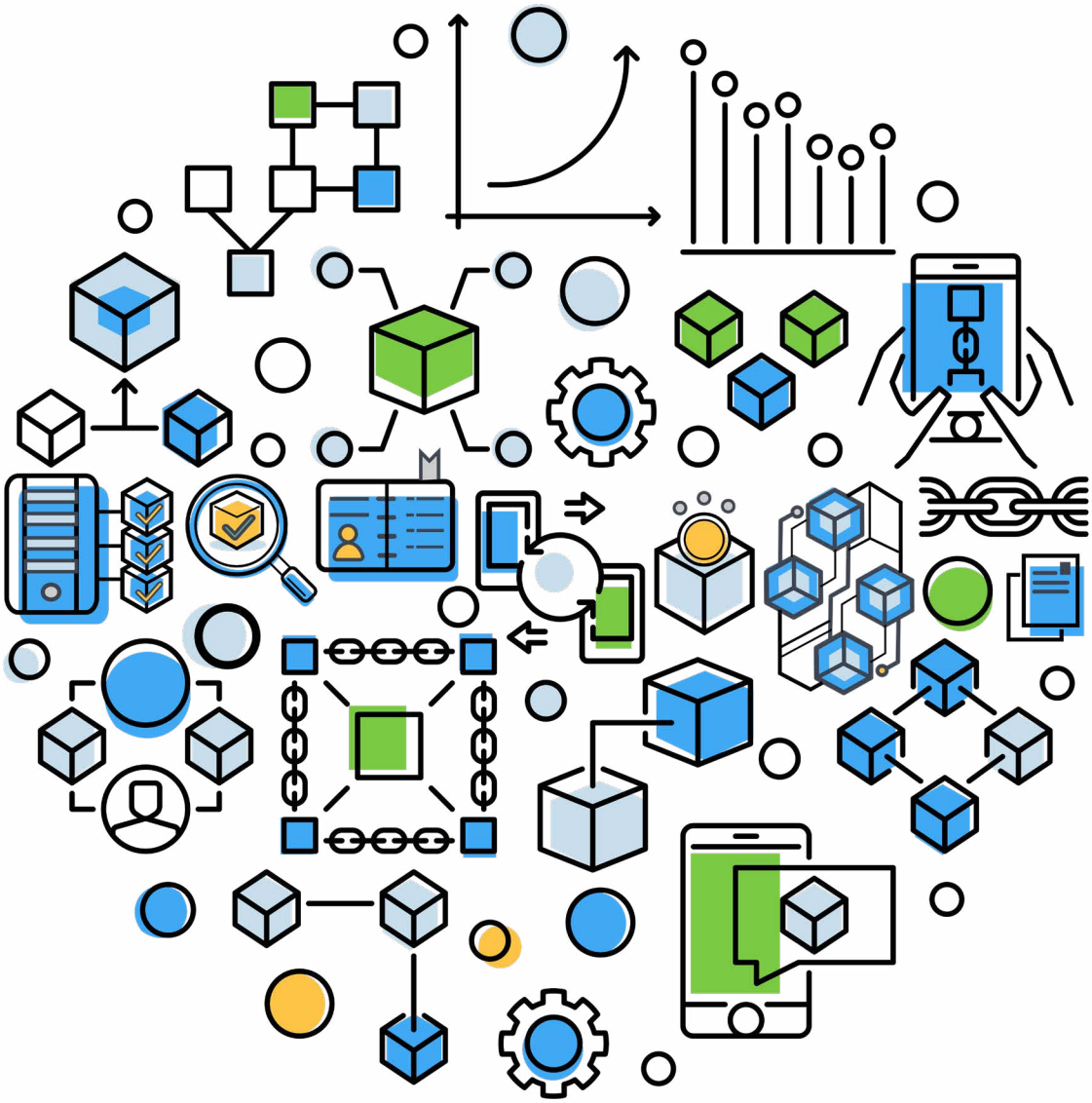
Deloitte.

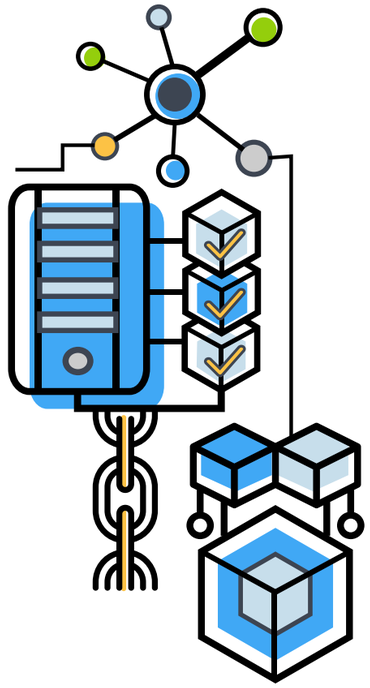
蚂蚁集团
ANT GROUP



Taking risk information sharing to the next level

Integrating Blockchain and Financial Crime Compliance - Deloitte · Ant Group

MAKING AN IMPACT THAT MATTERS since 1845



Blockchain is no longer the technology of the future – it is the technology of the now. It has already taken hold in a broad range of industries from financial services to hospitality. Institutions laying the foundations for blockchain technology are equipping themselves for the future. It is essential for financial institutions to understand, hypothesize about, invest in and deploy blockchain in their development roadmaps.

