

Ethereum

世界コンピューター

その社会応用実験例

Lifetime Mail Account Services / LiTMAS 合同会社 関 一典

**“Blockchain technology will have a
dramatic impact on business and society”**

Don Tapscott

「仮想通貨の技術が未来の主役になる」

野口悠紀雄

ハッシュ (Hashes)

入力:

ハッシュ:

- 任意の入力
- 同じ長さの出力
- 異なる入力と同じ出力になることはほとんどない
- チェックサムを計算するのと同じようにそのファイルが正しいことを確認できる

“Hello, Seattle!”



89053f58ec93cd74
0e44e1a79999663d

“Hello, Seattle”

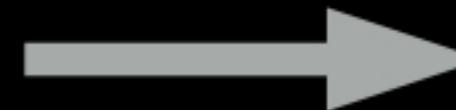


78c822c6b2f9cb44
62fa80e408496233

space_oddity.mp3



9955f0021f91b98cb
d3f08dd49827b67



6fdf28c41257de9fc
74c33eaaae226ef

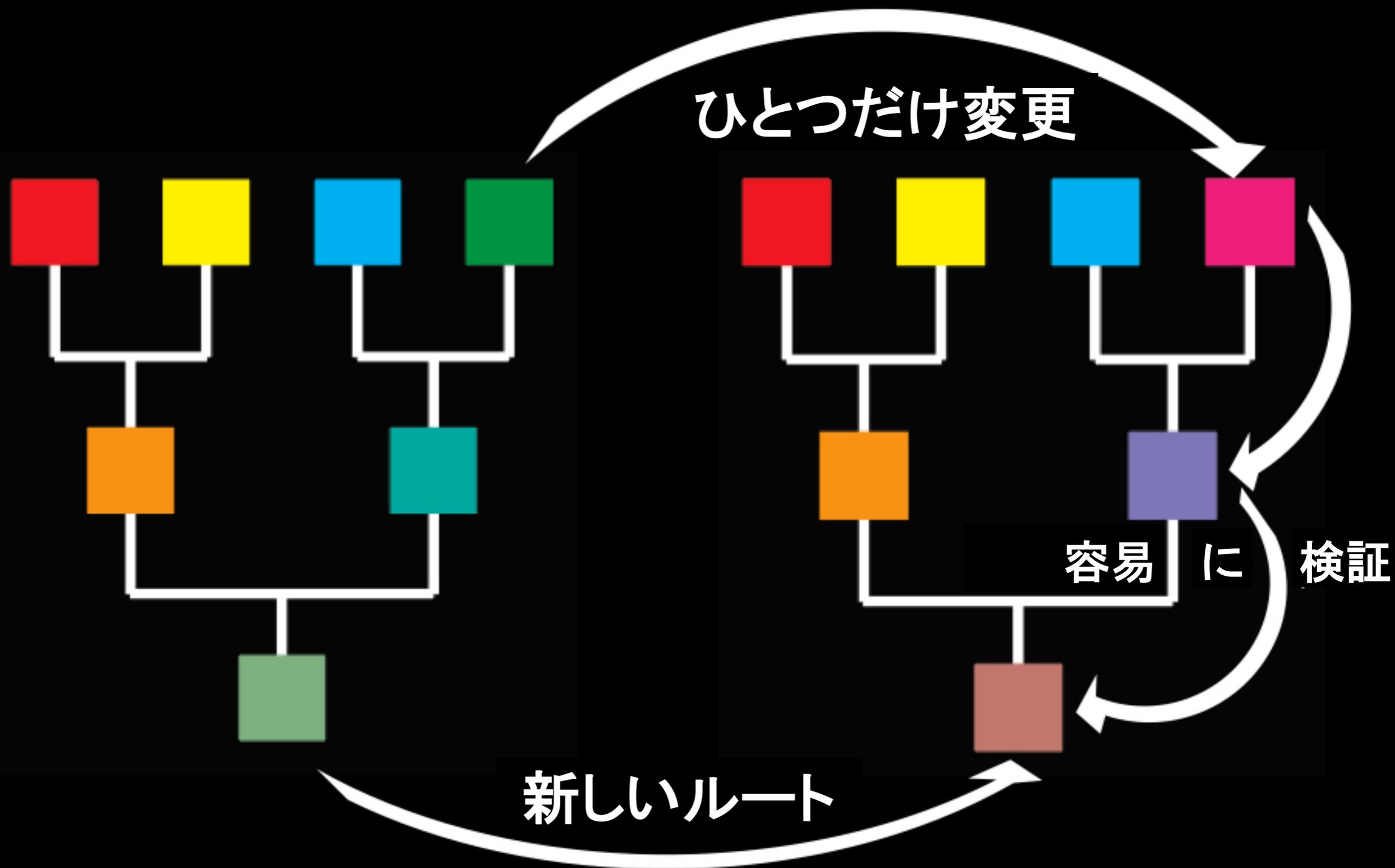
this_slideshow.ppt



????????????????

