

The Blockchain Technology & Application Summit was successfully held in Beijing on March 30–31, 2018, where focus was on topics such as core blockchain technology, development trend, industry application, and investment assets storage and trading. Roy Li, the founder of Ruff, was invited to attend the summit and delivered a speech entitled the “Application Practice of Blockchain Technology at the Enterprise Level”. The following is the record of his speech:

****Speech Record:****

At first, I’d like to express my gratitude to the organizers, huoxing24.com and CSDN, for giving me such an opportunity to deliver my speech. We are not sponsors. I’m a company invested by Jiang Tao and Wang Feng, who provide angel investment for me. So, I make it clear to you with this opportunity. We are also the one with the smallest sense of existence among their invested companies. Many people haven’t learnt about it, so it’s also an opportunity for me to display my sense of existence today. It is a technically-oriented forum today, and we are not sponsors, either. I’ll try to talk as little as possible about my company and as much as possible about the entire industry.

My topic today is the application & practice of blockchain technology in enterprises. The market environment has not been so favorable recently, and a great many guys say that, due to the immature infrastructure, blockchain technology is still at its early stage, and it is difficult to implement in a real sense. For this reason, some on the market hold that, the Tokens before us may turn into an air currency, which, in my view, can not be too absolute.

There are indeed some technologies in the market that are not very mature, with poor adaptability to be realistically implemented. However, there are some technologies that are easy to be applied at the enterprise level. During such a process, we should analyze from a relatively rational perspective, and should not feel that blockchain is quite extraordinary just through patting the head, or that blockchain is far from realistic implementation.

Today, I’ll talk about the application of blockchain technology at the enterprise level. We ourselves are also engaged in enterprise-level applications, during which a lot of explorations have been made, with tons of analyses of technical practice as well; we’ve also observed how open-source technologies are really like on the external market and whether they can meet relatively high TPS. Of course, TPS is not an indicator good enough. It depends on your mode of selling the currency and how you address the problems related to blockchain.

I wonder how many of you here really understand blockchain, and how many of you know the real meaning of the three words. After learning about the history of the three words, you might make brag of your knowledge with it someday.

n ****Origin of the three words: Ropsten/Kovan/Rinkeby****

The first word is Ropsten. In fact, these three words are all the names of the Ethereum test network. These three are all optional Ethereum test networks. There are two clients on Ethereum, and Geth is the first client. Since its performance is not so strong, it is very slow to synchronize, and later, an Ethereum full-node software was developed, written in the Last language. Later, as the two client versions have some compatibility problems with each other, for allowing for compatibility in the Ethereum test network, significant modifications were made to the test network, which finally resulted in the generation of Ropsten.

The next two are also test networks. Since Ethereum’s material mechanism is POW, and this W requires costs, for the miner needs cost, the earliest Ethereum’s test network was of little value due to the very low coin price. In addition, it was impossible to acquire a lot of computing power to support the Ethereum’s test network, so it was vulnerable to malicious attacks. Since the computing power of entire network was not big enough, tons of attacks were targeted at this Ropsten. For one block, 10 million is the maximum gas, and a gas of 4,750,000 was made into a gas of over 9,000,000,000 for one block by attacks. It became impossible to proceed any more.

In Ropsten, it is, at first, impossible to apply POW when it is so low. So, they used a POA, and this concept was finally turned into Kovan, a POA-based network. For example, if you’re a big name in the community of a well-known organization, I trust you and make you into that. So, it’s quite like DPOS, but it’s not selected through voting; instead, it is through recognition in the community, and you guys are now big nodes. So, that’s what he did. The foundation also favored that, and decided not to follow the original mode but produced a test network in the POA mode, called Rinkeby; hence the three words here.

We can learn from this story that, as for any public blockchain at its early time of being capable of launching, you should pay attention to one thing: it is highly challenging to conduct very, very high decentralization at the early start. POW intends to solve decentralization, and its computing power is quite dispersed. However, it is relatively centralized at the early stage. The so-called “decentralization” does not mean no center; there might be several concentrated centers, more appropriate for the launch of network.

