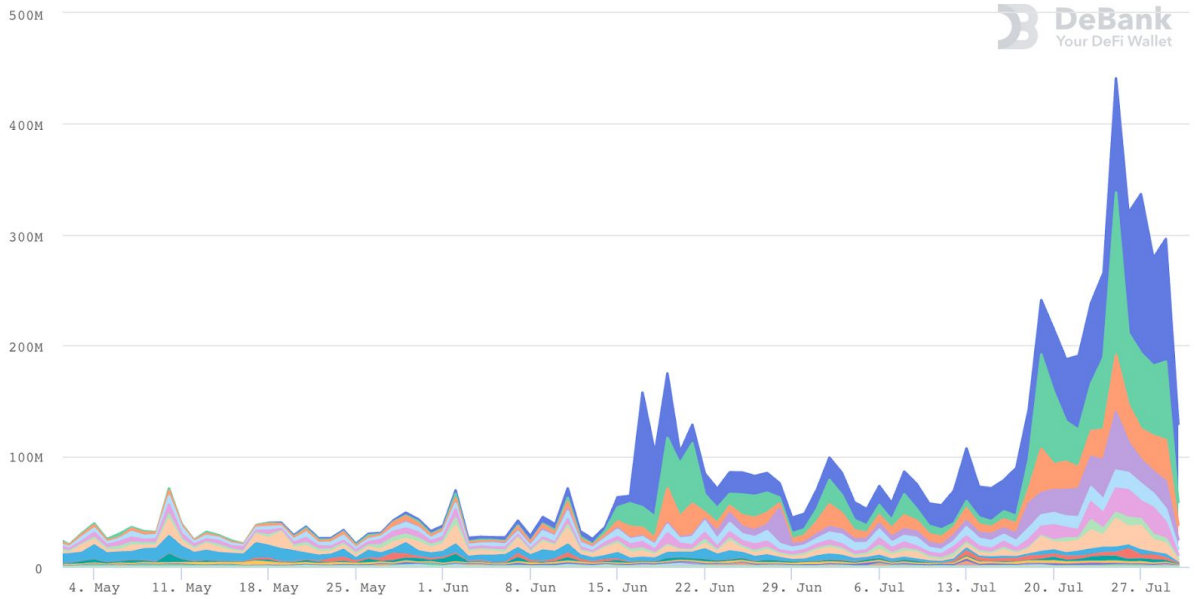
Trading Volume

Total trading volume(24h)
$300.22M

3M

Uniswap V2 Curve 1inch Balancer Kyber Network 0x
Tokenlon dYdX Uniswap Bancor Oasis IDEX
ParaSwap Loopring DDEX Airswap DEX.AG dForce Swap
Radar Relay dex.blue

Check all Uncheck all



#	NAME	TYPE	24H VOL	24H TXS	24H USERS
1	Uniswap V2	Liquidity Pool	$136,544,206	61,338	11,469
2	Curve	Liquidity Pool	$58,766,864	1,156	229

Ethereum2.0 (旧Serenity)

- もともとあった概念におけるSerenity(静けさ)の段階
  - Frontier、Homestead、Metropolis、Serenityをローンチ時に想定してた
- 言葉が出てきたのは、Ethereum 2.0 mauve paperというのが2016/9/10くらいに出てきた時から。そこからEthereum2.0というのが一般的に
- 大きな変更としては
  - Proof of WorkからProof of Stakeに
  - Shardingの導入
  - (あとはStateless Ethereumとか諸々)

Ethereum2.0

- Ethereum 1.0と2.0は別チェーン、変更は1.0のDeposit ContractにDepositして2.0にうつす
- Ethereum 2.0の段階
  - Phase 0: Beacon Chainのみ。ETH転送は基本できない。
  - Phase1: Sharding, No VM
  - Phase 1.5: Ethereum 1.0のStateを持ってくる
  - Phase 2: eWASMと多様なVM

Ethereum2.0

- ETH2でのDeFi
  - とりあえず今のような手数料は抑えられそう(ただBeacon Chainに刻むコストはかなり高めではありそう)
  - Composabilityの確保は、Liquidity Provider的なものかinvoiceで行う？
-