BAE SYSTEMS
INSPIRED WORK

Managing the risks of cryptocurrency

Cryptocurrencies like bitcoin have forever changed business and personal finance.

Executive summary

On one level, cryptocurrencies function just like cash - all that's different is their entirely virtual nature. On another level, these new currencies, which use peer-to-peer payment technology, remove the long-time players from the equation. Central banks, mints, financial institutions and regulators, and established transaction networks such as SWIFT, NACHA and existing card platforms are out of the picture and are figuring out how to adapt. The resulting environment is uncertain and risky.

But one thing is perfectly clear: criminals have already adapted their attacks to include these platforms wherever and whenever the opportunity arises. Financial institutions need to remain vigilant and be agile to stay ahead of nefarious actors and ensure they remain relevant in an increasingly virtual, mobile and hyper-connected world.

Overview

Virtual- and cryptocurrencies have suffered many high-profile failures over the years. From currencies themselves, such as E-Gold, via the murky collapse of exchanges like Mt Gox and the high-profile failures of legally questionable marketplaces such as Sheep Marketplace and Silk Road, criminality and controversy have stalked the idea of virtual- and cryptocurrencies.

But it's not just the marketplaces and currencies that are subject to misfortune. Malware created specifically to steal bitcoin and any of the 200 other cryptocurrencies currently in circulation has emerged, fuelled by a rapid increase in value of bitcoins in 2013 and 2015 as the currency became more popular. Attacks are commonly aimed at bitcoin wallets and the compromise of private keys.

One of the most oft-cited strengths of cryptocurrency, Distributed Ledger Technology (DLT), can also be a great source of weakness. DLT holds all kinds of promise; a public decentralised blockchain that records that transaction's occurrence and authenticity. However, the need to mine new bitcoins has a negative impact on the rate of transactions and throughput. In the short to medium term, this will hinder the transaction rate, even at the comparatively low rates of 1-200,000 transactions a day.

In this report we focus on the application of DLT in the context of cryptocurrency and financial crime. We also investigate the burgeoning cryptocurrency landscape and advise financial institutions on essential steps they can take to ensure they have the right defences and habits in place.

The cryptocurrency gold rush

The business potential for virtual- and cryptocurrencies is unprecedented. Bitcoin transaction volumes are now approaching 200,000 per day (see Exhibit 1). Although still small compared with the hundreds of millions of conventional transactions in the world every day, there is clear opportunity for people and businesses to participate in this new and disruptive gold rush. Furthermore, while there are inherent scalability issues with older cryptocurrencies and blockchains (for bitcoin in particular) which will impact their ability to scale to real world transaction volumes, these limitations are being worked through in some of the emerging cryptocurrencies and blockchains. Some financial institutions already allow the use of cryptocurrency to open an account or make transfers into existing accounts from exchanges or retailers.

Financial Institutions need to remain vigilant and be agile to stay ahead of nefarious actors and ensure they stay relevant in an increasingly virtual, mobile and hyper-connected world.