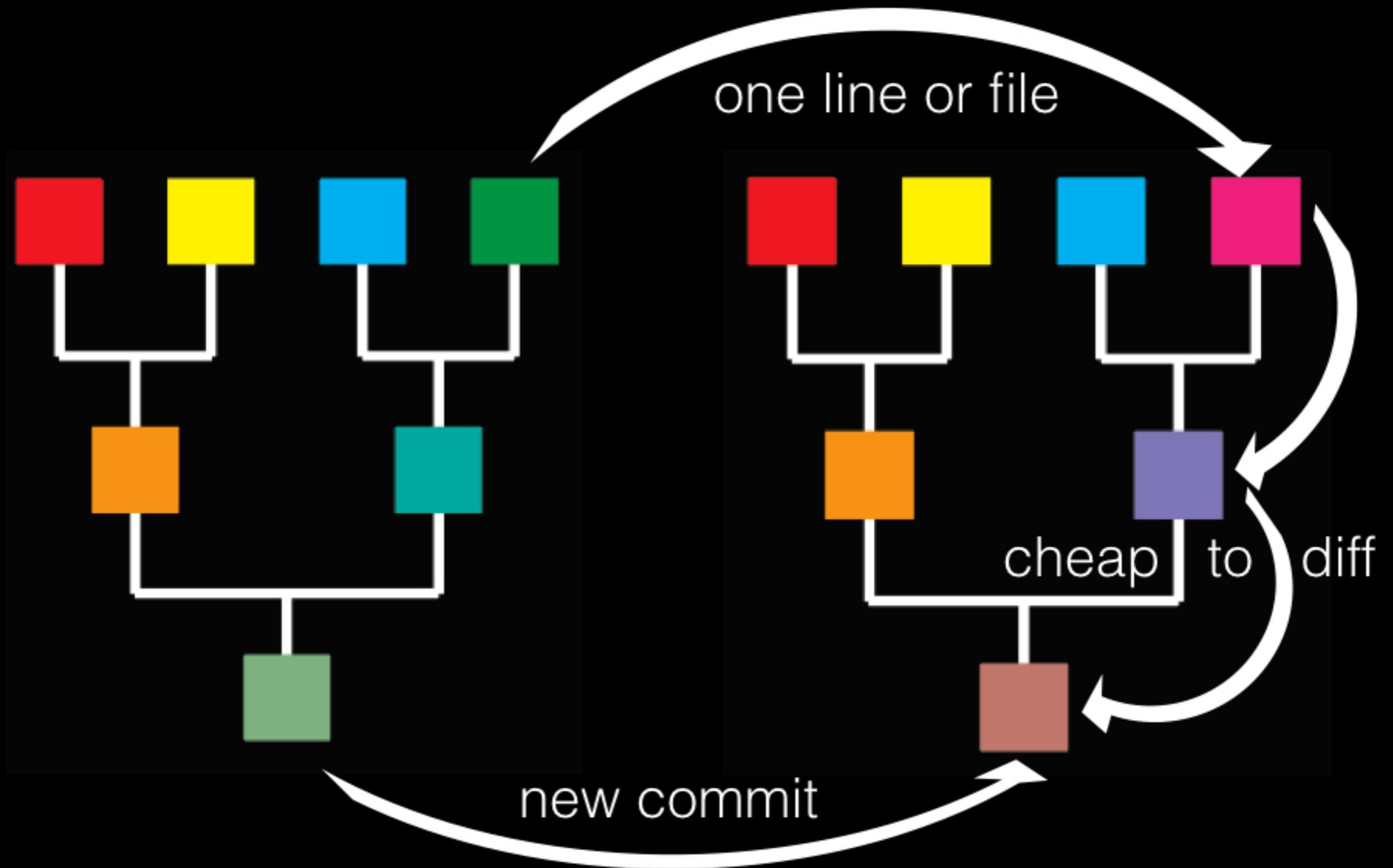
マーケルツリー (Merkle Trees)

ハッシュのハッシュ!



Git

Merkalized Version Control



ブロックチェーン

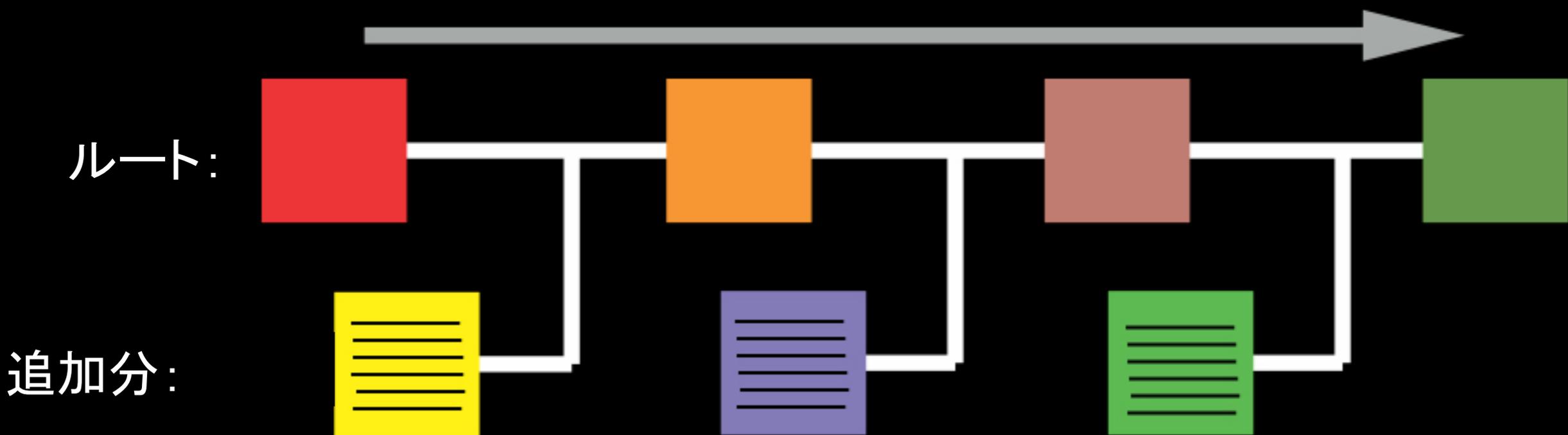
恒久的に増え続けるマークルツリー





Bitcoin

ブロックチェーンによる台帳や元帳



Avoids double-spending
by ensuring transaction ordering.