This whitepaper explores the integration of blockchain technology with Financial Crime Compliance ("FCC"). It sets out the key advantages and challenges that come with leveraging the blockchain technology in the FCC areas.

Over the past decade we have witnessed a sharp acceleration in the pace, depth, and complexity of regulations worldwide. In response, financial institutions have worked vigorously to achieve a competent FCC control framework addressing inherent risks and ultimately realizing an institution-wide culture of compliance, integrity, and reputation. This has paved the way for sustainable business development and stronger bonds of trust among financial institutions and their stakeholders, regulators, and customers.

Financial institutions are mobilizing their resources towards agile and scalable solutions to ensure standardization, security, and targeted strategies. The goal is that each FCC process is devised to meet regulatory expectation, and operational efforts are streamlined on a risk-based approach with automated assistance. Traditional FCC measures tend to be **manual** and **labor-intensive,** requiring a relatively high level of resource input to establish a robust institution-wide FCC framework while continuously monitoring customer information and transactions. With the large volume of manual processes, financial institutions are prone to human errors and exposed to risks associated with **data accuracy** and **reliability.**

In addition, high reliance on manual work makes an institution relatively slow-moving in responding to fast-evolving financial crime typologies and pose major challenges to mitigate risks effectively. As a result, financial institutions are turning to new technologies and innovations to increase effectiveness of risk management and greater security of data. This is also allowing workforce to focus on less repetitive and more strategic tasks. In addition, this also alleviates potential challenges in operational transformation and customization of a technological application to cater fully for an institution's specific demands.

Thanks to the growth of technology in the financial sector, a variety of innovative financial services and offerings are developing, and the line between financial services and technology is blurring. The integration of financial services and technology is continuously expanding the breadth and depth of financial markets, and also changing the manner in which risk must be managed in the financial services sector. This is due to the emerging threats as a result of new products and services as well as ever-changing mechanisms in laundering money and promoting terrorist financing.

Given that risk management today must keep up with the evolution

mentioned above, customers and shareholders seek comfort that they can place trust in the business or the services they are consuming. Trust has become a key factor for regulated entities to build and continuously maintain – with regulators, clients, stakeholders, employees, and each other. There is an opportunity for each of us to participate in developing the future of trust within a Secure Multi-party Computation ("SMPC") ecosystem, specifically in the FCC domain. We can:

1. Provide transparency and enhance efficiency in how laws and regulations are interpreted;
2. Improve how financial crime risks are managed; and
3. Automate reporting to senior management and regulators.

蚂蚁集团
ANT GROUP

AntChain is a leading technology brand of Ant Group, which aims to build innovative trust infrastructure in the age of the digital economy. AntChain focuses on core technological breakthroughs and integrates technologies including blockchain, AIoT, and intelligent risk management. AntChain is looking to solve practical industry issues by linking various networks and promoting widespread applications of the blockchain technology. From 2016 to 2020, AntChain was ranked as number one in the number of blockchain-related patent applications and licenses in the world. AntChain adheres to an open ecosystem, where all of its partners can achieve common wins and benefits brought by the blockchain technology. So far, AntChain has provided trust solutions to business partners covering over 50 scenarios.

Deloitte.

Deloitte's global network has developed an ecosystem of financial crime compliance and blockchain labs, pooling professionals around the world to devise innovative blockchain solutions , ideation, strategy, prototyping, and development. The Deloitte Asia Pacific Blockchain Lab works with technology specialists across the region to conduct client workshops, create thought leadership, develop prototypes, provide production support and deliver innovative ideas and solutions for deployed blockchain networks in the financial services industry.

Dr. Paul Sin, leader of the Deloitte Asia Pacific Blockchain Lab says, "While there is regulatory uncertainty or even outright bans on digital assets and cryptocurrencies in Asia-Pacific, blockchain is uniquely capable of meeting the need for data sharing across national and industry borders without breaching privacy. Cross-border track-and-trace is key to sustainability and anti-counterfeiting efforts, while identity validation is essential for virtual banks, SME trade financing, and financial inclusion. These topics are on top of most Asian governments' agendas, especially in the post-COVID-19 economy."

How can blockchain build and maintain trust?