Similarly, you might have heard about LTA. It has a centralized coordinator for such coordination. As for miner building, they adopt this mode. In early enterprise-level applications, if you’d like to create a public blockchain, you must consider such issues at the early start. So, you might resort to POA for fixing. Here, I’ve told you this little story, so that you can brag to your audience and, for those dedicated to public blockchain development, consider how to start when you have a strong computing power for support at the early stage.

n ****Which consensus mechanism should be for public blockchain?****

Our next topic is, for a company, if you want to conduct a public blockchain, the first issue you face now is which consensus mechanism you shall choose. For example, BFT is an option, with high fault tolerance, but it has a problem, i.e. scalability. Its performance is inversely proportional to the square of the node; that means, if your nodes are ten times more, your performance will drop by 100 times. Based on the data of Hyperledger, including analyses by many people, it would be highly difficult to apply BFT when your nodes reach 100.

By contrast, its advantage also lies here: if 50% of your nodes are crocodile nodes, there would be no big impact. Personally, I prefer DPOS. You can use it at the early stage of public blockchain and rely on DPOS for transition. A double-layer POS works the same, but it has a greater scalability, which, for bitcoin, is not a big issue indeed. I myself specialize in security, and the bottleneck of security never lies in that layer. It has more problems indeed. It has been proved that, a SPV node can still guarantee high security even if it does not store the data of an entire block, since you can finally discover a POW mechanism with long- and short-chain. But, many such problems exist in DPOS. If you’re a light node in DPOS, not storing all the data, problems many occur.

Besides, the voting mechanism of DPOS is designed to be a vulnerable point, which should also be taken into consideration. POW is certainly the best, but, as I mentioned before, when the computing power of entire network is low, or the value of your coin is not high, some problems may occur in POW.

Another point is about our CAPA. A lot of infrastructure now aims to address some issues in blockchain, including Sharding technology, which is not quite mature up to now but is still an extensively recognized direction. There’s no need to divide the entire network into many blocks to conduct what I desire to do in parallel. This Cluster includes contract execution. For example, US has done something, and I feel US quite interesting. Due to the reliance of contract during its execution, I might suppose it is highly difficult to execute the contract in parallel. The better you cleanse my data, the higher my parallel execution efficiency will be, and the higher the award I will give you. This task fulfilled by US is quite interesting, which is what we all desire to solve in Cluster. US hands over the issue to data packers; you pack the data in any way you like, and I just want to solve my problem. I admire companies dealing with this.

At last, in Optimization, more efforts are on the optimization of node ends themselves. The ledge nodes of “gas” itself are limited, and the quantity of “gas” you can reach within the required block generation period is limited. Basically, it’s how to improve the magnitude. Ethereum is not in the TSO mode; it uses over 400G for storage, and it is a problem to read and write this 400G. Some one improves the ability of data reading and writing, and it is now conducted on the market. It’s quite interesting. As these technologies slowly grow mature, blockchain expansion technologies have grown much stronger. And your hard disk can have the performance of instantaneous reading and writing, and, theoretically, “gas” can be significantly improved, which is something we should consider during optimization.

n ****Iteration difficulty of blockchain technology is much greater than that of traditional technology****

Why is the iteration of blockchain technology more difficult than traditional technologies? That’s because the problems the distributed system of blockchain faces are different from those faced by centralized systems, possibly quite distinct. In US, for example, one paragraph of the whitepaper reads: In atomic transactions between mega and mega, atomicity is indivisible, and the atomicity between multiple mega-s can only be executed in parallel, not in series. When you conduct optimization, you’ll see that, 80–90% of these conflicts are avoidable, and only those relationships with unclear sequences, like at exchanges, have 1–2% probability, which you can not handle. However, the overwhelming majority of them can be handled. Next is storage. A company has said that, he has already added IPFS. There are big problems in IPFS. The performance can not be guaranteed now. As to this point, I’ve asked many P2P old pros and experts, who expressed that, it is currently unsolvable in terms of unstructured data storage. It is highly difficult to be really IPFS.

Personally, I am quite optimistic about the future of IPFS, but, currently, the problems of its practical implementation are still unsolvable. The last point is “contract”, immediate execution of contract. If it’s easy for you to apply the UTSO mode, just execute it. I chatted with Shuai Chu a couple of days ago about this, and he said: the contract is quite complex; conflicts among contracts are not necessarily conflicts among mega-s, but most likely to be conflicts of others.

At present, the contract is still at an early stage. The future development direction should be, for us, how to more efficiently adjust the sequence of contract execution, and adjust their sequence and more efficiently execute contracts by finding the correlation among contracts.

n ****Blockchain technology is currently at the stage of transition from theory to practice****

Finally, I believe that, at present, the blockchain is at the stage of transition from theory to practice. In 2019, when we talk about blockchain again, please do not mention it to me if you have no practical technologies. I think you can do it in 2017. In 2018, in particular, it has been quite difficult to do that. All of us feel that too many people brag about their own things, including some things that can not be acquired within ten years. There are problems of practical implementations for all of them.