同じ「お金」が何度も使われることを防ぎ
順序を間違えることなく行う

合意形成 (Reaching Consensus)

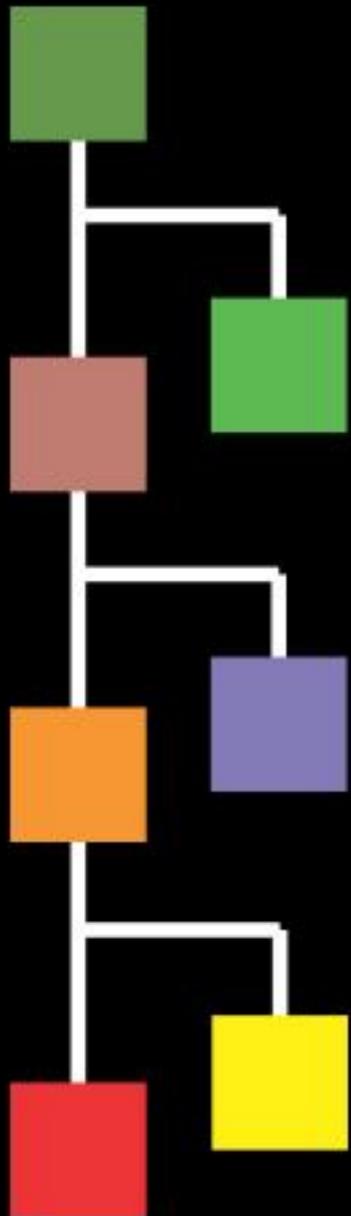
共有している元帳にどうやって追加していくのか

Proof of Work

(より多くの作業が行われているものを正しいとすること)

- Blocks are added gradually. 少しずつ順番に
- People take turns adding blocks. (“One CPU One Vote”) 自分の番の時
- Bitcoin style: The root checksum must start with a number of zeroes! (Difficulty) 独自のルールで
- The block includes a nonsense “nonce” that can be changed to create new checksums. 新しいチェックサムとわかる印をつけて
- The difficulty is adjusted to target a desired time between blocks.

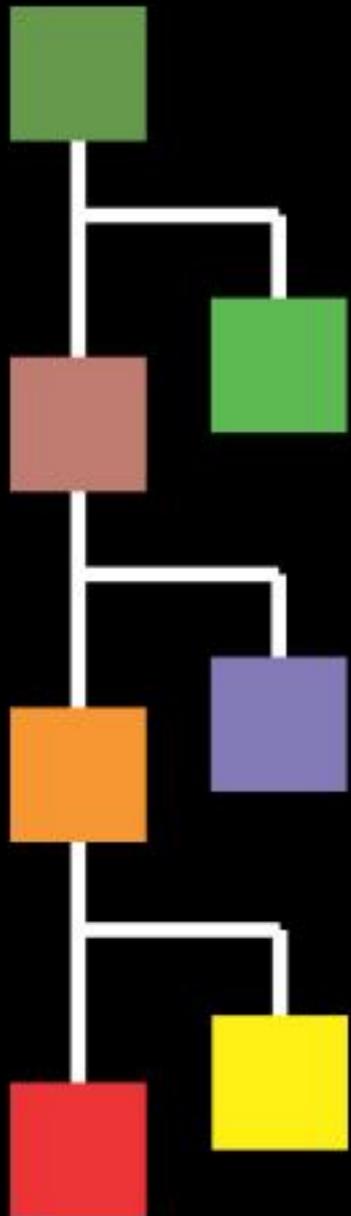
ある程度難しい計算が完了してから次が作られるようにして調節



合意形成 (Reaching Consensus)

共有している元帳にどうやって追加していくのか

Incentives / 報奨機能



- The miner who finds a new block, gets a reward. 最初に見つけるとご褒美
- This reward is used as currency, and to pay transaction fees. 「それ」は譲渡交換でき、使用料金として使える
- In addition to the block reward, the miner gets transaction fees. その塊の使用料金も同時に取得
- This encourages miners to process blocks with transactions. そのため採掘業者が他人の分を取り込む
- This encourages users to pay fees depending on urgency. 処理の迅速性に応じて支払い額をユーザーが決める

処理の迅速性に応じて支払い額をユーザーが決める



Ethereum (イサーリアム/エサリウム)

Put a computer on the blockchain

(ブロックチェーン上に作り上げた仮想計算機)

ルート:



仮想計算機
の内部状態:



その使用を
使用料金として算出することができる
仮想計算機を規定したもの

ethereum.org

[\(traffic\)](#)



Build unstoppable applications

Ethereum is a **decentralized platform that runs smart contracts**: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.

These apps run on a custom built **blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property**. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk.

The project was bootstrapped via an ether pre-sale during August 2014 by fans all around the world. It is developed by the [Ethereum Foundation](#), a Swiss nonprofit, with contributions from great minds across the globe.

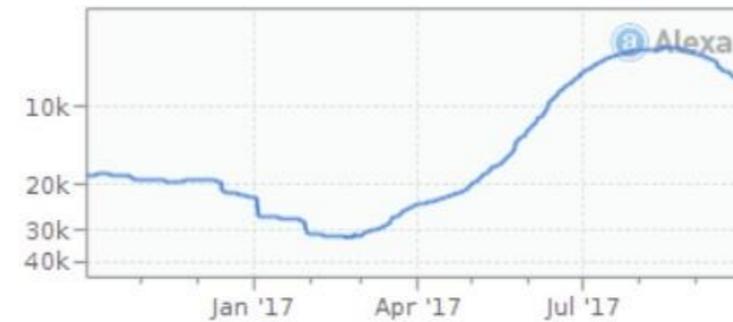
YOUR FRIENDS

YOUR VIDEOS

OPEN CHAT

Alexa Traffic Ranks

How is this site ranked relative to other sites?



Global Rank ?

8,439 ▼ 1,047

Rank in United States ?

