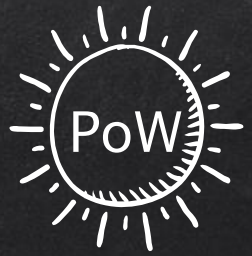


Consensus Algorithms

搞懂 共识算法

你好！我是讲师虞双齐

Nerthus
CTO

登链学院
外聘讲师

MOCHAIN
磨链区块链技术社区
共建者

史前文明

今日的文明，始于昨日的奉献

生而为人

自由

平等

隐私

故事遍地

敌人

强权

垄断

监听

强权无公理

美元强权-经济危机

- 委内瑞拉对抗美国制裁
- 阿根廷法币贬值70%

政府强权-民为鱼肉

- 土改，杀地主
- 别让有钱人跑了-外汇管制

大国强权

- 科索沃危机
- 伊拉克战争
- 利比亚战争
- 叙利亚空袭

~~强权即是公理~~

垄断无公平

政府垄断

- 独家法币发行
- 行业牌照
- 土地
- 信息监管

寡头垄断

- 的士-车份子钱
- 电信-跨省业务

国家垄断

- 稀有资源
- 石油资源

监听无处可逃

棱镜事件

互联网审查

五眼行动

智能广告推荐

苹果iCloud自动上传通话记录

QQ音乐等18款APP疑似存在过度收集“短信”“通讯录”“位置”“录音”等用户敏感信息

监听无处可逃

电子时代

序号	应用名称	版本	所涉问题
1	QQ音乐	v8.9.1.4	过度申请短信功能
2	酷我音乐	v9.0.7.2	过度申请短信功能
3	网易新闻	v 48.1	过度申请录音功能
4	书旗小说	v10.7.4.72	过度申请定位功能
5	携程旅行	v8.0.1	过度申请通信录功能
6	同程旅游	v9.0.7	过度申请短信功能
7	快手	v5.11.1.7527	过度申请短信功能
8	手机天猫	v7.9.0	过度申请短信功能
9	虎牙直播	v6.8.2	过度申请短信功能
10	花椒直播	v6.6.5.1017	过度申请通讯录功能
11	熊猫直播	v4.0.40.8058	过度申请短信功能
12	网易有道词典	v7.7.3	过度申请定位功能
13	有道翻译官	v3.7.6	过度申请定位功能
14	万能看 （百度手机助手）	v9.5.3	未经用户同意收集使用用户个人信息

