DEL区块链技术分享

开启区块链4.0时代

DEL创始人--刘星

- 镭达技术团队的程序员。
- 虚拟币玩家， 拥有一个小规模矿场，偶尔搬砖， 对冲套利。

镭达技术团队从2014年开始从事区块链技术开发，项目包括交易平台，数字货币钱包，公链，区块链社区，区块链相关媒体等领域开发。

区块链4.0发展历程

区块链 v1.0

比特币为代表的数字货币，其场景包括支付、流通等货币职能；虽然存在效率底下、POW耗能、政府监管等问题，但其仍然是区块链技术最成功的应用。

区块链 v2.0

以太坊为代表的数字货币与智能合约相结合，对金融领域更广泛的场景和流程进行优化的应用。但仍然存在性能问题以及挖矿耗能等问题。

区块链 v3.0

EOS为代表的高速公链，性能和能耗问题也得到了解决，但智能合约安全问题频现， 区块大小问题依然限制着其应用范围。

区块链 v4.0

DEL为代表的最终服务于实体企业的公链，用容器化技术隔离智能合约的运行环境， 分片技术解决区块大小无限制增长的问题。

区块链3.0存在的问题

智能合约安全漏洞频现

智能合约虚拟机和节点进程共享系统资源，具有严重的安全隐患。

区块大小制约行业发展。

以太坊交易占用117字节， 以此计算支持百万TPS的区块链， 每秒区块大小增长117M。以此速度增长的区块大小， 是目前计算机无法承载的。

DEL区块链简介

DEL是将会被大规模实体应用的最终技术选择方案

DEL的目标是实现一个安全的高速公有链，各领域的合作伙伴可以快速在复式账本的基础上构建上层应用，帮助企业各种业务架构在区块链平台上，让企业、客户、机构在多样化的应用环境中受益。

DEL链的主要特征：

01 链上容器

符合标准的程序可以不经过任何修改的运行于区块链之上。

02 分片技术

彻底解决区块容量问题，随着节点数量的增加， 区块数据将逐步分摊到多个节点之上， 从而降低单一节点的负载。

DEL链技术架构——智能合约

从系统底层， 分离执行智能合约所需要的系统资源， 从理论上杜绝执行合约可能产生的安全隐患。

```
int clone(int (*fn)(void *), void *child_stack, int flags, void *arg);
```

Mount	CLONE_NEWNS	Mount points (since Linux 2.4.19)
User	CLONE_NEWUSER	ser and group IDs (started in Linux 2.6.23 and completed in Linux 3.8)
Cgroup	CLONE_NEWCGROUP	Cgroup root directory (since Linux 4.6)
IPC	CLONE_NEWIPC	System V IPC, POSIX message queues (since Linux 2.6.19)
Network	CLONE_NEWNET	Network devices, stacks, ports, etc. (since Linux 2.6.24)
PID	CLONE_NEWPID	Process IDs (since Linux 2.6.24)
UTS	CLONE_NEWUTS	Hostname and NIS domain name (since Linux 2.6.19)

DEL链技术架构——智能合约

cgroup限制进程的内存, CPU等系统资源。

/sys/fs/cgroup/memory/
mkdir del
echo 64k > memory.limit_in_bytes
echo 17985 > tasks

```
1: del.c
 1 int main()
 2 {
 3     while(1)
 4     {
 5         malloc(1024 * 1024 * 32);
 6         sleep(1);
 7     }
 8     return 0;
 9 }
10
```

```
[root@izbp18qasm44xlhnf5l9nbz randylau]# ./del
Killed
```

DEL链技术架构——智能合约

DEL将使用何种语言作为智能合约？

任何语言，任何程序

均可作为DEL的智能合约。

DEL链技术架构——智能合约

只要对于相同的输入具有相同的输出， 那么就可以作为智能合约。

优点：⇨ 极高的可移植性， 现有程序不需要任何修改， 就可以运行于DEL之上。

DEL链技术架构——智能合约

追踪程序执行过程，判断否能作为智能合约。

一个读取外部数据的非法程序。strace追踪其运行过程发现它不可以作为智能合约。

1: del.c

```c
#include "stdio.h"

int main()
{
    char c;
    FILE *fin;
    fin = fopen("del.c", "r");
    c = fgetc(fin);
    putchar(c);
    return 0;
}