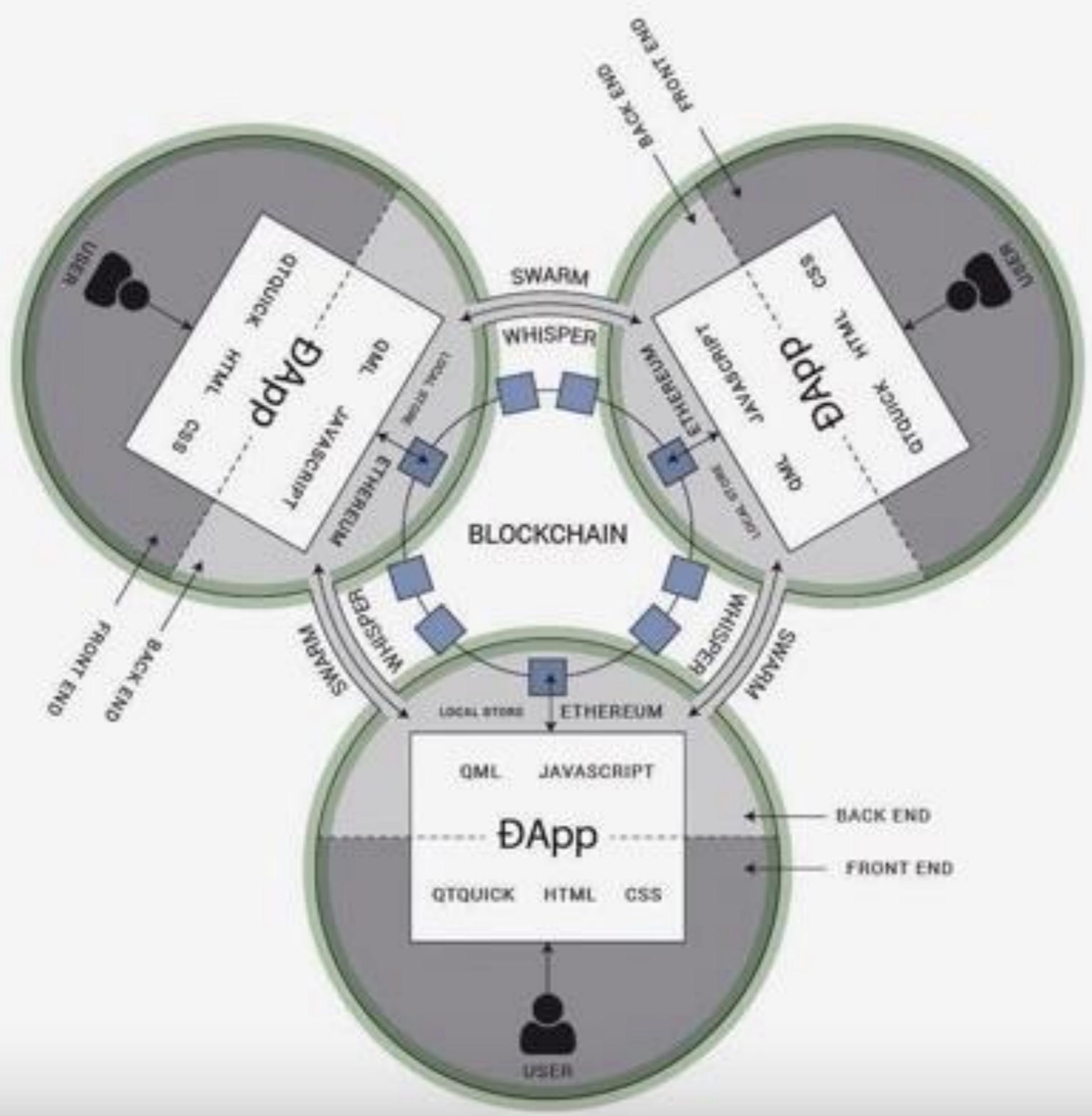
6,288

Country	Percent of Visitors	Rank in Country
United States	26.4%	6,288
China	8.0%	10,943
Japan	5.5%	9,503
India	4.7%	9,854
United Kingdom	4.0%	6,813

[Subscribe to View](#)

How engaged are visitors to ethereum.org?

?



分散型アプリケーションカタログ

stateofthedapps.com (dapps.ethercasts.com)

STATE OF THE DAPPS A Curated Collection of 714 Decentralized Apps for **ethereum**

What's a DApp [Submit a DApp](#)

Search by DApp name or tag

Showing 200 results Show recently added and hide nothing

T The Pyramid Game by Jesse Busman Place blocks to build a pyramid and profit LIVE	B Blockaction.io by Avrach +1 Secure and simplified transactions for digital assets LIVE	H HelloSugoi by Angello Pozo +1 Create and purchase tickets for events LIVE	T Tug Of War by Etherplay A fully decentralised 2 player game of wit PROTOTYPE	A Arbiz Platform by Danil Lalygin Marketing cross platform CONCEPT	E evolve110 by Vanya A. Sergeev Rule 110 is a Turing-complete cellular automaton LIVE	E Eth Capsule by wy Bury ether for as long as you want LIVE
T Trippki by Ed Cunningham Hotel booking and rewards platform WORK IN PROGRESS	G Goal Bonanza by Veljko Ristic Football betting PROTOTYPE	E EthCrow by Nedodn Escrow Service PROTOTYPE	D DECENTREX by Decentrex Team Smartcontract powered tokens exchange LIVE	S Sifetly by bellaj badr P2P money transfer WORK IN PROGRESS	S SOLFI by Jamel C Lyons Financial services WORK IN PROGRESS	B BioPayCoin by Stephen Arsenault New layer of wallet security WORK IN PROGRESS

稼働状況

BEST BLOCK
#3,901,990

UNCLES (CURRENT / LAST 50)
0/4

LAST BLOCK
31s ago

AVG BLOCK TIME
16.33s

AVG NETWORK HASHRATE
35.7 TH/s

DIFFICULTY
830.41

ACTIVE NODES 62/62

GAS PRICE 20.000 gwei

GAS LIMIT 4712394 gas

PAGE LATENCY 25740 ms

UPTIME 100%

BLOCK TIME

DIFFICULTY

BLOCK PROPAGATION

LAST BLOCKS MINERS

0x61c808d82a3ac53231750dad13c777b59310bd91

0xea674fdde714fd979de3edf0f56aa9716b898ec80

UNCLE COUNT (25 BLOCKS PER BAR)

TRANSACTIONS

GAS SPENDING

GAS LIMIT

ATTENTION! This page does not represent the entire state of the ethereum network - listing a node on this page is a vol