The blockchains that seem quite successful now may not be the best in performance, but one thing is certain: it has dramatically reduced the developer’s cost of developing APP. Why was ICO so hot last year? Why were so many guys engaged in Token last year? So many people did this every year before, and now, you can directly release your own Token when you make your own Token based on ICO. For someone who has one year of programming experience, he/she can make it within 3 days after learning a little of JAVA. It is so common that all programmers can do it.

In future, maybe some of you do not know how to develop the blockchain, but you can develop an APP and develop your own distributed application, which will be a big trend in future. The Ruff Company has run for four years. We have been successfully engaged in IoT OS for years in the field of IoT, and we can now, in a more abstracted way, develop some applications of peripheral computing. And, these applications can be combined with blockchain. The updated applications are all standardized and abstracted data, which I’m quite proud of. That’s why many people are optimistic about Ruff when it is launched in a programmers’ community. They hold that, this is where we are close to the physical column.

I’ve been dealing with the public blockchain for a long time, and I feel the same when I’m now dealing with the public blockchain and when I dealt with the OS before. Only when I lowered the threshold of development can more people come in. Only after the threshold is lowered, there are more applications. People who are more creative than me can produce applications beyond our imagination. So, here comes my slogan: “Code Easier, Change Faster”. A public blockchain is not successful until all the people can develop applications in a relaxed and joyful manner. That’s my attitude towards the public blockchain and how can a public blockchain succeed.

Thank you very much for giving me such an opportunity to share with all of you here today. That’s all of my sharing today. Thanks.

****Introduction to the Honorable Guest:****

Roy Li: the founder of Ruff Chain, Ruff CEO, a noted security expert and IoT expert, the founder of the world’s leading IoT OS — ruff.io, and an MSE master student supervisor in Fudan University. He used to be a security consultant to Verisign and Trend Micro, former Chief Technology Officer to Nokia OVI in North America, QCon (Software Development Conference) Outstanding Producer for four years, and GITC (Global Internet Technology Conference) lecturer for three years.

区块链技术与应用峰会于2018年3月30-31日在北京成功举办，聚焦区块链核心技术、发展趋势、行业应用、投资资产存储与交易等议题。Ruff创始人Roy Li受邀出席峰会并发表了题为“区块链技术在企业层面的应用实践”的演讲。以下是他的演讲实录：

****语音记录：****

首先，我要感谢主办方 huxing24.com 和 CSDN 给了我这样一个演讲的机会。我们不是赞助商。我是江涛和汪峰投资的公司，他们为我提供天使投资。因此，我借此机会向您说明。我们也是他们投资的公司中存在感最小的一个。很多人还没有了解，所以今天也是我一个展示存在感的机会。今天它是一个以技术为导向的论坛，我们也不是赞助商。我会尽量少谈论我的公司，尽可能多地谈论整个行业。

我今天的主题是区块链技术在企业中的应用与实践。最近市场环境不太好，很多人说，由于基础设施不成熟，区块链技术还处于起步阶段，很难真正实现。为此，市场上有些人认为，我们面前的Token可能会变成空气币，在我看来，不能太绝对。

市场上确实有一些技术不是很成熟，适应能力差，无法实际落地。但是，有些技术很容易在企业级应用。在这样的过程中，我们应该从一个相对理性的角度来分析，不能光拍脑袋就觉得区块链很了不起，或者说区块链离实际落地还差得很远。

今天，我来谈谈区块链技术在企业层面的应用。我们自己也在做企业级的应用，在这个过程中进行了很多探索，也有大量的技术实践分析；我们还观察了开源技术在外部市场上的真实情况，以及它们是否能够满足相对较高的 TPS。当然，TPS 并不是一个足够好的指标。这取决于您出售货币的方式以及您如何解决与区块链相关的问题。

