0.P1 brief

0．Agenda

1. Blockchain

区块链是这几年最火名词之一，想必大家多多少少都听说过。简单地说blockchain是一种特殊的数据结构。它是一种新型分布式的共享账本和数据库。它可以储存任何信息。blockchain具有去中心化、不可篡改、可以追溯、公开透明等特点。

区块链由一个个区块（block）组成。区块很像数据库的记录，每次写入数据，就是创建一个区块。每个区块包含两个部分。区块头（Head）记录当前区块的特征值。区块体（Body）记录实际数据。区块链上的每一个全节点都完整保存数据库的所有内容。区块头包括了生成时间，本区块体的Hash，上一个区块的哈希。这里的SHA256是区块链的哈希算法。如果当前区块体的内容变了，或者上一个区块的哈希变了，一定会引起当前区块的哈希改变。这一点对区块链有重大意义。如果有人修改了一个区块，该区块的哈希就变了。为了让后面的区块还能连到它（因为下一个区块包含上一个区块的哈希），该人必须依次修改后面所有的区块，否则被改掉的区块就脱离区块链了。由于后面要提到的原因，哈希的计算很耗时，短时间内修改多个区块几乎不可能发生，除非有人掌握了全网51%以上的计算能力。

当新的（交易）数据被写入链时，节点 通过共识机制对新的数据进行验证，验证真实后的数据被打包进入区块，加密后每一个区块包含前一个区块的哈希值，形成“首尾相连” 的链式结构，因而得名区块链。区块链的设计特点让其具有以下的特征：

**弱中心化。**在一个分布式的账本系统下，任一节点均拥有所有记录的副本，每一笔新写入链的数据都经过有效的共识机制验证真实， 交易双方无需信任彼此，无需第三方背书，即可完成点对点的交易活动。在区块链场景下，并无强势的中心掌控所有的数据，每一参与 都在平等的位置，在共享风险的同时也在共享利益都在平等的位置，在共享风险的同时也在共享利益。

**不可篡改。**区块链具有只可添加性（append-only），新生区块附加在最长链上，不对之前区块产生影响。同时，由于每个区块都 引用前一区块的哈希值，若强行对先前任意区块进行破坏，则需替换自该区块后的所有区块以满足哈希值的变更，这使得数据篡改的可能 性近乎为零。

**数据可追溯**。区块链中有时间戳服务器运行，会为每一个区块的生成印上时间戳，储存于哈希值中。链式结构下，每一区块时间戳引 用前一个区块的时间戳，时间信息随区块高度增大而增加，结合入链信息无法篡改的特性，交易发生的先后可以追溯。使用区块浏览器， 个体可轻易查询到交易时间、区块生成时间、区块确认时间等，公开透明。

**安全加密**。采用不对称加密方式，由公私钥完成加解密过程。只有公私钥匹配才能解锁账户价值；私钥由用户保存，只要私钥不泄 露，黑客就无法对账户进行攻击。同时，由于每一节点都分布式地储存全部数据，可利用冗余性抵抗攻击。

通过Consensus mechanisms(共识机制) Smart contract（智能合约）Distributed Ledgers（分布式账本） RSA algorithm（非对称加密）等技术使得区块链在安全领域得到广泛应用。如数字货币比特币，确保数字货币不受任何组织机构影响。著名音乐平台spotify 使用区块链技术来提高音乐版权支付的可追踪性。 右图可以看出越来越多的企业使用区块链技术应用到自己的核心业务中。

1. **international trade**

随着全球化的加剧，国际贸易已经非常普遍。我们也能从这张图中看到传统国际贸易流程非常复杂。进口方与出口方之间存在很多中间环节。包括：双方bank，Customs, inspector, forwarder。 进出口方与Insurer 三方需要通过document courier 拟定贸易合同。货物运输过程中需要通过 Pre-shipment Inspector、Terminal、shipper 、Customs等环节。而结算时不光需要双方银行参与，还需要correspondent bank的介入。

With the accelerating pace of globalization, international trade has become very common. We can also feel the complexity of traditional international trade processes from this picture intuitively.