Node Name	Client	Latency	Sync	Uptime	Version	OS	Block	Hash	Gas	Uptime	Latency	Block Time
arcturus	Parity/v1.6.8-beta-c396229-20170608/x86_64-linux-gnu/rustc1.17.0	118 ms	⊗	510	0	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+8.7 s
Bootnode-AU	Geth/v1.6.5-stable-cf87713d/linux-amd64/go1.7	233 ms	⊗	448	443	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+2.6 s
ethfra.globalmine.net	Geth/v1.6.5-stable-cf87713d/linux-amd64/go1.8.1	68 ms	0 KH/s	128	161	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+4.2 s
rigel	Parity/v1.6.8-beta-c396229-20170608/x86_64-linux-gnu/rustc1.17.0	118 ms	⊗	13	0	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+707 ms
Foundation Monitoring (Latest)	Geth/v1.6.5-stable-cf87713d/linux-amd64/go1.7.3	431 ms	⊗	12	1180	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+1.7 s
ethiz.globalmine.net	Geth/v1.6.5-stable-cf87713d/linux-amd64/go1.8.1	495 ms	0 KH/s	128	17	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+4.7 s
kinETH	Geth/v1.6.5-stable-cf87713d/linux-amd64/go1.8.1	50 ms	⊗	55	445	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+4.5 s
5chdn-supernode-deneb	Parity/v1.6.7-unstable-e12841814-20170518/x86_64-linux-gnu/rustc1.17.0	71 ms	⊗	87	0	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+3.5 s
fomalhaut	Parity/v1.6.8-beta-c396229-20170608/arm-linux-gnu/rustc1.17.0	74 ms	⊗	25	0	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+3.5 s
Cotton Candy	Geth/v1.6.5-unstable-ac92d7c4/linux-amd64/go1.7.3	446 ms	⊗	100	898	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+1.3 s
kinETHity	Parity/v1.6.8-beta-c396229-20170608/x86_64-linux-gnu/rustc1.17.0	183 ms	⊗	50	0	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+504 ms
kingbubbles	Geth/v1.6.5-stable-cf87713d/linux-amd64/go1.8.1	32 ms	⊗	11	254	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+6.9 s
Astatium	Parity/v1.6.7-beta-e128418-20170518/x86_64-linux-gnu/rustc1.17.0	366 ms	⊗	511	0	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+1.4 s
ethny.globalmine.net	Geth/v1.6.5-stable-cf87713d/linux-amd64/go1.8.1	6 ms	0 KH/s	128	169	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+4.1 s
ethist.globalmine.net	Geth/v1.6.5-stable-cf87713d/linux-amd64/go1.8.1	120 ms	0 KH/s	128	125	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+8.2 s
MrYukonC	Parity/v1.7.0-unstable-2ec51fc-20170517/x86_64-linux-gnu/rustc1.17.0	53 ms	⊗	49	0	#3,901,989	ba5e9438...98d802ec	374,443,753,332,649,100,000	221	0	3 min ago	+775 ms

使用料金情報 (ETH GAS STATION)