不知道在座有多少人真正了解区块链，又有多少人知道这三个字的真正含义。在了解了这三个词的历史之后，有一天你可能会用它来吹嘘你的知识。

n****三个词的由来：Ropsten/Kovan/Rinkeby****

第一个词是罗普斯滕。其实这三个字都是以太坊测试网的名字。这三个都是可选的以太坊测试网络。以太坊上有两个客户端，Geth 是第一个客户端。由于性能不是那么强，所以同步很慢，后来开发了一个以太坊全节点软件，用Last语言写的。后来，由于两个客户端版本之间存在一些兼容性问题，为了在以太坊测试网络中兼容，对测试网络进行了重大修改，最终产生了Ropsten。

接下来的两个也是测试网络。由于以太坊的物质机制是POW，而这个W需要成本，对于矿工来说需要成本，以太坊最早的测试网络由于币价非常低，价值不大。此外，以太坊的测试网络无法获得大量的计算能力来支持，因此容易受到恶意攻击。由于整个网络的计算能力不够大，因此针对这个Ropsten进行了大量的攻击。一个区块的gas上限是1000万，475万的gas被攻击变成一个区块的gas超过90亿。再也无法进行下去了。

在 Ropsten 中，当 POW 如此之低时，一开始是不可能应用 POW 的。所以，他们使用了 POA，这个概念最终变成了 Kovan，一个基于 POA 的网络。例如，如果您是某知名组织社区中的大人物，我相信您并让您成为其中的一员。所以，它很像 DPOS，但它不是通过投票选出的；相反，它是通过社区的认可，你们现在是大节点。所以，他就是这么做的。基金会也看好这一点，决定不沿用原有模式，而是制作了一个POA模式的测试网络，叫做Rinkeby；因此这里的三个词。

我们可以从这个故事中了解到，对于任何一个公有链在能够上线的早期，你应该注意一件事：在早期进行非常非常高的去中心化是非常具有挑战性的。POW意在解决去中心化，其算力相当分散。但是，它在早期是相对集中的。所谓“去中心化”，不等于没有中心；可能有几个集中的中心，更适合网络的启动。

同样，您可能听说过 LTA。它有一个中央协调员来进行这种协调。至于矿工建设，他们采用这种模式。在早期的企业级应用中，如果你想创建一个公共区块链，你必须在早期开始考虑这些问题。因此，您可能会求助于 POA 进行修复。在这里，我给大家讲了这个小故事，让大家可以吹嘘一下，对于那些致力于公共区块链开发的人来说，在早期有强大的计算能力支持的情况下，请考虑如何入手。

n****公共区块链应该采用哪种共识机制？****

我们下一个话题是，对于一个公司来说，如果你想做一个公链，你现在面临的第一个问题是你应该选择哪种共识机制。比如BFT是一种选择，容错性很高，但它有一个问题，即可扩展性。它的性能与节点的平方成反比；这意味着，如果您的节点增加十倍，您的性能将下降 100 倍。根据 Hyperledger 的数据，包括很多人的分析，当你的节点达到 100 个时，应用 BFT 将非常困难。

相比之下，它的优势也在这里：如果你50%的节点是鳄鱼节点，影响不大。就个人而言，我更喜欢 DPOS。您可以在公链的早期使用它，并依靠 DPOS 进行过渡。双层 POS 的工作原理相同，但它具有更大的可扩展性，这对于比特币来说确实不是什么大问题。我自己是专攻安全的，安全的瓶颈从来不在那个层。它确实有更多的问题。事实证明，一个SPV节点即使不存储整个区块的数据，仍然可以保证高安全性，因为你最终可以发现长链和短链的POW机制。但是，DPOS 中存在很多这样的问题。如果你是 DPOS 中的轻节点，不存储所有数据，就会出现很多问题。

此外，DPOS 的投票机制被设计成一个脆弱点，也应该考虑到这一点。POW当然是最好的，但是我之前说过，当全网算力低，或者你的币值不高的时候，POW可能会出现一些问题。

另一点是关于我们的 CAPA。现在很多基础设施都是为了解决区块链中的一些问题，包括分片技术，目前还不太成熟，但仍然是一个被广泛认可的方向。无需将整个网络分成许多块来并行执行我想做的事情。该集群包括合约执行。比如美国做了一些事情，我觉得美国很有意思。由于合同在执行过程中的依赖，我可能认为并行执行合同非常困难。你清理我的数据越好，我的并行执行效率就越高，我给你的奖励也越高。美国完成的这个任务很有意思，这也是我们在Cluster中都希望解决的。美国将问题移交给数据打包者；你以任何你喜欢的方式打包数据，我只是想解决我的问题。我钦佩处理这个问题的公司。