```

```
read(3, "#include \"stdio.h\"\n\nint main()\n{"..., 4096) = 126
fstat(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) =
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS
write(1, "#", 1#)                                = 1
exit_group(0)                                    = ?
+++ exited with 0 +++
```

DEL链技术架构——智能合约

如何计算Gas(合约消耗)?

系统内存的占用+合约的CPU占用+区块数据的占用=Gas(合约消耗)

Any Question?

DEL链技术架构——分片

分片技术是一项非常成熟的分布式存储技术， 它工作将整体数据平均分摊在多个节点之上， 从而降低单个节点设备的数据存储量。广泛的被云存储厂商使用， 用来降低冷数据的存储成本。

区块链数据的特点：

区块链由于其只可追加， 不可修改的特性， 使得在分片的时候不需要考虑数据的平均分配问题， 所以更加适合使用分片技术来优化存储。

DEL链技术架构——分片

首先分析一下区块链钱包的常用功能

查询余额？

同步区块时顺序遍历交易， 计算每个账号的余额。

转账？

查询余额判断是否可以转账， 私钥签名， 发送交易。

结论：块数据只在同步的时候会被访问到。

DEL链技术架构——分片

如何进行数据分片？

一个简单的实现方法是使用取模运算来进行Block存储的划分。单数号节点丢掉模4为0的块， 双数号节点丢弃模4为3的块。

DEL链技术架构——分片

这样存储安全吗？

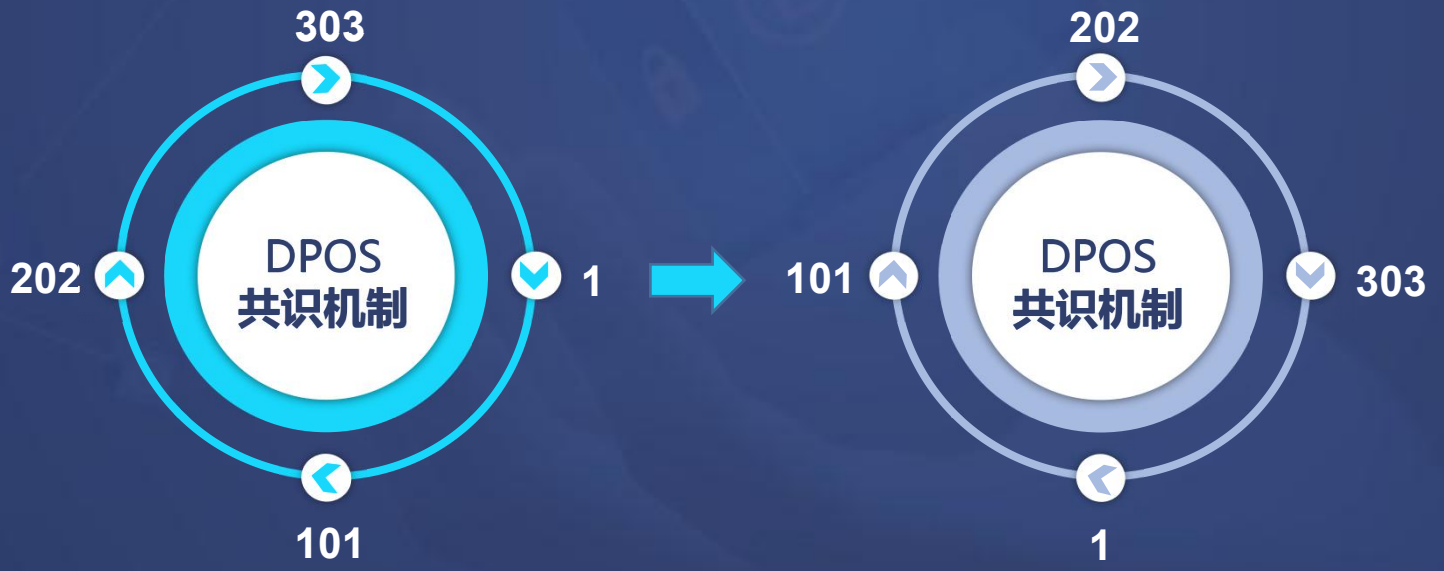
当用户数量较少的时候， 每个节点都会保存完整区块数据来保证数据安全。
当用户的数量逐渐提升， 已经并不需要这么高冗余度的时候， 节点会逐渐丢弃一些不需要保存的区块数据。