Estimates over last 10,000 blocks - Last update: Block 3902000

Change Currency

GENERAL

Main Page

Gas-Time Calculator

Miner Stats

Hash Power by Gas Price

Low Gas Price Watch List

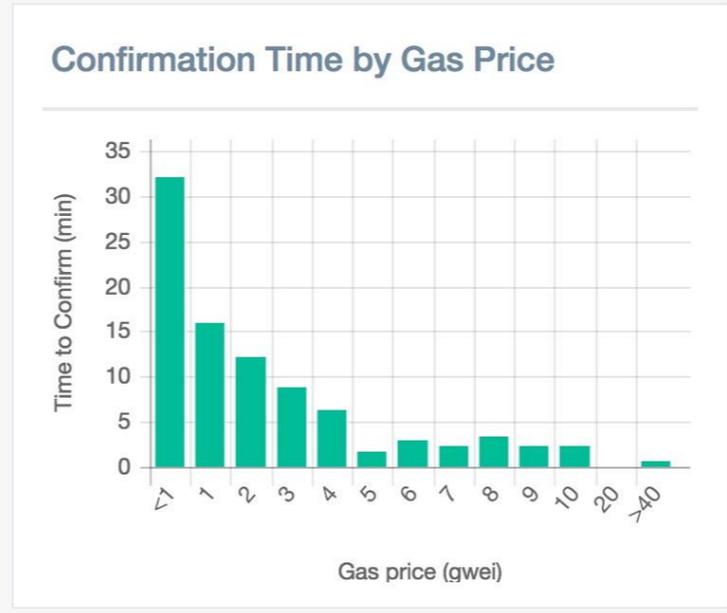
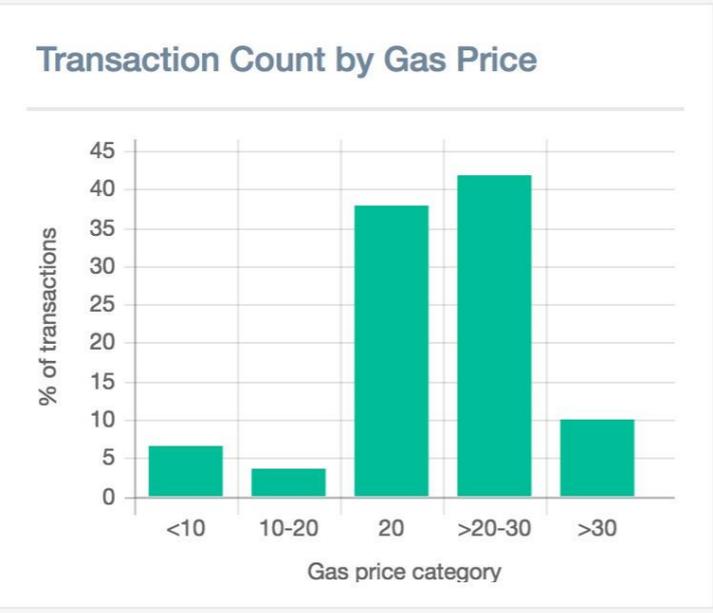
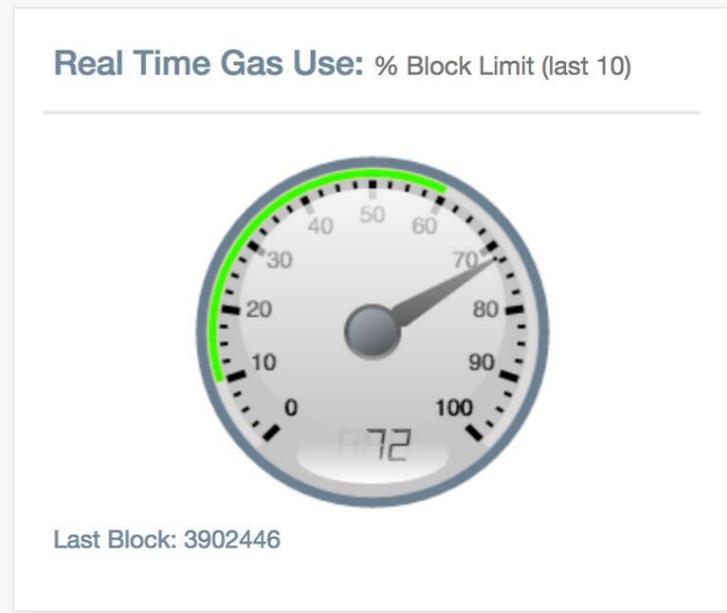
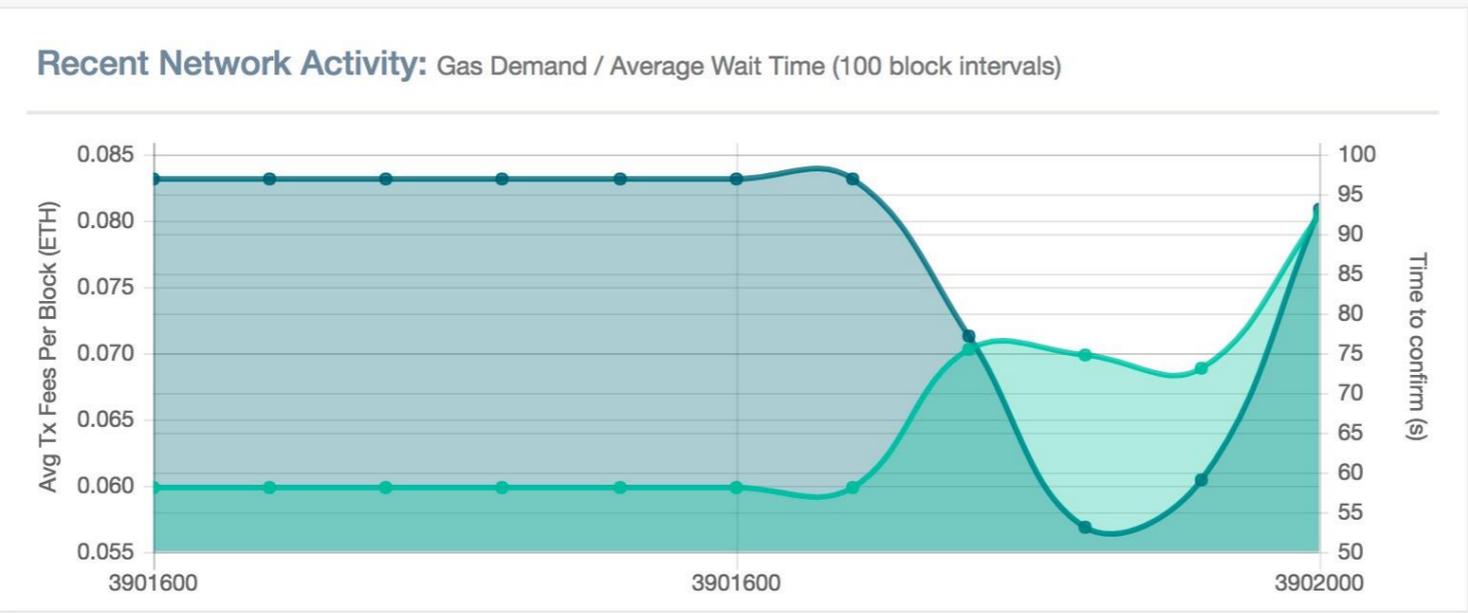
Gas Profits

Gas Burners

FAQ

External Links

<p>Median Cost for Transfer</p> <p>\$0.152</p>	<p>SafeLow Cost for Transfer</p> <p>\$0.015</p>	<p>Median Wait (s)</p> <p>65</p>	<p>Median Wait (blocks)</p> <p>4</p>	<p>Gas Price Mid (Gwei)</p> <p>20</p>	<p>Gas Price Low (Gwei)</p> <p>0.501</p>
---	--	---	---	--	---



Recommended User Gas Prices

Desired Tx Speed	Gas Price (gwei)	Average Wait (m)
Safe Low	2	0
Average	4	0
Fastest	27	0

Top 10 Miners by Blocks Mined: Support for user transactions

Misc Stats (Last 10,000 blocks)

MyEtherWallet CX (簡易UX)

必ずここに保管するすべてのお財布の「外部バックアップ」を作成してください。このChrome Extensionでは、再導入などで、データが保存されず消失することが頻繁に起こります。このエクステンションは容易な操作を提供するのみで、「バックアップ」は行いません。

MyEtherWallet CX 3.10.3.7 日本語 GAS価格: 5 Gwei Network: ETH (MyEtherWallet)

自分のお財布 お財布の追加 Ether/トークンの送送 通貨の両替 契約 ENS 処理状況を確認 Help

自分のお財布

	015 8b0214e7F9c10	0 ETH	
	Be1F3aCa1f9c	0.02 ETH	
	IP2016A ea62Eee1a6fd	0 ETH	
	ask#1 387ad56C3222	0.05 ETH	
	01 3FCE8767f0ED7	0 ETH	
	02 3d065dB3D1452	0 ETH	
	6 0CB930dc6202c	0.13 OMG 2,013 SGT	