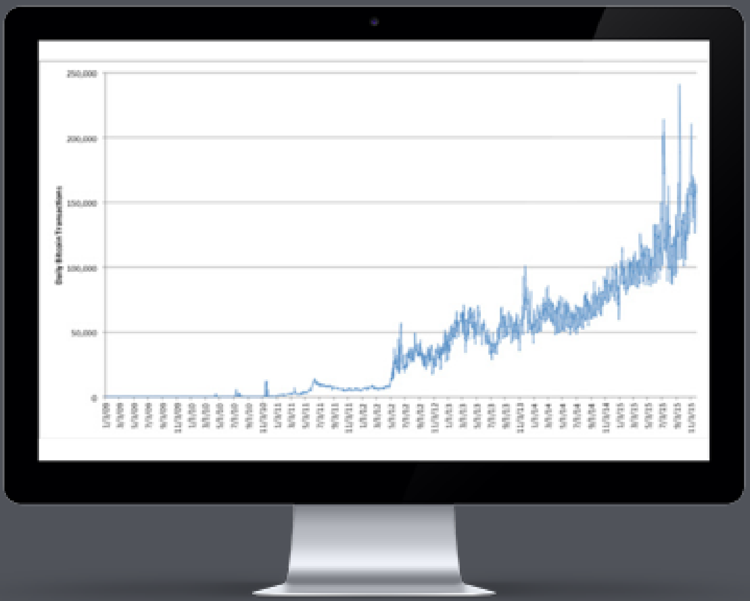


Exhibit 1: Daily bitcoin transaction volume

Source: https://www.quandl.com/data/BCHAIN/NTRAN-Bitcoin-Number-of-Transactions

Transaction volumes have been growing at breakneck speed, and the demand from all sides is increasing. There are plenty of black market outlets, but there also many legitimate commerce sectors that are embracing new cryptocurrencies, even if the methods might fall into something of a grey market. For example, a clothing retailer might accept bitcoins for a sale that it then trades with a technology vendor for new PCs or software. In the process, it immediately turns stock into value to defray business cost. But here's where it gets a bit grey. It might be able to do this without paying taxes. Even the property sector, which comes with many Anti-Money Laundering (AML) risks, is embracing cryptocurrency for payments. Significant sums are changing hands, and AML departments need to be concerned.

For retailers, cryptocurrency could allow them to go on the offensive, pushing into new markets. For others, it enables a defensive strategy to protect market- or mind share, particularly with millennials and 'digital natives'.

The following kinds of operations are fertile ground for cryptocurrency:

- Clothing and music retailers
- Art dealers
- Casinos
- Property agencies
- Restaurants and coffee shops
- Hotels
- Investment funds, including dedicated bitcoin hedge funds
- Universities
- Financial Institutions that accept bitcoin deposits
- Charities and advocacy groups

The upward trend is clear, but cryptocurrency has not fully disrupted the established or legitimate world just yet. Nonetheless, there is another indication of the cryptocurrency insurgency - the level of venture capital that has flooded the market in recent years.

Bitcoin and cryptocurrency has seen significant capital infusions, with investments by venture capitalists reaching US$361 million in 2014. As of November 2015, cryptocurrency startups have raked in US$481 million, for a total of $940m VC investment since its meager beginnings in 2012.

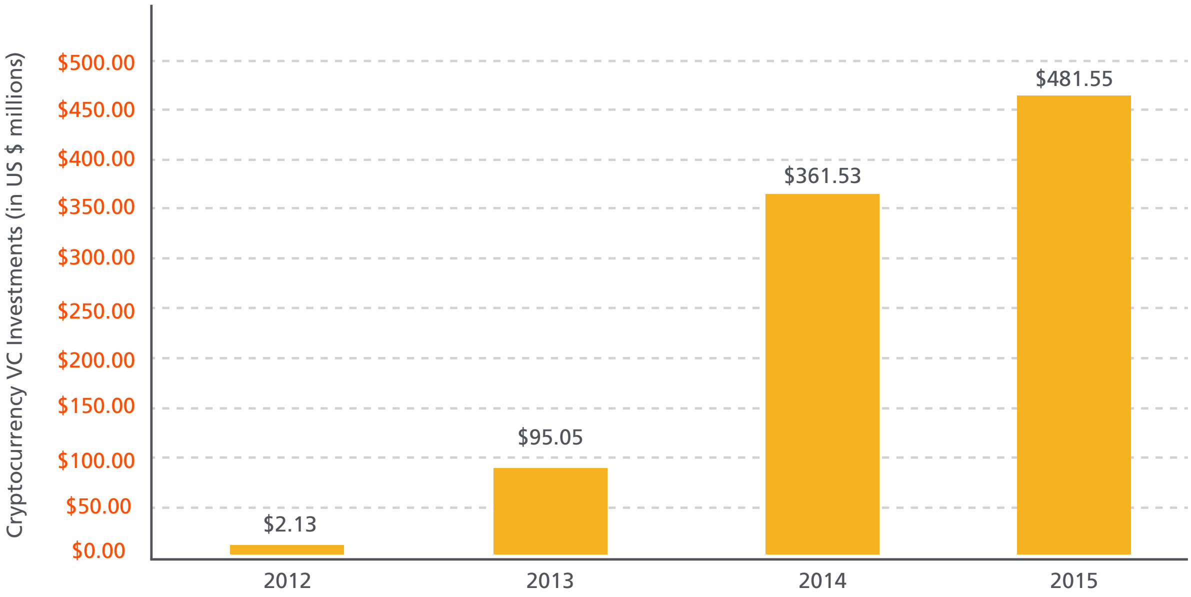


Exhibit 2: Bitcoin venture capital investments 2012-2014

Source: Coin Desk, Bitcoin Venture Capital chart (http://www.coindesk.com/bitcoin-venture-capital/) The Risks of Cryptocurrency