Any Question?

DEL链技术架构——共识机制

采用DPOS共识机制， 约5秒出一个块， 由303个生产者轮流记账。每303层统计投票状况， 选出下一轮的303个生产者节点。

优点：更加民主



DEL链技术架构——共识机制

每一个区块设置一个重量值：投票数量/生产时间

合法的客户端会追踪总重量最重的链，从而保证投票数量越多，生产时间越短的链会被最终认可。

攻击区块链所需要的成本：

1、连续控制若干个生产者， 来保证出块速度。

2、持币数量超过主链， 来保证投票的数量。

DEL链技术架构——共识机制

激励制度每一个块具有64个币的固定奖励和158.0246914的额外奖励, 奖励随着高度增加而减少。

1、记账节点获得固定的块奖励64个币

2、得票前303名的节点， 每一个会平分158.0246914 * 40%的额外奖励,。

3、得票前23名的超级节点， 每一个块会平分158.0246914 * 10%的奖励。

4、投票人按照排名的比值， 分配158.0246914 * 50%的奖励。

DEL链技术架构——共识机制

每一个区块设置一个重量值：投票数量/生产时间

合法的客户端会追踪总重量最重的链，从而保证投票数量越多，生产时间越短的链会被最终认可。

攻击区块链所需要的成本：

1、连续控制若干个生产者， 来保证出块时间。

2、持币数量超过主链， 来保证投票的数量。

DEL链技术架构——共识机制

激励制度每一个块具有64个币的固定奖励和158.0246914的额外奖励, 奖励随着高度增加而减少。

1、记账节点获得固定的块奖励64个币

2、得票前303名的节点， 每一个会平分158.0246914 * 40%的额外奖励,。

3、得票前23名的超级节点， 每一个块会平分158.0246914 * 10%的奖励。

4、投票人按照排名的比值， 分配158.0246914 * 50%的奖励。

DEL链技术架构——共识机制

如何计算我的挖矿收益？

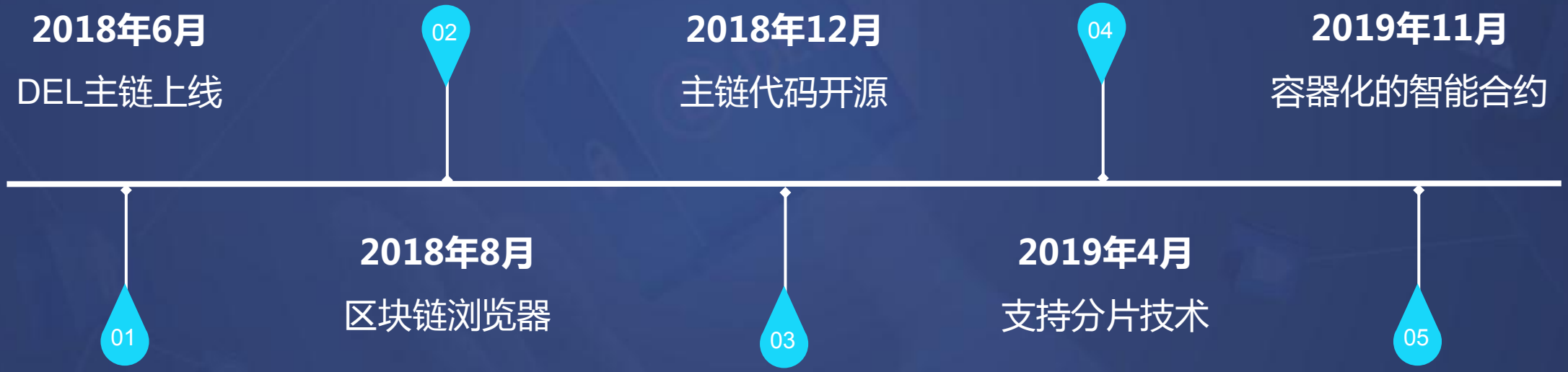
1、一个普通记账节点每303个块获得：64+158.0246914 *0.4=127.20987656