- ETH (MyEtherWallet)
- ETH (Etherscan.io)
- ETH (infura.io)
- ETC (Epool.io)
- Ropsten (MyEtherWallet)
- Ropsten (infura.io)
- Kovan (Etherscan.io)
- Rinkeby (Etherscan.io)
- Rinkeby (infura.io)
- RSK (GK2.sk)
- EXP (Expansetech)
- UBQ (ubiqscan.io)
- Add Custom Node

世界コンピューターは、

『分散型自律組織』DAOが

『合意形成プロトコル』を用いて

『スマート契約』を実行する

分散型自律組織先進例1: The DAO – 分散型自律ベンチャーファンド (2016)

 The DAO

[CREATION](#) [PROPOSALS](#) [MANIFESTO](#) [CURATOR](#) [PRINCIPLES](#) [VOTING](#) [FORUMS](#) [TERMS](#) [SUPPORT](#) [BLOG](#)

786.91 M
DAO TOKENS CREATED

7.87 M
TOTAL ETH

81.52 M
USD EQUIVALENT



1.00
CURRENT RATE
ETH / 100 DAO TOKENS

11 hours
UNTIL NEXT PRICE
CHANGE

14 days
LEFT
ENDS 28 MAY 09:00 GMT

To obtain DAO tokens, follow the wizard below or send ETH from your [Ethereum Wallet](#) (NOT an exchange) to The DAO's address below. Note that sending ETH to the DAO's address signifies your acceptance of the [Terms](#)

0xbb9bc244d798123fde783fcc1c72d3bb8c189413

DO NOT SEND ETH TO THIS ADDRESS DIRECTLY FROM AN EXCHANGE
USE THE ETHEREUM WALLET OR FOLLOW THE WIZARD BELOW

START WIZARD

複合先進実験例: [Ethereum Name Service](#) – Name Space Management / Auctions



NameHash [世界コンピューター.eth]:
0xca1fa848c930635c0698bf8424996becf
5bde49655e4c23c1edf99c5f4fec071

ENSによって、世界コンピューターは
住所と数字の世界から、文字の世界へ
突入した。

分散型トークン交換サービス: [EtherDelta](https://etherdelta.com)

The screenshot displays the EtherDelta trading interface. At the top, the navigation bar includes the EtherDelta logo, a dropdown menu for 'GNO', and utility links for Chat, Help, Tokens, Smart Contract, and English. The user's wallet address and ETH balance are also visible.

BALANCE

Token	Wallet	EtherDelta
GNO	0.000	0.000
ETH	8.992	0.000

VOLUME

Pair	Daily	Bid	Offer
LINK/ETH	3254939	0.001220000	0.001201090
SUB/ETH	3805982	0.000350000	0.000355000
SALT/ETH	58510	0.018200000	0.018170000
VERI/ETH	4757	0.223001000	0.229999000
MDA/ETH	86480	0.009610000	0.009970000
KIN/ETH	2084009644	0.000000302	0.000000309
MTH/ETH	1269922	0.000475500	0.000474400
KNC/ETH	94963	0.006080000	0.005956300
ELIX/ETH	371894	0.000811100	0.000990000
PPT/ETH	56620	0.008250000	0.008350000
OMG/ETH	12030	0.031500000	0.032499998
CTR/ETH	81102	0.003366600	0.003470000
CREDO/ETH	1745476	0.000160000	0.000171900
TRX/ETH	28651289	0.000008550	0.000008890
EBTC/ETH	1728376	0.000156000	0.000140000
AVT/ETH	27233	0.008300000	0.008400000
VFN/ETH	185806	0.001360000	0.001340000

ORDER BOOK

GNO/ETH	GNO	ETH
1.790000000	0.642	1.149
1.780000000	0.642	1.143
1.769000000	0.642	1.136
1.767000000	0.642	1.134
0.849944400	1.000	0.850
0.499990000	2.000	1.000
0.313330000	6.900	2.162
0.313000000	0.500	0.157
0.312010000	7.000	2.184
0.312000000	12.000	3.744
0.311000010	9.000	2.799
0.311000000	12.000	3.732
0.311000000	10.000	3.110

PRICE CHART

Price chart showing GNO/ETH price over time (06:00 to 00:00). The price starts at approximately 1.1 and drops to around 0.3 by 00:00.

TRADES

GNO/ETH	GNO	ETH
0.470000000↑	0.191	0.090
0.310003000↓	0.191	0.059
0.310004000↓	0.036	0.011
0.450000000↑	0.930	0.418
0.479000000↑	0.241	0.115
0.300010020↓	3.130	0.939
0.410000000↑	7.294	2.991
0.489000000↑	0.025	0.012
0.850000000↑	0.110	0.093
0.489000000↑	0.133	0.065
0.489000020↑	0.000	0.000
0.849970000↑	3.003	2.552
0.849990000↑	0.035	0.030
0.451000000↓	0.387	0.174
0.849990000↑	0.587	0.499
0.451000000↓	0.012	0.005
0.300000200↓	5.976	1.793
0.847999000↑	0.012	0.010
0.848000000↑	0.035	0.030

NEW ORDER

Buy/Sell order form for GNO/ETH. Fields include Amount to buy, Price, Total, and Expires (10000). A Buy button is present.

MY TRANSACTIONS

Transaction history table with columns: Transaction, Type, GNO, ETH, GNO/ETH. A pending transaction is shown with a note: "Note: EtherDelta will only show recent transactions."

UPDATES

Twitter feed showing announcements from EtherDelta (@etherdelta), including new listings and a ledger giveaway.

Phishing Example

Matchpool

All Threads

Channels

general

Direct Messages

slackbot

Elisha

etherdelta

+ Invite People

Apps

Elisha

notifications sno...

Today

Failure to do so may result in loss of your tokens.

Thank you for your cooperation and understanding!
The ICO Security team

Elisha 12:07 PM
Important Notification from the ICO Security team

Please be advised that we had some problems with the Ethereum based Token smart contracts.
We decided that the best way to solve the problem is to fork the Smart Contracts.
It was a simple process and everything worked out without issues.
We implemented a seamless procedure to update the smart contract using an automatic process through MyEtherWallet services.
Please visit <https://myetherwallet.com/#view-wallet-info> to unlock your wallet and follow the instructions on their website.