Bitcoin transactions are decentralised - validated by a distributed ledger or blockchain. There is no centralised route for transactions for monitoring, screening or CDD. There are no established transaction networks like SWIFT or NACHA supervising the network, but the distributed ledger is publicly available, so the transactions are recorded. Even so, the participants in the transactions are semi-anonymous (or pseudonymous) and they can use electronic tools to disguise themselves further, which can lead to trouble.

Potential financial crime risks span compliance, money laundering, fraud and cyber threats. Financial institutions need to consider and understand each risk individually and then in aggregate.

Compliance risk

Although cryptocurrencies are new, AML risks in payments or alternative remittance are not. Hawala and various money services businesses, stored value and "anonymous" prepaid instruments, and SMS (Short Message Service) payment are all familiar risks to AML departments. Money Service Businesses or Money Value Transfer services, in their various form are among the highest risks for both money laundering and terrorist finance. But cryptocurrency presents new challenges and opportunities for financial crime.

In its 2012 Typology update, the Australian regulator, Austrac, demonstrated the need for financial institutions to focus on the interface between virtual and fiat currency. From the perspective of a financial institution, this means monitoring the flow of funds through a customer account on a risk basis, covering the risk associated with the instrument of exchange, the counterparty, the countries involved and the value of the transaction.

Accurate assessment of this risk means financial institutions must have insight into their counterparties-not just bitcoin exchanges, but corporate customers that accept bitcoins as a material source of revenue, such as art dealers, property dealers, and precious stone dealers. Monitoring the source, destination and value of funds through accounts is an important aspect of ongoing due diligence, especially where the potential source of funds could be the proceeds of crime.

The anonymity of bitcoin transactions is a key consideration, and there are a variety of digital tools criminals use to disguise the participants further and the net trade from point A to point B. As a result, transparency and monitoring at the entry and exit is the key (see Exhibit 3).

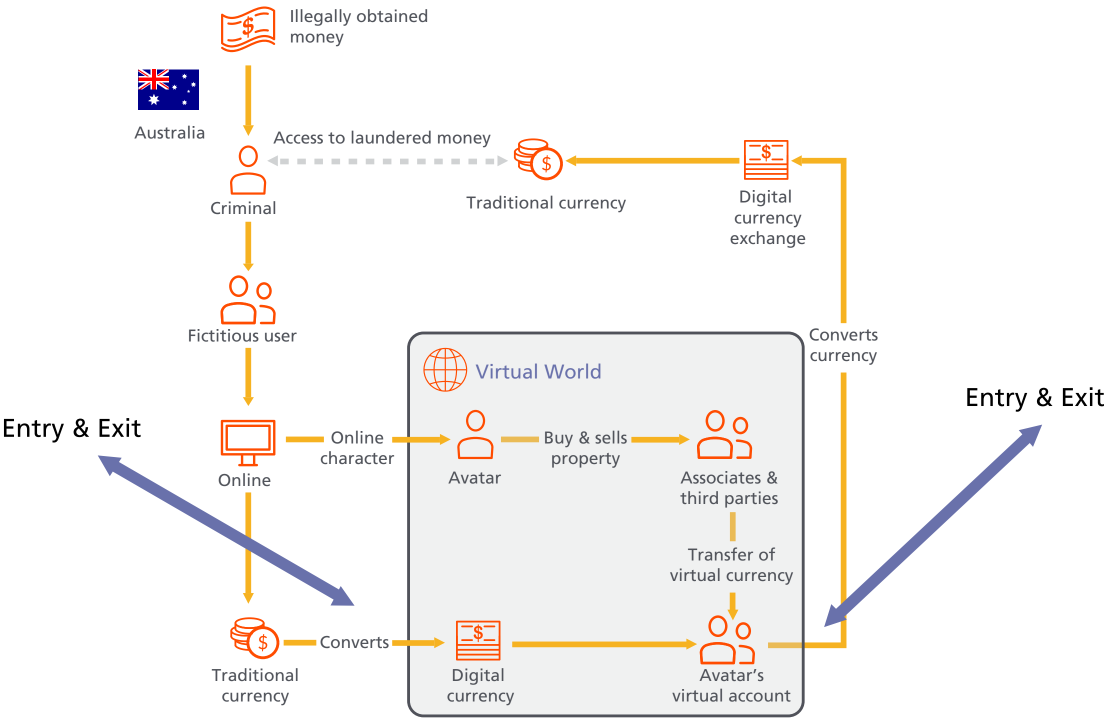
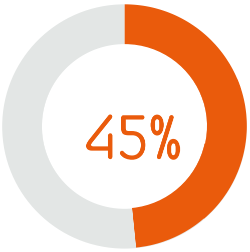