There are many intermediate links between the importer and the exporter. It includes import and export banks, Customs, inspectors, forwarders, and so on. The importer and exporter, and Insurer need to draw up a trade contract by the document courier. The cargos have to pass Pre-shipment Inspector, Terminal, shipper, Customs, and other transportation links. The settlement involves not only the banks on both sides but also need the correspondent bank.

Recent research by the Boston Consulting Group finds that more than 20 players are usually a party to a single trade finance transaction throughout the process, with data captured in 10 to 20 documents, creating approximately 5,000 data field interactions. While the entire transaction process is cumbersome, there are also many security risks, such as misoperation and fraud.

传统国际贸易痛点具体规划为以下四点

There are 4 pain points of traditional international trade as follows:

2.1 **数据孤岛**

国际贸易参与方众多，业务流程复杂。导致数据生产源众多，数据流也错综复杂。与此同时数据具有高度商业机密性。出于信息安全及自身商业利益的考虑，参与方无法也没有意愿与任何第三方，这导致数据孤岛的形成。

由于地域文化差异，跨境贸易中结构化数据难以统一，如订单、发票、申报单等。这使得欺诈风险变得更高。

**Data silo**

A large number of International Trade participants and complex business processes resulted in fragmented data sources. And the data is generally highly commercially confidential. Therefore, considering information security and their commercial interests, participants cannot and do not have the will to share data with any third party. It leads to the formation of data islands.

Due to regional and cultural differences, it isn't easy to unify structured data in cross-border trade, such as orders, invoices, and declarations. It grants the transaction process a higher risk of fraud.

**2.2 信任缺失**

大量通过传统的纸质文件、手写签名、第三方托管等模式，不但无法有效降低欺诈风险，也在一定程度上 影响了跨境贸易的处理效率。

*数据源真实性难确认*

不同国家和地区的管 辖区，任意一方想要确认其他各环节的参与方身份的真实性，避免贸易欺诈风险都面临着 巨大的挑战。

*层层传递影响数据可信度*

当前跨境贸易业务中，业务链较长。数据经过层层传递，其可信度势必大打折扣，导致跨境贸易过程中仅信息核实环节便需要投入大量的时间和人力成本。

**Lack of trust**

There are many traditional paper documents, handwritten signatures, third-party custody, and other modes, not only cannot effectively reduce the risk of fraud, but also affect the efficiency of cross-border trade processing to a certain extent.

The data sources are distributed in different countries and regional jurisdictions. It is hard to confirm the authenticity of the participants' identity in the other business links to avoid the risk of trade fraud. In the current international trade business, the business chain is relatively long. The credibility of data passed through layer by layer is bound to be greatly compromised. As a result, only information verification in the cross-border trade process requires a lot of time and labor costs.

**2.3 流程协同低效**

国际贸易环节中涉及不同国家多个参与方，甚至不同国家监管机构间的协同合作。由于地域文化等因素很难行程一个涵盖各个环节的高度数字化和自动化系统，提高国际贸易整体的安全性与协同性。

**Inefficient process collaboration**

Most of these links involve multiple participants from different countries, and even cooperation between regulatory bodies in different countries. Due to the business particularity of cross-border trade, the absence or problem of any link in logistics, capital flow, and information flow may lead to an inefficient collaboration of the whole business process, directly affecting the overall security and synergy.

* 1. **中心化平台瓶颈**

目前大部分国际贸易采用中心化的服务或平台。中心化平台拥有远高于一般参与方、极不对称的权利和义务。并且还存在着中心化平台透明度低、对中心化平台依赖性强的问题。一旦中心化平台违约、丧失或连接丧失，整个系统的安全性会遭受巨大的破坏。

**Bottleneck of centralized platform**

At present, most international trade uses centralized services or platforms. Centralized platforms have extremely asymmetric rights and obligations that are far higher than those of general participants. And there are also the problems of low transparency of centralized platforms and strong dependence on centralized platforms. Once the centralized platform breaches, loses, or loses connection, the entire system's security will suffer huge damage.