Blockchain and Distributed Ledger Technology ("DLT") is much-discussed in today's digital transformation era owing to their **immutable** and **distributed** nature. Blockchain technology can help financial institutions achieve compliance automation[1] that embodies **transparency,** due to its decentralized nature where all nodes can access information on the chain; **reliability,** as the technology is tamper-proof; and **efficiency** and **cost-effectiveness** by accelerating processes and reducing costs while eliminating error-prone repetitions in solutions for the financial services industry.

Blockchain technology offers potential in solutions in numerous FCC practice areas.

KYC digital identity creation (identification) and authentication (verification)

- By creating digital identities and filing verification data on blockchain, institutions can improve efficiency in the client identification and verification process

Automated transaction monitoring

- Where an institution adopts blockchain-supported monitoring systems, each transaction is logged securely and traceably on the chain. This will enable transaction monitoring and payment fraud detection using smart contract as transaction records on the chain be tamper-proof

Data storage and maintenance

- Financial institutions may consider moving their know-your-customer ("KYC") databases, transaction history records and digital documentation to blockchain resting assured of data security

1.Deloitte, Over the horizon: Blockchain and the future of financial infrastructure Research from Deloitte & the World Economic Forum, https://www2.deloitte.com/global/en/pages/financial-services/articles/gfsi-disruptive-innovation-Blockchain.html

In the Asia Pacific region – especially in China – there continues to be a strong belief in the transformative and strategic value of blockchain. There are numerous initiatives to develop private/permissioned blockchain use cases. Embracing the fundamental value of trust generated by blockchain technology paves the way for institutions to re-shuffle their FCC focus and future resource planning.

According to Deloitte's 2020 Global Blockchain Survey, 34 percent of China Mainland and 52 percent of Hong Kong SAR respondents plan to spend at least USD5 million on the Blockchain technology over the next 12 months.

Blockchain as a Top 5 strategic priority 55 percent of the 1,500 senior executives across 14 countries and regions see blockchain as a Top 5 strategic priority. Meanwhile, 89 percent of Asia-Pacific respondents are hiring or plan to hire blockchain expertise, and 39 percent have already deployed blockchain in a production environment. Some 83 percent believe failing to adopt blockchain will diminish their competitive advantage.

Data sharing, reconciliation and traceability are the top three blockchain use cases in Asia-Pacific.

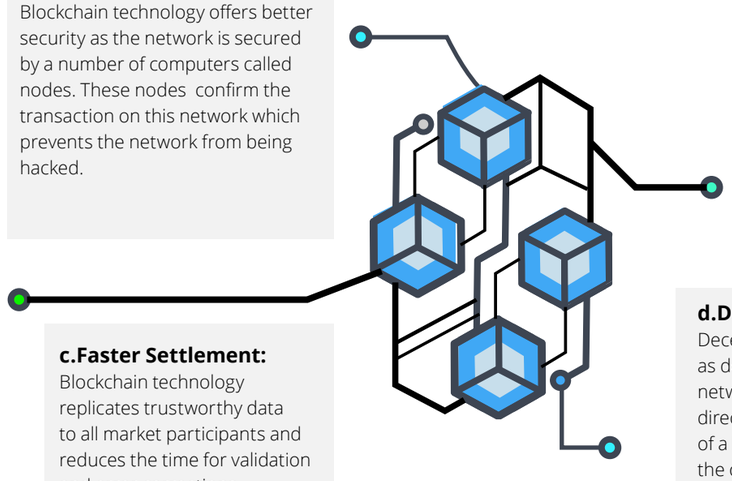
The report also reveals that nearly 89% of executives believe in the potential of digital assets in the next three years, and 70 percent regard the pace of regulatory change as very or somewhat fast. Although digital currency has become the top use case globally, data sharing, reconciliation and traceability are the top three blockchain use cases in Asia-Pacific.

What is Blockchain?

Blockchain first came to public attention in the 2009 Bitcoin revolution. Bitcoin is a protocol which allows peer-to-peer exchange of value without the need for a third-party intermediary and is applied based on a public ledger system that uses cryptography to validate transactions. While this has captured the imagination of the business world, it is the underlying technology – known as blockchain.

Four key characteristics of blockchain:

a.Better Security:
Blockchain technology offers better security as the network is secured by a number of computers called nodes. These nodes confirm the transaction on this network which prevents the network from being hacked.



b.Immutability:
The creation of immutable ledgers is one of the main values of blockchain. The technology keeps ledgers in a never-ending state of forward momentum, which means the ledgers would often remain in real form and be tamper-proof.

c.Faster Settlement:
Blockchain technology replicates trustworthy data to all market participants and reduces the time for validation and error corrections.

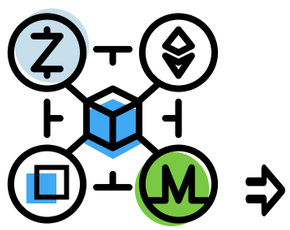
d.Decentralized System:
Decentralized technology allows assets such as documents and contracts to be stored on a network. Through this system, the owner has direct control over his/her account by the means of a key that is linked to the account which gives the owner the power to transfer the assets to anyone.

