Iranian Virtual Currency Activity and Risks to Financial Institutions

Standard Chartered Bank – April 2019

Introduction

In October 2018, the US Financial Crimes Enforcement Network (FinCEN) published a Public Advisory (FIN-2018-A006) titled "*Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System.*[1]" The Advisory highlights that one of the main methods used by Iran to circumvent sanctions is its use of Virtual Currency (VC) and/or use of VC Exchanges (VCX), including Peer-to-Peer (P2P) type exchanges operating as unlicensed money service businesses (MSBs). FIN-2018-A006 advises financial institutions to review blockchain ledgers for activity that may originate or terminate in Iran, including P2P exchanges. In this paper, we have shared our review of the VC activity in Iran and set out an approach to managing this risk that we at Standard Chartered have found useful.

Given the current geopolitical environment and ongoing sanctions regimes against Iran there has been a navigation by both citizens and the state towards VC use. Most VCs are decentralised by design and offer a layer of obfuscation wherein transactions can be relatively private, assuming the parties involved. In the case of Iran, which has had to adapt to years' worth of sanctions (and likely evasion thereof), VC is a viable, if not ideal, option. As FIN-2018-A006 points out, Bitcoin (BTC), the most popular VC, has been used in Iran since approximately 2013 and its popularity is growing. In August 2018, Iranian officials announced their intention to creat a national VC. An early 2018 Forbes article estimated Iranians have moved as much as $2.5 billion out of the country in cryptocurrency.

Current Iranian VCX Environment

Main Entry/Exit Points

- Native Iranian VCX
- Third Country based VCX
- P2P VCX or Face to Face Exchange(s)
- E-Commerce and VC Payment Processors

Native Iranian VCX

Public domain research found approximately 28 Iran based VCXs. Native Iranian VCX primarily function as a platform for Iranian entities to exchange or trade and therefore provide the most direct sanctions exposure risk for financial institutions (FIs). Processing transactions, either directly or indirectly, on behalf of such exchanges or any payments facilitating investments in or trade with such VCX would likely expose FIs to heightened risk of breaching sanctions requirements.

Whilst Iranian VCX do present a challenge, they are likely the most straightforward of the VCX risks to mitigate, considering the extensive controls already in place to screen and block any potential dealings with Iranian entities. These entities can be added to payment filters and transactions screened as a proactive measure to manage this risk. Whilst many FIs will have existing controls in place to screen for Iranian indicators and block these entities, additions to payment filters may be beneficial as a secondary line of defense.

Third Country VCX

Iranian based parties utilizing third country VCX can present a more challenging scenario. Research of the top ten international VCX by market capitalization identified that all but one explicitly state they do not accept clients in Iran. Third party sources indicate that the single VCX exception does accept clients in Iran, and searches of the VCX's site did not find reference to any prohibitions on dealings in Iran. Allowing access to Iranian based clients can provide the ability for funds to move in and out of Iran and into the financial system.

OFAC Bitcoin Wallet Designations

On November 28, 2018, US Treasury's Office of Foreign Assets Control (OFAC) took a precedent-setting action against two Iranian nationals, Ali Khorashadizadeh and Mohammad Ghorbaniyan, who are alleged to have facilitated the exchange of Bitcoin proceeds on behalf of Iranian malicious actors who perpetrated the notorious SamSam ransomware. This was the first time OFAC included VC wallet addresses in their SDN designation, thus prohibiting any US persons and/or entities from dealing with these wallets and subjecting violators to secondary sanctions. Also noteworthy was the fact that these wallets involved Iranian parties alleged to be facilitating the movement of criminal proceeds from Iran based cyber actors and the wallets had direct and indirect links with known Iranian VCX, including two of the most well-known VCX in Iran (see Fig 1). These events further substantiate the need for situational awareness of the Iranian VC space and taking measures to identify potential risk, both proactive and reactively (in cases such as these).