1. Blockchain advantage

**3.1 数据互通**

***数据一致性，整合零散数据。***

区块链系统上参与方上传的数据，在经过共识机制验证后，会被记录在一个系统内所有人共同拥有的 “账本”中。极大地提升零散数据汇总整合的效率，使全流程数据的系统化共通成为可能。区块链系统可以方便监管，使得个个环节接收到的信息是真实有效的。确保整个交易流程的安全。

***隐私方案解决数据安全与共享的矛盾***

区块链技术能够通过技术手段解决商业数据隐私机密和商业数据共享价值间存在已久的矛盾。既可提高物流供应链上下游企业的风险控制能力，也有助于海关对贸易环节的监管。

**Data connectivity**

Blockchain technology can integrate scattered data and ensure data consistency on the chain. The data validated by a consensus mechanism and recorded in the "ledger" shared by everyone in the system, eliminating the link between the "respective ledger" data of different participants, significantly improving the efficiency of the consolidation of fragmented data aggregation, and making it possible to systematize the whole process of data. The blockchain system can facilitate supervision and make the information received in each link is true and effective. Ensure the safety of the entire transaction process.

Blockchain technology can solve the contradiction between commercial data privacy and confidentiality and retail data sharing through cryptographic techniques. It can improve the risk control capabilities of upstream and downstream enterprises in the logistics supply chain and help the customs supervise the trade links.

**3.2 增强信任**

***链上信息不可篡改、可追溯。***

区块链链式结构不可篡改，信息记录可追溯的特性，使得所有通过共识验证成功上链的数据，都无法因 个别参与方的意愿，在其他参与方不知情的情况下被修改。即使信息经过层层传递，贸易参与方或海关仍能够通过区块链系统高效地核实 数据真伪，有效替代传统的纸质文件、手写签名等相对易伪造的方式的同时，也更贴合跨境贸易数字化趋势的需求。

**Trust enhancement**

The tamper-proof features and the traceability of information records make it impossible for all data to be modified without the individual participants' knowledge. Even if the information is transmitted layer by layer, trade participants or customs will be able to verify the data's authenticity through the Blockchain system efficiently. Furthermore, it effectively replaces the traditional paper documents, handwritten signatures, and other methods~~, which are relatively easy to forge, and more attuned to the demands for digital trends in the cross-border trade.~~

***身份认证和信息交叉验证。***

不可篡改特性与智能合约的应用，可以为数据提供方进行身份验证。从源头上杜绝欺诈风险，进一步提高安全性能。

**3.3 优化流程协同**

区块链引入智能合约的应用，在提高自动化程度，增加效率 的同时，也能在一定程度上规避信用欺诈风险和操作风险，。

**Optimized process collaboration**

The blockchain introduces the application of smart contracts while improving the degree of automation and increasing efficiency, and avoiding the risk of credit fraud and operational risks to a certain extent.

**3.4 弱中心化网络**

去中心化将不再不依赖权威机构的认证和信用背书，可以简化交易流程，缩短交易周期。减少对中心化平台依赖性。

**Weakly centralized network**

Weakly centralized network will no longer rely on certification and credit endorsements from authoritative institutions and simplify transaction processes and shorten transaction cycles. Reduce dependence on centralized platforms.

（13）我们可以看到传统的国际贸易复杂的流程，可以通过使用区块链进行优化。与此同时可以提高整个国际贸易的安全性。

We can see that the complex process of traditional international trade can be optimized through blockchain. At the same time, the security of the entire international trade can be improved.

大家提及区块链都会想到比特币。然而区块链还有非常广泛的应用场景。很多传统行业都可以借助区块链进行优化。

区块链的核心概念是去中心化。这也是一个颠覆传统的创新。但并不是一味地去中心化才是最优解。在国际贸易中并不需要完全的去中心化。每一个应用场景都需要寻找到一个合适平衡点。

Proof of work 消耗非常大的能源。区块的生成需要矿工进行无数无意义的计算。 在某些场景中，proof of work 并不是最佳的选择。在某些应用场景中使用proof of stack 效果更好。