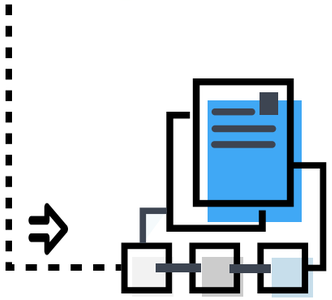
In the context of the financial services industry, these characteristics bring advantages such as:

1. **Process Integrity:** Due to the independently operating nodes, blockchain is designed in such a way that any block or transaction that adds to the chain cannot be edited. This protects the entirety and integrity of the process.
2. **Traceability:** All actions that occur on a blockchain can be easily located, which allows for easier tracing and remediation actions, and creates an audit trail.
3. **Security:** Individuals entering the blockchain network are provided with a unique identity linked to their accounts. This encryption ensures that only the account owner can operate the transactions and makes it difficult for hackers to disturb the chains.
4. **Enabling processing and settlement:** Before the invention of blockchain, traditional banking organizations took days to initiate and process transactions. Blockchain enables transactions to take place .

How can Blockchain be leveraged to share risk information?

A fundamental trait of blockchain technology is that it enhances information sharing. Blockchain allows storage, maintenance and exchange of units of value within a network. These units are pieces of information ranging from money to intellectual property to many different types of information. As the information bearer, a blockchain creates a layer of trust between the participants of the network without the need for a third-party intermediary.





Transparency is key to tackling financial crime

Information sharing is essential for the effective functioning of Anti-Money Laundering and Counter Terrorist Financing ("AML/CFT") programs. Criminals today use the global financial system to their advantage and continue to formulate new ways of laundering money or undertaking terrorist financing. While our regulatory and legal frameworks tend to be jurisdiction-specific, criminals do not operate in such silos. In fact, criminals actively exploit this vulnerability in AML/CFT programs.

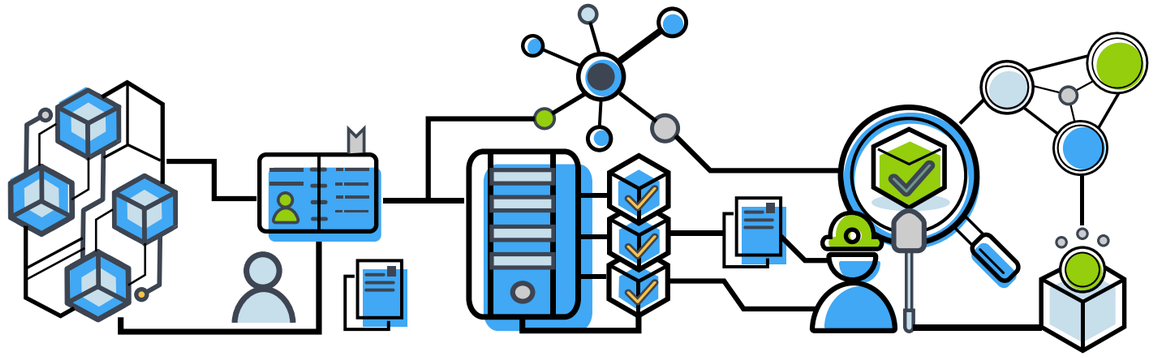
Data privacy and secrecy laws sometimes limit the ability of law enforcement agencies to identify, capture, and build cases against criminals. An information sharing mechanism that is compliant with privacy and secrecy regulations will enable law enforcement agencies in different jurisdictions to join forces in tackling financial crime.

Effective information sharing is also a key aspect of the recommendations set out by the Financial Action Task Force ("FATF"), a major AML standard-setting body and international organization, as it pointed out that effective information sharing is a key factor in combating financial crime as it improves transparency and protects the integrity of financial systems. In November 2017, a guidance paper[2] was published by the FATF aiming to highlight the value of information sharing amongst the private sectors, identify challenges that inhibit this information sharing, and provide examples of how such information sharing can be implemented within financial institutions and between financial institutions that are not part of the same group.

Access to information completeness of transactions is a key challenge in mitigating financial crime. Information can be scattered in various pockets at the moment: within the financial institution, with the regulator and law enforcement agencies, with the customer or with other financial institutions. Without access to comprehensive information and data, identification of specific threats and typologies becomes all the more challenging. In many instances, financial institutions file SARs due to the lack of information to corroborate transactions.

2.*FATF, Private Sector Information Sharing,* https://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf

Taking risk information sharing to the next leve



This, in turn, has increased the burden on financial intelligence units ("FIU") worldwide. Globally, the number of SARs filed has been gradually rising in recent years, and suspicious activity reporting is increasingly considered as one of the fundamental pillars for AML/CFT programs and regimes.

