Outcome report: Blockchain and Cybersecurity opportunities and challenges for digital finance

Session Date and Time: Thursday, 8 July 2021 (10:00 – 11:00 Geneva time). 60 minutes.

Opening Remarks: Bilel Jamoussi, Chief Study Groups Dept, TSB, ITU

Master of ceremony: Rouda Alamir Ali, Programme Officer, ITU Regional Office for the Arab States

Moderator: Suleiman Barada, Head of UAB digital & Sr. Advisor, Union of Arab Banks

Panelists:

- Suzana Maranhão Moreno, BNDES, Brazil
- Philippe Oeschlin, Director, Objectif Securite SA
- Sohail Munir, Advisor Emerging Technologies and Digital Transformation, Smart Dubai Government
- Arnold Kibuuka, Project Officer, TSB, ITU

Session summary : This session focused on blockchain and cybersecurity challenges and opportunities for digital finance in emerging economies and a specific focus on financial inclusion.

Digital finance and mobile payments have and continue to hold the promise to improve the standard of living for many people in the developing world. Emerging technologies such as blockchain are swiftly entering the financial services sector and could resolve the trust issue more efficiently. However, the security of the mobile applications providing digital financial services needs a rigorous method to test for systemic vulnerabilities in a comprehensive manner. Being able to detect such vulnerabilities is no easy task for developers, regulators and DFS providers.

This session will provide a high level overview of the innovative applications of blockchain, cybersecurity concerns for regulators and related policy and regulatory challenges for the digital financial services sector.

Main opportunities and challenges for blockchain and cybersecurity in digital finance discussed in the session are:

1. Blockchain and DLT may enable new business models, data ownership and new relationships based on trust and enable vulnerable groups to have access to finance
2. Blockchain and DLT can bring in new possibilities and permissionless innovation in Decentralised Finance (DeFi) which can make financial services more efficient and cheaper for people. For example In one year, the value of digital assets locked in DeFi smart contracts grew by a factor of 18, from $670 million to $13 billion; the number of associated user wallets grew by a factor of 11, from 100,000 to 1.2 million; and the number of DeFi related applications grew from 8 to more than 200.

3. Blockchain and DLT can help address the lack of identification issue and help more people to become financially included. Blockchain-based solutions have been implemented in Sierra Leone by KIVA in solving issues of identity and providing credit history enabling more people to have access to financial services.

4. Interoperability in DeFi is one of the hardest challenges when it comes to blockchain technology. Different blockchain networks have different communities, consensus, and hashing algorithms implementations which make standardization quite important. But we can only unlock blockchain's true value in DeFi if we can continuously improve user experience and leverage the network effect by creating interoperable blockchain solutions. The work from ITU-T Study Group 16 on interoperability for DLTs was noted.

5. Data privacy issues need to be addressed by regulators in blockchain fintech applications, especially when Artificial Intelligence is being used.
6. There must be processes in place to verify the transparency of Artificial intelligence algorithms used for digital financial services to avoid discrimination and bias which could lead to financial exclusion.
7. Regulators need to implement adequate risk management processes to take into account the new threats introduced by emerging technologies such as Blockchain and DLT and also introduce measures to adequately supervise and regulate intermediaries which are non-banks
8. The security of mobile payment applications used by consumers to access digital financial services needs a rigorous method to test for systemic vulnerabilities in a comprehensive manner.
9. There is at the moment not a standard way for regulators, DFS providers and developers to detect such vulnerabilities. Moreover, this is not an easy task for developers, regulators and DFS providers given the diversity of the mobile payment ecosystem and the different third parties involved in providing the different parts of the applications and the service.
10. During the session, an overview of the ITU DFS Security Lab was shared and the services that are provided to DFS regulators and service providers, in emerging economies, in auditing mobile payment applications was explained. The DFS Security Lab provides a standardized method for testing the vulnerabilities in DFS applications based on USSD, STK and Android platforms. The tests conducted for the security audit for mobile payment applications based on Android are based on the Open Web Application Security Project (OWASP) Mobile Top 10 risks framework.
11. Some of the most common system vulnerabilities noted in DFS applications are:
    a) application is using weak encryption cphers;
    b) the application does not verify the authenticity of digital certificates
    c) weak authentication methods are used
    d) the application can leak personal information of consumers
    e) payment information can be intercepted by man in middle attacks

12. Under the Financial Inclusion Global Initiative (FIGI) which is a joint collaboration between the ITU, World Bank and Committee on Payments and Market Infrastructure (CPMI) of the Bank for International Settlements, ITU has developed a number of knowledge resources such as the DFS Security Assurance Framework, methodology for testing of USSD, STK and Android apps and DFS Security Audit Guidelines which

provides guidance to regulators and providers on how to address these vulnerabilities. The ITU is also working towards implementing the recommendations in these reports at country level to guide regulators and DFS providers in developing and low income countries to implement structured approach based on international standards to securing their digital payments infrastructure and mobile payment applications.

13. The decentralization which is what blockchain or distributed ledger enables lead to the evolution of new business models in digital finance.
14. Because of blockchain there are new opportunities in digital finance in terms of new actors, new assets, new trust paradigms, and new business models.

Key Takeways

1. Blockchain and DLT can enable new business models, data ownership and new relationships based on trust and enable vulnerable groups to have access to finance.
2. The issue of providing people in emerging economies with an ID so that they can have access to financial services can be addressed by DLT and Blockchain as was shown in Sierra Leone.
3. At the same time, Blockchain and DLTs bring new risks and new players such as non-banks in the digital finance ecosystem and there is a need for regulators to address those risks and develop regulatory measures for non banks that will not hinder innovation.
4. Standards for blockchain and DLTs are required in order to enable interoperability among different blockchain implementations in DeFi in order to leverage network effects.
5. There is not a common methodology to conduct security audit for mobile payment applications and address systemic vulnerabilities.
6. The ITU DFS Security Lab provides a common methodology to conduct security audit for DFS applications and guide regulators and DFS providers in emerging economies on how to implement the DFS Security Assurance Framework, methodology for testing of USSD, STK and Android apps and DFS Security Audit Guidelines reports to enhance the security of their DFS ecosystem.
7. The policy and regulatory framework is required for Emerging Technologies, specially Blockchain in the Digital Finance ecosystem
8. Blockchain and DeFi have an impact in accelerating Cashless and Financial Inclusion