最后，在优化方面，更多的精力放在了节点端自身的优化上。“gas”本身的账本节点是有限的，在所需的出块周期内，你能达到的“gas”数量也是有限的。基本上，它是如何提高幅度。以太坊不处于 TSO 模式；它使用超过400G的存储空间，读写这400G是有问题的。有的提高数据读写能力，现在市面上也有。这很有趣。随着这些技术逐渐成熟，区块链扩展技术变得更加强大。而你的硬盘可以具备瞬时读写的性能，理论上可以显着提升“gas”，这是我们在优化时应该考虑的。

n****区块链技术迭代难度远大于传统技术****

为什么区块链技术的迭代比传统技术更难？那是因为区块链分布式系统面临的问题与中心化系统面临的问题不同，可能非常不同。以美国为例，白皮书中有一段写道：在mega和mega之间的原子交易中，原子性是不可分割的，多个mega-s之间的原子性只能并行执行，不能串行执行。当你进行优化时，你会发现，80-90% 的冲突是可以避免的，只有那些序列不明确的关系，比如在交换中，有 1-2% 的概率，这是你无法处理的。但是，绝大多数是可以处理的。接下来是存储。一家公司表示，他已经添加了IPFS。IPFS 存在很大的问题。现在无法保证性能。关于这一点，我问过很多P2P老手和专家，他们都表示，目前在非结构化数据存储方面是无解的。真正成为 IPFS 是非常困难的。

就个人而言，我对 IPFS 的未来是相当乐观的，但目前，它的实际实施问题仍然无法解决。最后一点是“合约”，即立即执行合约。如果您很容易应用 UTSO 模式，只需执行它。前几天和帅楚聊了聊，他说：合同挺复杂的；合同之间的冲突不一定是巨头之间的冲突，但很可能是其他人的冲突。

目前，该合同仍处于初期阶段。对我们来说，未来的发展方向应该是如何更高效地调整合约执行的顺序，通过寻找合约之间的相关性来调整它们的顺序，更高效地执行合约。

n****区块链技术目前处于从理论到实践的过渡阶段****

最后，我认为，目前区块链正处于从理论到实践的过渡阶段。2019年再谈区块链，没有实用技术的请不要跟我提。我认为你可以在 2017 年做到这一点。尤其是在 2018 年，做到这一点相当困难。我们都觉得有太多人在吹嘘自己的东西，包括一些十年都买不到的东西。它们都存在实际实现的问题。

现在看起来相当成功的区块链在性能上可能不是最好的，但有一点是肯定的：它极大地降低了开发者开发APP的成本。去年ICO为何如此火爆？为什么去年那么多人搞Token？以前每年都有很多人这样做，现在，你可以在基于 ICO 制作自己的 Token 时直接发布自己的 Token。对于有一年编程经验的人，在学习一点JAVA后，他/她可以在3天内完成。它是如此普遍，以至于所有程序员都可以做到。

未来可能有些人不知道如何开发区块链，但是可以开发一个APP，开发自己的分布式应用，这将是未来的一个大趋势。Ruff 公司已经经营了四年。我们在物联网领域已经成功从事物联网操作系统多年，现在我们可以用更抽象的方式开发一些外围计算的应用。而且，这些应用程序可以与区块链相结合。更新的应用程序都是标准化和抽象的数据，我对此感到非常自豪。这就是为什么当 Ruff 在程序员社区推出时，很多人都看好它。他们认为，这是我们接近物理柱的地方。

我跟公链打交道已经很久了，现在跟公链打交道和以前跟操作系统打交道的时候我也有同感。只有我降低了开发门槛，才能有更多的人进来。只有降低了门槛，才有更多的应用。比我更有创造力的人可以产生超出我们想象的应用程序。所以，我的口号出现了：“代码更简单，改变更快”。除非所有人都可以轻松愉快地开发应用程序，否则公共区块链不会成功。这就是我对公共区块链的态度，以及公共区块链如何成功。

非常感谢你们今天给我这样的机会与大家分享。这就是我今天的全部分享。谢谢。

****贵宾介绍：****

Roy Li：Ruff Chain创始人，Ruff CEO，著名安全专家和物联网专家，全球领先的物联网操作系统ruff.io创始人，复旦大学MSE硕士生导师。曾任威瑞信、趋势科技安全顾问，前北美诺基亚OVI首席技术官，四年QCon（软件开发大会）杰出制作人，三年GITC（全球互联网技术大会）讲师。