However, research shows that only a low proportion of SARs submitted to FIUs are actioned – interviews with FIU heads showed that 80-90 percent of SARs are of no immediate value to active law enforcement investigations[3]; FIUs in the EU pointed out, on average just over 10 percent of the SARs submitted are put to use[4]. FIUs need to investigate a vast number of SARs, which have insufficient information or details to assist in the investigation. The scattered information between institutions and financial intelligence agencies affects each other, posing major challenges to the fight against financial crimes.

Blockchain opens up opportunities for organizations, regulatory bodies, and governments to achieve information sharing in a secure manner.

As such, the old way of connecting dots and detecting criminals is increasingly inefficient and may not necessarily be the most effective manner in which we can come together as a community to combat financial crime. As of now, more than 20 countries[5] recently committed to developing public–private financial information-sharing partnerships ("FISPs") to close the information gap by sharing public and private insights and co-develop typologies of risk that banks and establish risk consensus on financial crime.[6]

3.Royal United Services Institute for Defence and Security Studies, The Role of Financial Information-Sharing Partnerships in the Disruption of Crime, https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_report_-_oct_2017.pdf

4.European Union Agency for Law Enforcement Cooperation (Europol) Financial Intelligence Group, From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact, https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact

5.Afghanistan, Argentina, Australia, Colombia, France, Georgia, Indonesia, Ireland, Italy, Japan, Jordan, Kenya, Malta, Mexico, the Netherlands, Nigeria, Singapore, Spain, Switzerland, Trinidad and Tobago, Tunisia, the United Arab Emirates and the UK made such commitments policy at the London Anti-Corruption Summit on 12 May 2016.

6.Royal United Services Institute for Defence and Security Studies, The Role of Financial Information-Sharing Partnerships in the Disruption of Crime, https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_report_-_oct_2017.pdf.

How has the private sector explored the sharing of "money laundering risk information"?

Information sharing is important in targeting money laundering risks, and there have been numerous international efforts made to enhance it. We set out below three examples here, each of which exemplifies a different type of public-private and private enterprise collaboration.

In April 2017, the Association of Banks of Singapore, the Monetary Authority of Singapore, and the Singapore Police Force, where Singapore's FIU is located, formed an AML-CFT Industry Partnership ("ACIP"). The ACIP brings together the financial sector, regulators, law enforcement agencies, and other government entities to work on risk identification, assessment and sharing of best practices. For example, on November 12, 2018, ACIP released a paper on Industry Perspectives - Adopting Data Analytics Methods for AML / CFT. This document shares best practices in deploying data analytics for the purposes of AML/CFT. The ACIP focuses on understanding broad-scale issues in the field of AML/CFT.

1

Another example of public-private partnership within a more explicit legal framework is the USA PATRIOT ACT 314(a) and 314(b) focusing on legal mechanism arrangements of financial intelligence information sharing led by regulatory authorities and voluntary sharing by private institutions. 314(a) prescribes a mandatory information sharing mechanism led by law enforcement and the Financial Crimes Enforcement Network ("FinCEN"), with a mandated mechanism including bi-weekly notifications to inform more than 34,000 points of contact at more than 14,000 financial institutions of suspected subjects. [7] 314(b), on the other hand, is a voluntary information-sharing mechanism led by financial institutions to enhance their own risk understandings and better support law enforcement investigations.

2

A third example of purely private partnership is Transaction Monitoring Netherlands ("TMNL")[8], which brings together five of the largest Dutch banks to establish an enterprise that will jointly monitor the transactions of these banks to detect money laundering. An estimated 16 billion euros is laundered in the Netherlands annually, tied to predicate offenses ranging from human trafficking, narcotics trafficking to terrorist financing. Banks are committed to detecting these money flows and the TMNL will jointly monitor the transactions of multiple banks with advanced analytics techniques such as network analytics and anomaly detection. Similar efforts are also emerging in other jurisdictions.

3

In order to achieve more effective and collaborative[9] risk prevention and mitigation measures, Ant Group, amongst several private sector financial institutions, is actively exploring the sharing of money laundering risk information. These institutions hope to leverage blockchain technology for money laundering risk sharing while maintaining information security and anti-money laundering confidentiality.

Ant Group conducted a trial operation with blockchain technology to share risk information among different regulated entities in China, help voluntary agencies efficiently identify high-risk customers, and improve the prevention and control effectiveness of anti-money laundering programs. This trial operation achieved significant positive results.

Building on the trial operation, these institutions further analysed the application value of the scheme from the multiple angles, including business and technical feasibility; information security; privacy protection; international practice; and anti-money laundering confidentiality. The project team suggests that this model is promoted and applied among domestic voluntary agencies, so as to promote the overall prevention and control effectiveness of anti-money laundering programs in China.