Despite many VCX's taking measures to prevent dealings with Iran, Iranian citizens are collectively some of the most tech savvy in the world due to the Regime's oppressive internet content and censorship policies. Additionally, state organizations such as the Islamic Revolutionary Guards Corps are highly technically sophisticated, with units specializing in cyber tradecraft. Whilst VCX can attempt to block traffic from Iranian IP addresses, this can be circumvented with use of a Virtual Private Network (VPN) or other tools such as the anonymizing browser, Tor, although some VCX are known to ban or block VPN/ Tor traffic.

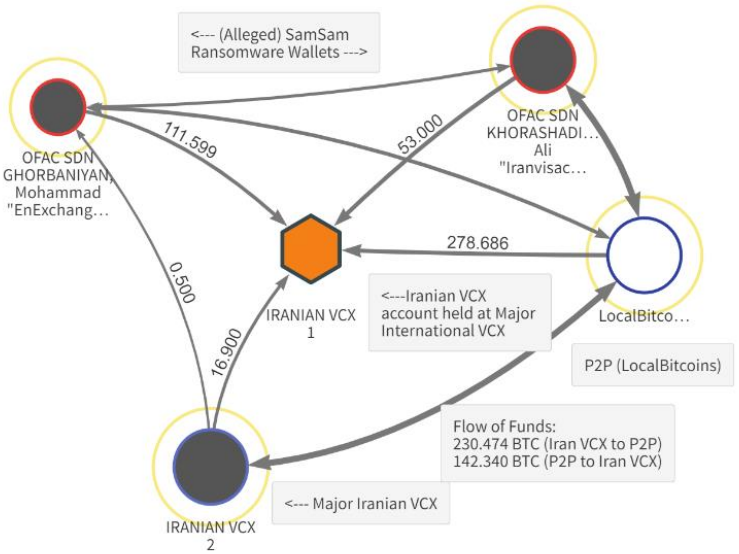

Fig. 1: Iranian VCX BTC interaction with SamSam Ransomware wallets and LocalBitcoins.com.

1. https://www.fincen.gov/sites/default/files/advisory/2018-10-12/Iran%20Advisory%20FINAL%20508.pdf

Iranian Virtual Currency Activity and Risks to Financial Institutions

Peer-to-Peer (P2P) Exchanges

P2P VCX allow parties to deal directly with each other and, by their nature, controls are limited. These platforms allow users to post advertisements for buying and/or selling cryptocurrencies in a specific geographic area, where other users can reply to these advertisements and either physically meet the buyer/seller or arrange for online payment / purchase. Whilst an examination of controls on P2P platforms is beyond the scope of this paper, the vast scale of this industry and the potential for manipulation and/or exploitation is potentially very high. Whilst Iranian P2P VCXs may pose a lower direct risk to FIs (as these transactions occur within Iran) the ability for Iranian entities to procure VCs in such an obfuscated manner may encourage growth in VC activity in the country.

Iranian National VC

In August 2018 Iran announced that it plans to unveil a national cryptocurrency, backed by its sovereign currency, the Iranian Rial (IRR). Numerous officials and advisors to Iranian President Hassan Rouhani commented publicly on this endeavor and indicated much planning and research has already taken place. Iran would be among a small number of jurisdictions which have developed a "sovereign" crypto, the most noteworthy of which is Venezuela, which announced development of its own sovereign crypto, "el Petro" in 2017, backed by oil. Whilst there have been relatively few attempts at launching a sovereign crypto currency, Iran will still have the advantage of "lessons learned," especially from Venezuela, which has been heavily criticised by experts with accusations that the Petro is a scam. Iran appears to be taking a conservative approach to implementation, with pilot testing, multiple phases and assistance from numerous public and private sector entities. If implementation is a success and the "Crypto Rial" could be openly traded for BTC and other major VCs, there could be a large uptick in VC activity in Iran. Any such uptick will present additional risks to FIs and proper monitoring and awareness will be key to taking appropriate actions.