破局者

江湖侠客

自由主义者

无政府主义者

破局者-密码朋克

互联网诞生的技术既是自由的威胁，又是自由的机遇：
它有望开拓世界，也有可能令国家侵入私人生活。

1993密码朋克宣言

电子时代，隐私是开放的社会不可或缺……
如果我们期望有隐私，那我们必须亲自捍卫。
我们用密码学，匿名邮件转发系统，数字签名以及电子货币保障我们的隐私。

密码朋克-超级贡献

Hash cash

WWW

P2P

RSA

B-Money

电子货币要解决的问题

去中心化

隐匿

安全

如何在一个去中心化环境中，达成共识，进行安全又隐私的交易？

共识算法

共识：在分布式网络中如何达成一致

算法：任何时候都能有相同的计算结果

生命会自己找到出路

黎明

比特币-破晓的晨光

比特币

2008年10月31日

中本聪写到：

我一直在研究一种全新的电子现金系统，它完全是点对点的，没有可信赖的第三方。

Cryptography Mailing List

Bitcoin P2P e-cash paper

2008-10-31 18:10:00 UTC - Original Email - View in Thread

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the
network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System
```

PoW- Proof of Work

是一个数学公式

$$Y = SHA256(X, a)$$

简单　干净

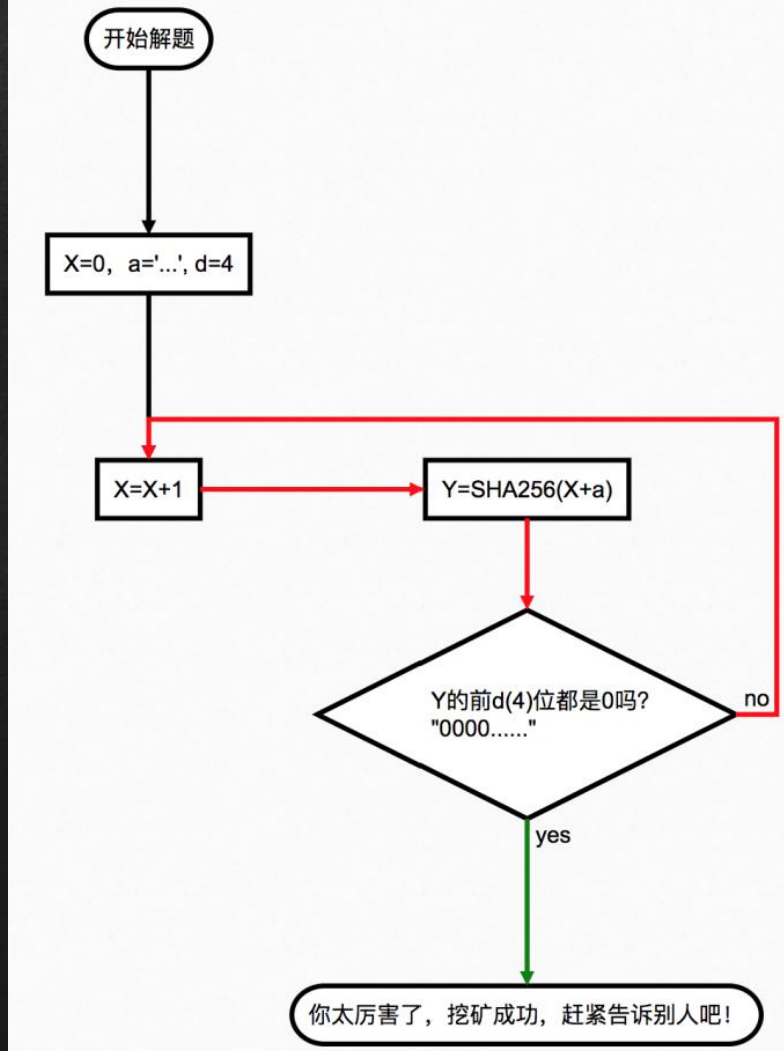
PoW-Sha256

Hello	185f8db32271fe2[illegible]61a6fc938b2e26430 6ec304eda518007d1764826381969
hello	2cf24dba5fb0a30e26e83b2ac5b9e29e1b 161e5c1fa7425e73043362938b9824
hello!	ce06092fb948d9ffac7d1a376e404b26b75 75bcc11ee05a4615fef4fec3a308b

PoW-求解

$$Y = SHA256(X, a)$$

已知 X的值,Y的前D位数都是0，
求数字N。



PoW- 栗子

Y=SHA256(‘hello’,N)

N	Y
0	5a936ee19a0cf3c70d8cb0006111b7a52f45ec01703e0af8cdc8c6d81ac5850c
1	91e9240f415223982edc345532630710e94a7f52cd5f48f5ee1afc555078f0ab