7.FinCEN, *FinCEN's 314(a) Fact Sheet*, https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf

8. Deloitte, *Deloitte connects 5 Dutch banks to make an impact with Transaction Monitoring Netherlands (TMNL)* , https://www2.deloitte.com/nl/nl/pages/financial-services/articles/5-dutch-banks-to-make-an-impact-with-transaction-monitoring-netherlands-tmnl.html

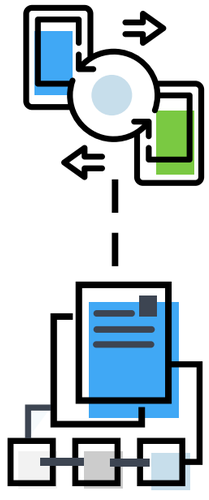
9.FATF refers to this as the Information Sharing Principle. FATF, *Consolidated FATF Standards on Information Sharing*, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Consolidated-FATF-Standards-information-sharing.pdf

What are the obstacles to sharing intelligence of suspicious transaction activity between private sector organizations and how can blockchain help?

Financial institutions face some critical challenges in sharing information with each other. The following issues and obstacles are some of the most pressing, and currently prevent private enterprises from effectively sharing risk information:

1. **Data privacy, banking secrecy, and personal data protection**
2. **Data security risks;**
3. **Data quality and accuracy across the private sector;**
4. **Risk ownership, legal and regulatory obligations of each institution; and**
5. **Cost of information sharing and operational challenge**

To address these challenges, the Institute of International Finance (IIF) and Deloitte published a whitepaper in 2019, titled "*The global framework for fighting financial crime*"[10]. This paper explored key areas in financial crime regulation, including cross-border and domestic information sharing. The paper outlined a number of recommendations on better information sharing across the private sector. From a policy and framework level, the paper suggested certain reforms to the FATF Recommendations to facilitate better information sharing, implementation of the current FATF standards for information exchange in FATF member states, regional and



10. Deloitte, *The global framework for fighting financial crime*, https://www2.deloitte.com/global/en/pages/financial-services/articles/gx-global-framework-for-fighting-financial-crime.html

11. ACAMS, *Distributed Ledger Technology: Streamlined CDD Examination Process through Blockchain Application*, http://files.acams.org/pdfs/2018/Distributed_Ledger_Technology_N_Zelensky.pdf

national reforms of current local laws and regulations, specifically those that appear to impede information sharing. The paper also suggested that technology should play a critical role in aiding this process.

In this regard, blockchain technology can be one avenue to enhance the information sharing process. Blockchain can help alleviate some of the issues and obstacles described above:

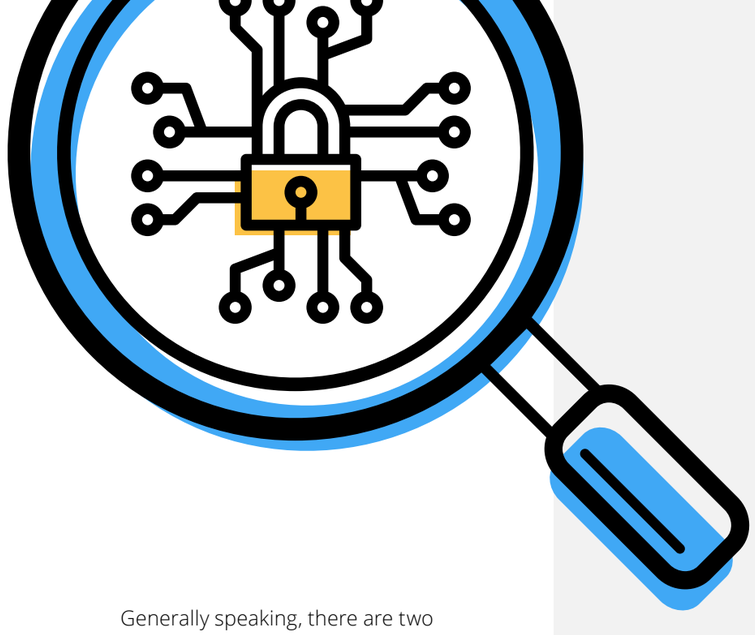
1. Legal frameworks with relation to data privacy, banking secrecy and personal data protection – Enhancing the regulatory and legal frameworks across the region or globally to allow non-personal information sharing would be beneficial. Even if the network is able to share anonymized data, consolidated from across financial institutions, it can assist in identifying new typologies, threats and patterns. With technological innovation, entity resolution and typology sharing techniques can help to piece together the transaction patterns, without requiring clients' personal data.

2. Another way to protect personal data is to encrypt such data using cryptographic algorithms on the blockchain. In addition, such a cryptographic function could be based on client data that is already in the possession of a financial institution, and therefore only another financial institution which possesses the exact same set of client data can read the relevant information. As such, only those financial institutions that need to know the information in order to understand the full picture of the transaction will be able to access the data.