2、一个超级节点每303个块获得：64+158.0246914*0.4 + 158.0246914 *0.1/23*303=335.39023088261

3、四个人分别投票：7, 8, 8, 9个币， 那么这四个人的升序名次为：1, 2, 2, 4。依次获得：1/9 * 158.0246914 * 0.5, 2/9* 158.0246914 * 0.5, 2/9* 158.0246914 * 0.5,4/9* 158.0246914 * 0.5

Any Question?

DEL 发展·未来


2018年6月
DEL主链上线
02
2018年12月
主链代码开源
04
2019年11月
容器化的智能合约
2018年8月
区块链浏览器
01
03
2019年4月
支持分片技术
05

DEL官方网站

del.io

DEL节点——区块浏览器

项目主页：del.io

区块浏览器

- 查询交易是否到账
- 浏览历史区块信息
- 分析区块数据
- ……

区块高度	区块大小	投票数量	时间戳
54876	72012	83	2018-06-08 15:06:40
54875	70838	84	2018-06-08 15:06:26
54874	73385	80	2018-06-08 15:06:14
54873	73326	82	2018-06-08 15:06:02
54872	72094	86	2018-06-08 15:05:50
54871	64082	79	2018-06-08 15:05:38
54870	73274	78	2018-06-08 15:05:25
54869	73527	92	2018-06-08 15:05:13
54868	68120	111	2018-06-08 15:05:01

DEL节点——在线钱包

项目主页：del.io

在线钱包:

- 查看余额
- 转账
- 发简讯
- ……

DEL节点——在线钱包

项目主页：del.io

在线钱包:

- 查看余额
- 转账
- 发简讯
- ……

DEL节点——在线钱包

项目主页：del.io

在线钱包:

- 查看余额
- 转账
- 发简讯
- ……

DEL节点——在线钱包

项目主页：del.io

在线钱包:

- 查看余额
- 转账
- 发简讯
- ……

DEL节点——开源代码

项目主页：del.io

DEL会逐步开放全部源代码

DEL节点——开源代码

项目主页：del.io

实现的功能:

- 查看余额
- 转账
- 简讯
- 挖矿

DELWallet (v0.9.0-unstable)

randylau released this on 26 Apr · 1 commit to master since this release

Assets

DELWallet.v0.9.0-unstable-windows_amd64.exe 76.3 MB

Source code (zip)

Source code (tar.gz)

全功能钱包——测试网络版

全功能钱包提供了最全面的主链功能， 同步完整的区块链数据，进行高级别的安全检测，是超级节点的最佳选择。
此版本运行于测试网络之上。

正式网络， 在线钱包，区块链浏览器， 矿池等产品将于近期发布， 请密切关注DEL社区的门户网站 https://www.del.io

Please see below the blockchain 4.0 changelog:

- 合约执行容器化
- 分片技术
- 高速共识机制

DEL节点——开源代码

项目主页：del.io

Any Question?


PLATFORM
Research
FINANCE
COMMUNICATION
NETWORK
WEBSITE
DATABASE
COLLABORATION
APPLICATION
MONITORING
RUNTIME
SEARCH
IDENTITY
OBJECT STORAGE
CONTENT
BLOG STORAGE

THANKS

谢 谢 观 看