2	87298cc2f31fba73181ea2a9e6ef10dce21ed95e98bdac9c4e1504ea16f486e4
3	47ea70cf08872bdb4afad3432b01d963ac7d165f6b575cd72ef47498f4459a90
4	e361a57a7406adee653f1dcff660d84f0ca302907747af2a387f67821acfce33
…	…
60067	**0000**e49eab06aa7a6b3aef7708991b91a7e01451fd67f520b832b89b18f4e7de

PoW- 解题特性

一题多解

只能穷举

校验简单

PoW- 解题关键

1. 要求Y值得零的数目

难度值

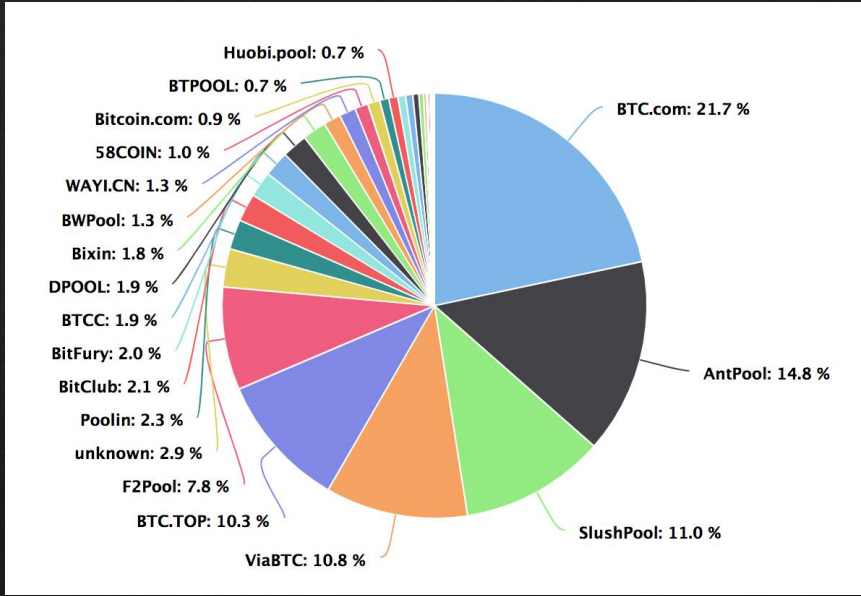
2. 一次SHA256的执行速度

算力

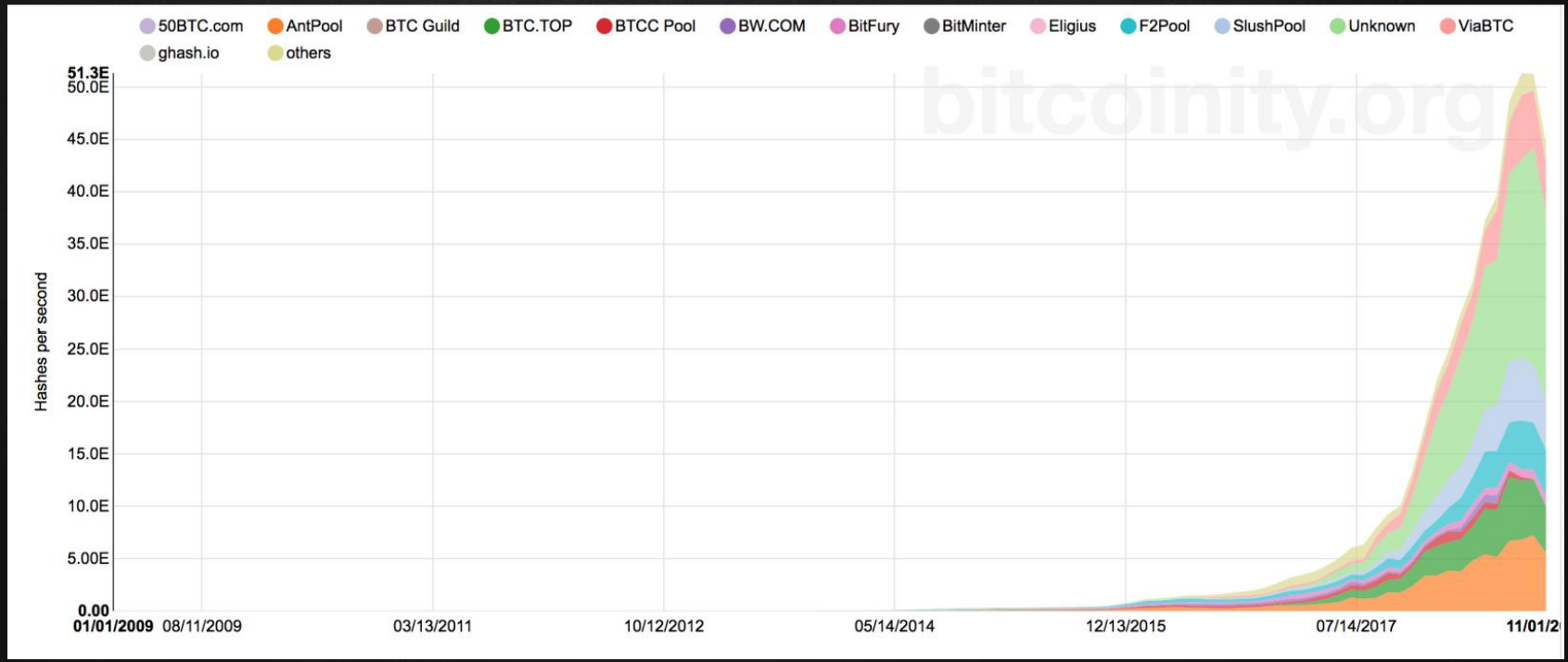
PoW-淘金法则

解题速度快可候选，但最终只有一个人中奖

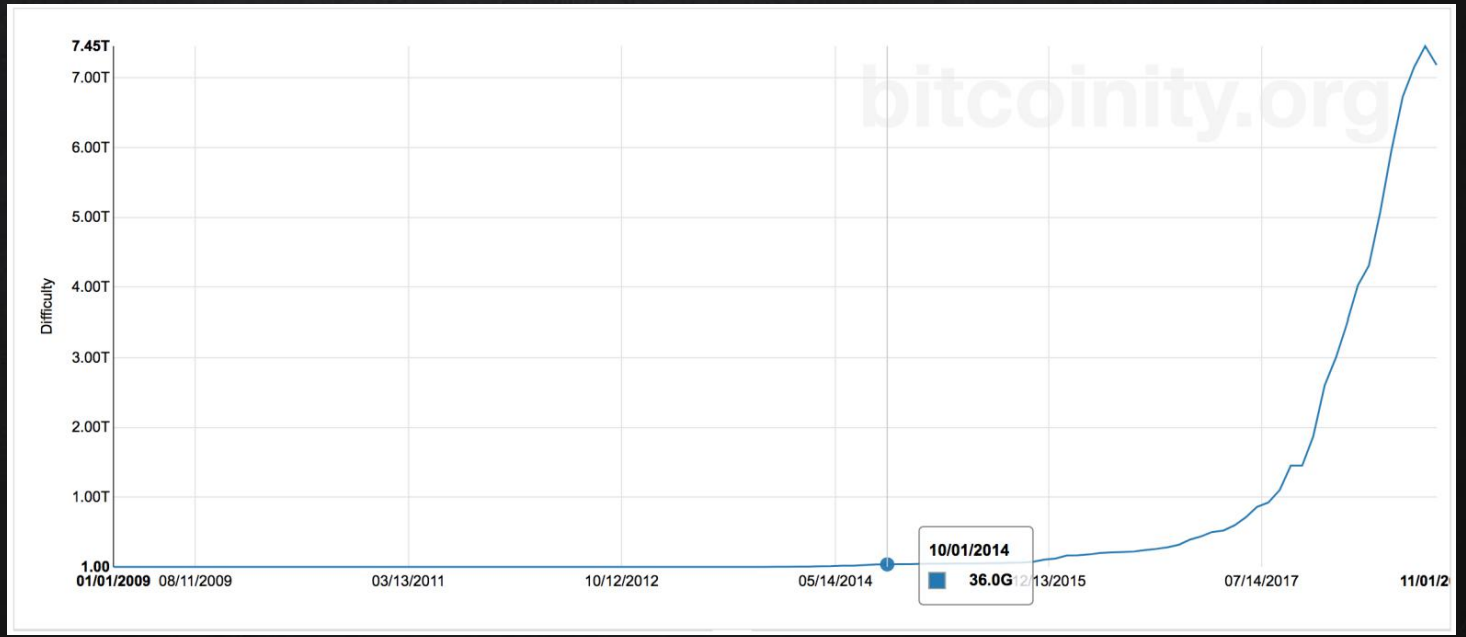
PoW-矿池-其利断金


Huobi.pool: 0.7 %
BTPOOL: 0.7 %
Bitcoin.com: 0.9 %
58COIN: 1.0 %