3. Data security risks – The distributed and shared nature of the system could facilitate the recovery of both data and processes in the case of an attack (assuming that not all the nodes are corrupted simultaneously). This could reduce the need for costly recovery plans. Sophisticated encryption techniques could also provide an additional layer of protection to pools of information stored on DLT, compared to existing systems. Nonetheless, the risk of a cyber-attack would still need to be considered seriously in a DLT context[11].

4. Data quality and accuracy across the private sector – A critical advantage of the DLT is the accuracy of data. Only information that is validated and verified can be put on the blockchain.

5. Cost of information sharing and operational challenges – By leveraging blockchain technology, authorized users can access relevant information directly, with limited third-party involvement and eliminating verification requirements. As such, the cost of information sharing across the private sector can be managed to a relatively low level. In addition, if blockchain technology is deployed in the end-to-end transaction flow, the operational challenges of putting the relevant information on the blockchain will be reduced.

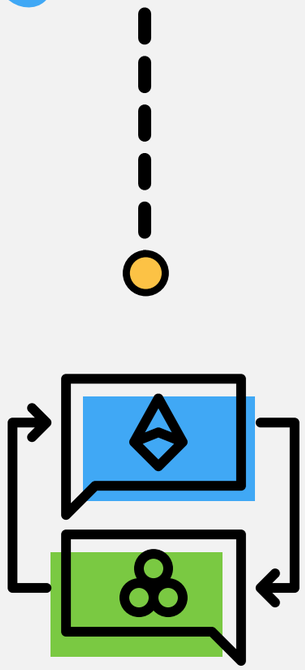


How can technology help realize AML risk sharing?

Generally speaking, there are two types of blockchain: public chains and permissioned chains. The two have different application scenarios.

Public chains are mainly used for cryptocurrency, which is characterized by decentralization and anonymity, diversification of businesses running on the chain, and no unified standard for system access. Therefore, the public chain is not recommended in this scheme.

Permissioned chain refers to a blockchain system where all participating nodes are licensed, and unauthorized nodes cannot access the system. One method of constructing the permissioned chain is to use an alliance chain, which is suitable for business scenarios that need multi-party cooperation and consensus building. Through encryption technology and point-to-point transmission, a shared account book (or shared database) is established among multiple business parties. This method reduces data processing cost, improves the efficiency of transmission, and at the same time, ensures data security and mutual trust. An alliance chain is the recommended method for this scheme.



What is the scope of risk information sharing?

At present, the scope of information that participating institutions can share focuses only on information relating to high-risk customers' risk rating and relevant control measures. In line with the FATF guidance on information sharing amongst private institutions, this scope can be further expanded to include suspicious intelligence, and highly suspicious but not yet reported information and other relevant risk labels that may help identify money laundering and terrorist financing behaviours. Alliance institutions in a blockchain alliance can enhance their respective institutional transparency and create a more effective collaborative environment through risk information sharing.

Blockchain and data privacy protection technology help ensure data security for all participating institutions. This will help balance compliance with regulations on customer information security on the one hand, and realize cross-organization information sharing on the other.

From a legal point of view, authoritative publications interpreting Mainland China's AML Law[12] have suggested that private enterprises should maintain basic customer privacy and confidentiality, with the exception of certain socially and commercially harmful activities such as money laundering.

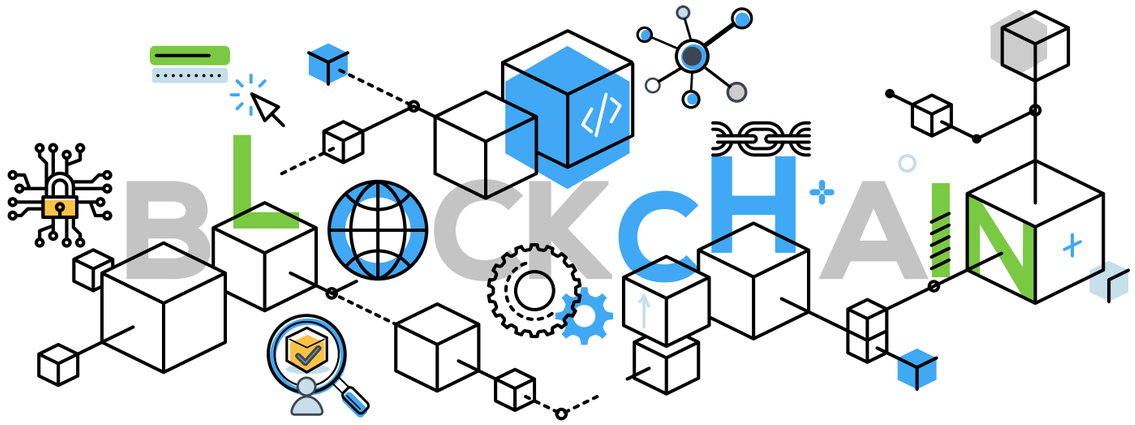
12.中国法制出版社，2007年1月，《中华人民共和国反洗钱法释义》(China Legal Publishing House, January 2007, *Interpretation on Law of the People's Republic of China on Anti-money Laundering*)

How to manage blockchain alliances?