E-Commerce and Payment Processors

E-Commerce sites and payment processors may present a greater opportunity for money laundering and possible terrorist financing risks. A simple search of one such site found a Bitcoin wallet for the Iranian Bonyad (religious charity) Imam Khomeini Relief Foundation (IKRF) (emdad.ir). The IKRF's Lebanon branch and its director, Ali Zuraik, were designated by the US Treasury for sanctions in 2010 for alleged financial/ material support of the designated terrorist organization, Lebanese Hezbollah. A search of the IKRF wallet address using blockchain analysis software found numerous donations and possible associated wallets. Whilst the amounts of these donations are relatively small, these nodes may represent an Iranian nexus, given the prominence of this Bonyad in Iran.

There are scores of entities whose sole business model focuses on assisting websites and organizations process BTC payments. Similar to third country VCX, these entities may or may not have policies limiting or banning dealings in Iran. For US-based BTC payment processors, there are legal obligations, but outside the US there is potential of direct or indirect dealings with Iranian entities. The same recommendations noted for third country VCX for risk mitigation and due diligence apply here. Effective use of blockchain analysis software is key in these efforts.

Bitcoin Mining in Iran

A key feature of Bitcoin (and other VCs) is mining, wherein networks of computers are utilised to validate and post transactions to the blockchain, with successful "miners" being rewarded for their efforts with BTC. In September 2018, the Islamic Republic of Iran (IRI) government officially recognised the mining of cryptocurrencies as an industry and the Central Bank of Iran planned to draft a policy/regulatory framework for this. Numerous IRI officials commented on IRI's acceptance of VC and willingness to embrace the technology, especially to facilitate trade in the wake of sanctions. Whilst it is possible to identify mining rewards on the blockchain, identifying the true beneficiaries of such rewards remains challenging.

What can Financial Institutions do?

• **Know the VC Space**: FCC professionals require more than a basic knowledge of blockchain concepts and the ecosystem of virtual/crypto currencies such as VC service providers and threat actors. Standard Chartered, through its Cyber-Financial Intelligence (CyFI) unit, develops expertise and builds engagements to better understand the VC ecosystem.

• **Deploy and utilize blockchain analysis solutions:** Such capabilities provide enhanced transparency into the flow of VC funds to enrich investigations and network analysis.

• **Collect, analyse and leverage Open Source Intelligence (OSINT):** VC activity not only encompasses actual transactions but social media forums. Such forums or 'sub-reddits' fuel the VC community. Key intelligence is often buried in the public domain but can be located, provided investigators / analysts know how.

• **Monitor and Investigate:** The development of actionable intelligence, especially if Iran experiences success in evading sanctions and/or gaining greater access to the global financial system by utilizing VC, will empower better financial crime investigations.

Conclusion

2018 has been a key year for the evolution of VC in Iran. The IRI's willingness to embrace VC and to take steps to implement a national cryptocurrency presents significant risks. Iran has often been described as the top state sponsor of terrorism, for its creation of and unwavering support for groups such as Lebanese Hezbollah and Asa'ib Ahl al Haqq. Whilst the scale of Iranian use of VC is still relatively small on the world stage, the environment is ripe for its growth and the IRI's willingness to embrace this and utilise it to possibly exploit sanctions is a concern. We believe rigorous and informed investigations need to be coupled with the use of cutting edge tools in order to effectively manage risk from VC activity, but collaboration will also prove vital. Strong collaboration between FIs and the VC/blockchain community, as well as members of the law enforcement who specialise in this area, is essential. Additionally, professionals who have a good understanding of VC/blockchain and possess cyber-related background as well as investigative and analytical skills will prove invaluable. As with any evolving technology which presents risk for money laundering, focus on building effective typologies will be instrumental in financial institutions identifying and tackling VC related risk.