WAYI.CN: 1.3 %
BWPool: 1.3 %
Bixin: 1.8 %
DPOOL: 1.9 %
BTCC: 1.9 %
BitFury: 2.0 %
BitClub: 2.1 %
Poolin: 2.3 %
unknown: 2.9 %
F2Pool: 7.8 %
BTC.TOP: 10.3 %
ViaBTC: 10.8 %
SlushPool: 11.0 %
AntPool: 14.8 %
BTC.com: 21.7 %

PoW-遇强则强


50BTC.com
AntPool
BTC Guild
BTC.TOP
BTCC Pool
BW.COM
BitFury
BitMinter
Eligius
F2Pool
SlushPool
Unknown
ViaBTC
ghash.io
others
bitcoinity.org
Hashes per second
51.3E
50.0E
45.0E
40.0E
35.0E
30.0E
25.0E
20.0E
15.0E
10.0E
5.00E
0.00
01/01/2009
08/11/2009
03/13/2011
10/12/2012
05/14/2014
12/13/2015
07/14/2017
11/01/2

PoW-遇强则强


7.45T
7.00T
6.00T
5.00T
4.00T
3.00T
2.00T
1.00T
1.00
Difficulty
01/01/2009
08/11/2009
03/13/2011
10/12/2012
05/14/2014
07/14/2017
11/01/2
10/01/2014
36.0G
bitcoinity.org

PoW- 缺点

效率低

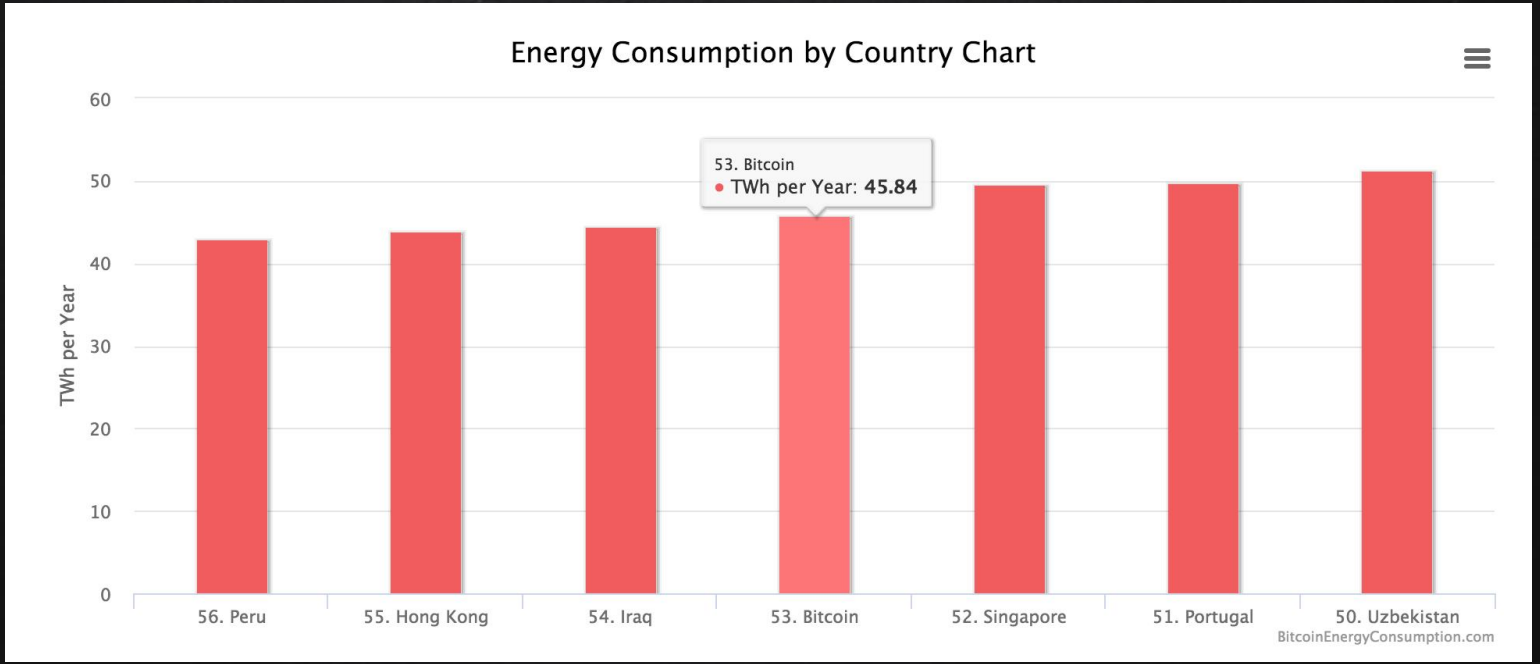
耗能高

被中心化

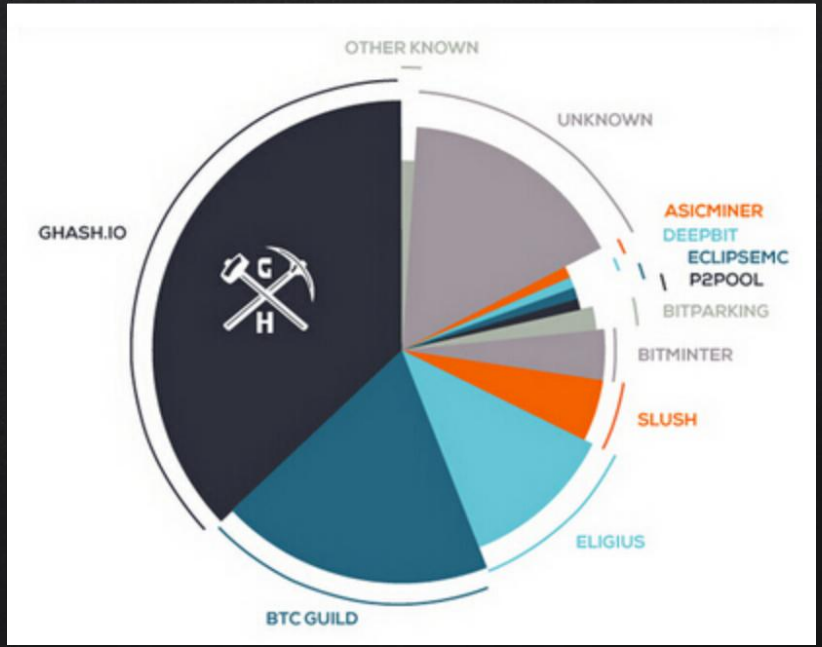
PoW-效率低

TPS：7笔/秒

PoW-高耗能


Energy Consumption by Country Chart
60
50
40
30
20
10
0
TWh per Year
53. Bitcoin
TWh per Year: 45.84
56. Peru
55. Hong Kong
54. Iraq
53. Bitcoin
52. Singapore
51. Portugal
50. Uzbekistan
BitcoinEnergyConsumption.com

PoW-超级算力

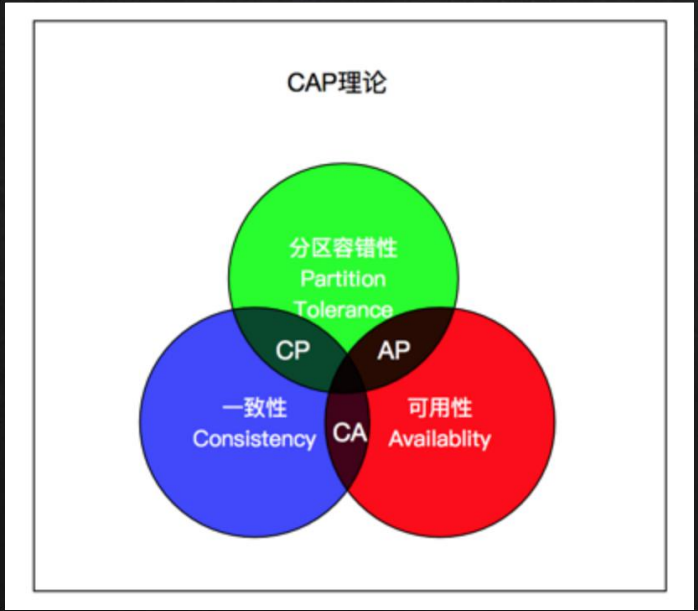


51%攻击

PoW-升级困难

扩容之争

PoW-高安全性



牺牲可用性

保证一致性

百家争鸣

哪里有痛点，哪里就有革新

PoS