According to established international practices, there are two common models of alliance for anti-money laundering information sharing: the voluntary organization model and the supervision coordination model.

1. Voluntary organization model: this model refers to a sharing alliance established voluntarily within a group or between cooperative organizations with close business relations. For example, within large financial holding groups, or between fund sales agencies and consignment banks, this model can be adopted to realize sharing while ensuring confidentiality for risk information.

2. Supervision and coordination model: this alliance model is composed of the main regulatory agency and its local branches, as well as volunteering agencies in the information sharing network. As participants, voluntary agencies share suspicious transaction intelligence data based on the consensus reached; regulatory authorities can act as the operation managers of the alliance chain to manage the entry and exit of participants, coordinate and supervise their actions on the chain, and also authorize a participating organization as an operation manager to exercise the aforementioned authority. In this model, the alliance chain can also take the supervisor's intranet as the construction environment.



What is the value of this suggestion?

We believe that implementing the alliance chain would bring the following advantages to inter-agency ML risk information sharing:

1. Breaking information islands of ML intelligence across institutions. We can form a joint prevention and control system on the basis of security and confidentiality, and comprehensively improve the effectiveness and timeliness of AML/CTF efforts by private enterprises.

2. FIUs can obtain more complete and valuable intelligence and high-quality SARs from regulated entities, and more data on – including identities of those involved – in transactions involving suspicious customers.

3. Implementing blockchain technology in anti-money laundering operations gives the network the potential to expand, to include public security, customs, taxation, industrial, commercial, and law enforcement agencies, and to form public-private alliance networks with mutual trust and close coordination at their core, to further improve the effectiveness of anti-money laundering work.

4. The formation of joint prevention and control systems will help reduce cross-industry money laundering risk, and ultimately mitigate money laundering risks at a national level.

5. Large financial institutions with strong anti-money laundering capabilities can work with smaller institutions to strengthen overall AML measures and controls, and enhance their effectiveness for better outcomes.

Recommended reference:

- ACAMS Today, *Digital Identity and Financial Crimes,* https://www.acamstoday.org/digital-identity-and-financial-crimes-2/
- IBM, *IBM Verify Credentials: transforming digital identity into decentralized identity,* https://www.ibm.com/blockchain/solutions/identity
- Frontiers in, *A decentralized digital identity achitecture,* https://www.frontiersin.org/articles/10.3389/fbloc.2019.00017/full
- Allen & Overy, *Cryptocurrency AML risk considerations,* https://www.allenovery.com/en-gb/global/news-and-insights/legal-and-regulatory-risks-for-the-finance-sector/global/cryptocurrency-aml-risk-considerations
- Global Legal Insights, *Blockchain & Cryptocurrency Regulation 2020 | 11 Cryptocurrency compliance and risks: A European KYC/AML perspective,* https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/11-cryptocurrency-compliance-and-risks-a-european-kyc-aml-perspective
- 101 Blockchains, *Top 50 companies that has adopted blockchain technology,* https://101blockchains.com/companies-using-blockchain-technology/
- Finextra, *Global banks and R3 test DLT for KYC services,* https://www.finextra.com/newsarticle/29747/global-banks-and-r3-test-dlt-for-kyc-services
- Fintech Futures, *Santander and Ripple to launch blockchain-based consumer payments,* https://www.fintechfutures.com/2018/02/santander-and-ripple-to-launch-blockchain-based-consumer-payments/
- Blockchain Council, *Top 10 companies that have already adopted blockchain,* https://www.blockchain-council.org/blockchain/top-10-companies-that-have-already-adopted-blockchain/

Contacts

Cheung, Chris Fung Yu
Partner, AML & Forensic
Deloitte China
Beijing
+861085125353
chrcheung@deloitte.com.cn

Singh, Radish
Partner, Financial Advisory
Deloitte AP
Singapore
+6597804580
radishsingh@deloitte.com

Zhang Hui
Ant Group Blockchain
Senior Advisor
shengchu.zh@antgroup.com

Li Shubo
Ant Group Blockchain
Senior Expert
daniel.lsb@antgroup.com

Sin, Paul Kwan Hang
Leader of Deloitte AP Blockchain Lab
Partner, Consulting, Deloitte China
Hong Kong
psin@deloitte.com.hk

Vasan, Mangala Kalyani
Director, Forensic
Deloitte China
Hong Kong
+85222586198
mavasan@deloitte.com.hk

Yang Wenyu
Ant Group Blockchain
Senior Product Manager
wenyun.ywy@antgroup.com

Wang Xinmin
Ant Group Anti-Money
Laundering Expert
xinmin.wxm@antgroup.com

BJ-001EN-20