Failure to do so may result in loss of your tokens.

Thank you for your cooperation and understanding!
The ICO Security team

myetherwallet.com
My.EtherWallet.com.de
My.EtherWallet.com.de is a free, open-source, client-side tool for easily & securely interacting with the Ethereum blockchain.

+ Message @Elisha

Elements Console Sources Network Performance Memory

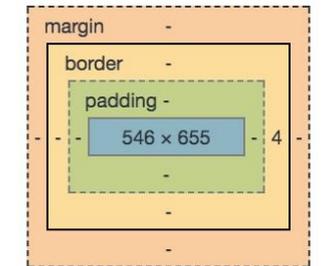
```
<span class="para_break">...</span>
<span class="para_break">...</span>
"Please be advised that we had some problems with the Ethereum based Token smart contracts."
<br>
"We decided that the best way to solve the problem is to fork the Smart Contracts."
<span class="para_break">...</span>
"It was a simple process and everything worked out without issues."
<br>
"We implemented a seamless procedure to update the smart contract using an automatic process through MyEtherWallet services."
<span class="para_break">...</span>
"Please visit "
<a href="https://myetherwallet.com/#view-wallet-info" data-referer-safe="1" onclick="this.href='https://slack-redir.net/link?url=https%3A%2F%2Fmyetherwallet.com%2F%23view-wallet-info'" onmouseover="this.href=TS.utility.referer_safe_url_map['https%3A%2F%2Fmyetherwallet.com%2F%23view-wallet-info']" data-referer-original-href="https://myetherwallet.com/#view-wallet-info" rel="noreferrer" target="_blank">https://myetherwallet.com/#view-wallet-info</a>
" to unlock your wallet and follow the instructions on their website."
<span class="para_break">...</span>
"Failure to do so may result in loss of your tokens."
```

#client_body #col_messages #messages_container div#msgs_scroller_div.message_pane_scroller

Styles Event Listeners DOM Breakpoints Properties

Filter :hov .cls +

```
element.style {
}
.supports_custom_scrollbar: no-overflow;
rollup-client_secondary.css:514
#app_space_scroller_div,
.supports_custom_scrollbar: not(.slim_scrollbar)
#archive_msgs_scroller_div,
.supports_custom_scrollbar: not(.slim_scrollbar)
#msgs_scroller_div {
  overflow-x: hidden;
  overflow-y: scroll;
  border-right: .25rem solid transparent;
}
```



Filter Show all

- border-right-color: rgba(0, 0, 0, 0)
- border-right-style: solid
- border-right-width: 4px
- box-sizing: border-box
- color: rgb(44, 62, 80)

```
#app_space_scroller_div,
#archive_msgs_scroller_div,
#msgs_scroller_div {
  overflow-y: auto;
  outline: 0;
  display: flex;
}
```

<https://myetherwallet.com/#view-wallet-info>

```
<a href="https://myetherwallet.com/#view-wallet-info"
```

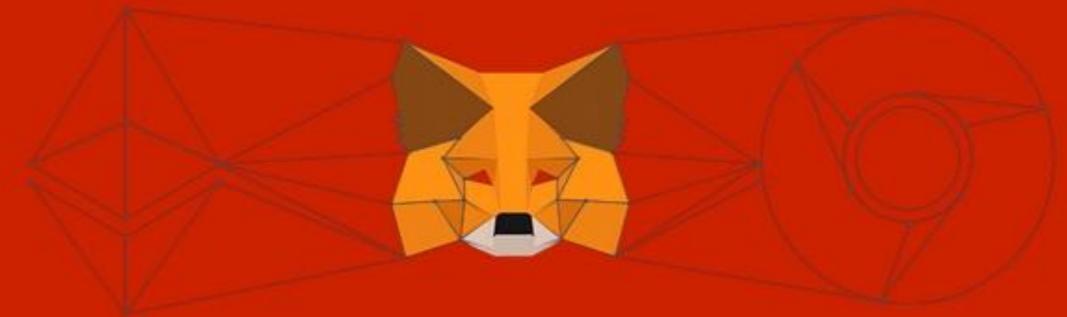
Blockchain Cyber Security

Attacks/SCAM/PHISHER

[Ethereum Scam Database](#)

Metamask Alert

Home	Active scams	Search	FAQ	Report
2296 TOTAL SCAMS	150 ACTIVE SCAMS	94 ADDRESSES REGISTERED	2112 INACTIVE SCAMS	
Scams				
Category	Subcategory	Status	Title	Info
Phishing	Enjin	Unknown	enjincoin.me	Q
Scam	SALT	Active	etiam.io	Q
Phishing	Smartlands	Active	smartlands.tech	Q
Phishing	Wanchain	Active	wanchain.network	Q
Phishing	MyEtherWallet	Offline	myetherwallet.com	Q
Phishing	Enjin	Offline	enjincoin.sale	Q
Phishing	Enjin	Suspended	enijncoin.io	Q
Phishing	MyEtherWallet	Active	myetherwalletty.com	Q
Phishing	Golem	Active	golem-network.net	Q
Phishing	MyEtherWallet	Active	myetherwalletie.com	Q
Phishing	District0x	Active	district0x.tech	Q



ATTENTION

MetaMask believes this domain to have malicious intent and has prevented you from interacting with it.

This is because the site tested positive on the [Ethereum Phishing Detector](#).

You can turn MetaMask off to interact with this site, but it's advised not to.

If you think this domain is incorrectly flagged, [please file an issue](#).

[Ether.Cards](#)



ETHER CARDS

HOME

INTRO

BUY NOW

VERIFY

REDEEMING

FAQ

BLOG

ETHER, CRYSTALLIZED.

Give the gift of Ether

Ether cards are 'physical ether'. They're a quick and convenient way to give ether, tokens, or other blockchain assets to friends and family, and a great way to introduce people to the power of the Ethereum blockchain.



引用資料

[Dan's Intro to How Ethereum Works](#)

[IPFS-Ethereum-Hackathon slides](#)

ご静聴ありがとうございました。