比特币之后

比特币之后2012

Proof of Stake

PoS- Proof of Stake

权益证明

$$Y = HASH(X, N)$$

但挖矿难度因人而异

持币越多则挖矿越容易

PoS

问题

第一个币

垄断

51%攻击

无利害关系

POS- Delegated Proof-of-Stake

点点币

黑币

以太坊2.0

PoS

DPOS- Delegated Proof-of-Stake

变体，委托其他节点出块

EOS

比特股

阿希

Leased Proof-Of-Stake (LPoS)

租赁权益

Practical Byzantine Fault Tolerance (PBFT)

实用的拜占庭容错

一伙出块人实时达成共识，
区块立即生效。

PBFT

PBFT-优缺点

立即
确认

沟通
困难

女巫
攻击

PBFT

Simplified Byzantine Fault Tolerance (SBFT)

简单的拜占庭容错

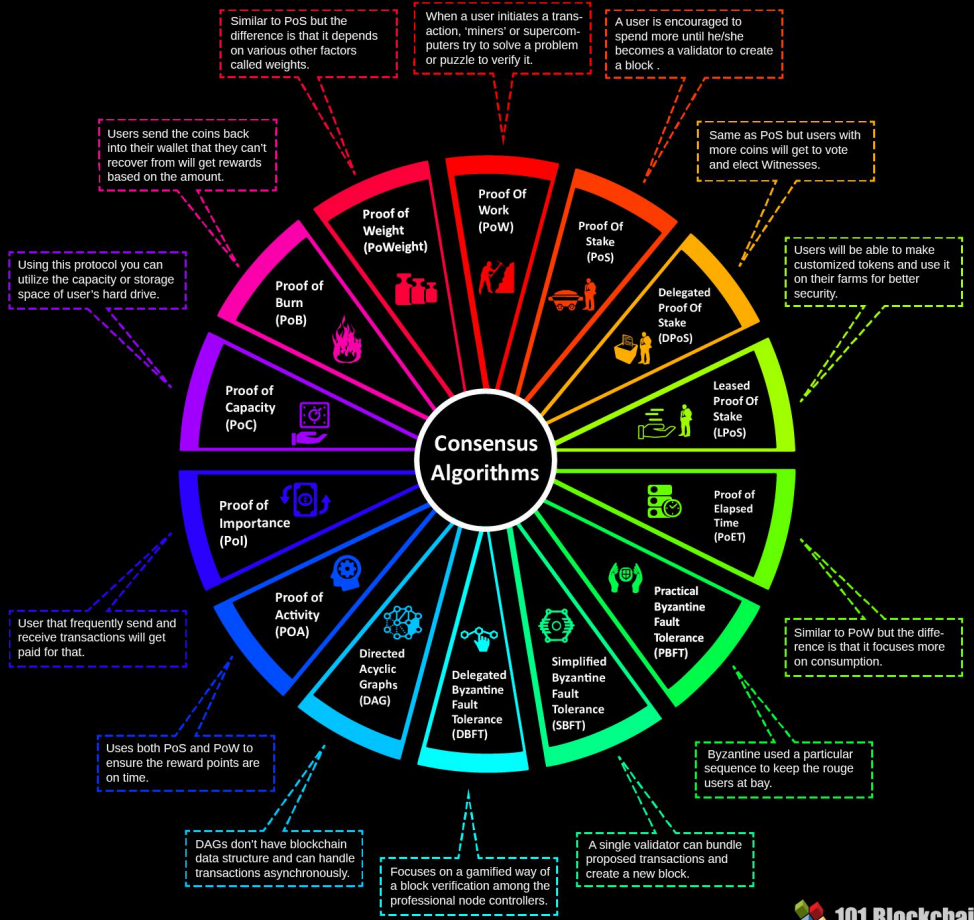
创建包含交易的区块的交易

PoS

各种改良

3680个货币
已在运行中

Different Types of Consensus Algorithms



thanks!

Any questions?