Exhibit 3: Virtual Currency, Typology Example

Source: AUSTRAC Typology Report, 2012

Customer Due Dilligence (CDD) - particularly for commercial customers - is another key aspect of the compliance challenge. Because of the ability to easily convert between virtual and fiat currency, an obvious focal point for laundering, bitcoin exchanges are high risk. Even when there is a clear understanding of the nature of the business and the associated risk, the beneficial ownership of the exchange is a key consideration. In the UK, the Financial Conduct Authority is looking into how blockchain technology can be harnessed to document and authenticate CDD activity. In a speech in early 2016, the FCA's Director of Strategy and Competition, Christopher Woolard, said the Authority was keen to explore how blockchain could be used by businesses for KYC and AML efforts.

Fraud and credit risks



45% of bitcoin exchanges globally have already failed or gone insolvent

In the short-lived, high-growth bull market of global cryptocurrency, some casualties are to be expected. However, the frequency of failure and the small army of deposit-holders and creditors who are out of pocket are deeply concerning. The volatility of bitcoin value has been a factor in losses, but a significant cause of this failure is outright theft. Bitcoins have been stolen from exchanges along with associated private key data that enables the transfer of the bitcoins anywhere on the planet.

The Bitcoin exchange nominally covers the resulting credit loss, but in too many cases the financial institutions and account holders bear the losses.

The Trendon Shavers case illustrates how classic frauds such as Ponzi Schemes can remain alluring when wrapped up in shiny new digital clothes. While Shavers is currently awaiting sentencing for Securities fraud and Wire fraud, this case is a strong indication of how existing fraud typologies will migrate to new modalities.

The categories of fraud losses are substantial and wide ranging (see Exhibit 4).

2013	US Department of Homeland Security seizes Mt Gox Exchange's funds at Dwolla
2013	Flexcoin, based in Alberta, Canada, suffers theft of $600,000 worth of Bitcoin
October 2013	Inputs.io hacked twice: $1 million stolen
December 2013	PB of China prohibits Chinese Institutions from accepting Bitcoins
2014	NAB Closes accounts with ties to Bitcoin
2014	HSBC refuses to serve a hedge fund with ties to Bitcoin
February 2014	Mt Gox files for bankruptcy in Tokyo: $350 million in Bitcoins stolen
February 2014	Silk Road 2 has $2.7 million stolen from escrow accounts
November 2014	Sheep Marketplace: $100 million of stolen illicit goods discovered
January 2015	Coinbase launches the first regulated Bitcoin exchange
February 2015	Chinese exchange BTER loses $2 million to hackers

Exhibit 4: Cryptocurrency losses as a result of fraud

Source: BAE Systems research of publicaly available information

The money laundering risks that come with online gambling are well known. But paying, playing and cashing out using cryptocurrency presents a new level of anonymity. Some online casinos only deal in cryptocurrency and make themselves available on the shadowy TOR network. Conveniently for cyber criminals, in the world of cryptocurrency there is no distinction between domestic and international payments because it's peer-to-peer. There are no international borders - only a mix of copper, fibre, bits and ether - the native playground for cyber criminals.

The cyber risks of cryptocurrencies

The 2014 Interpol Internet Organised Crime Threat (IOCTA) report noted that, since, "the takedown of the first E-Gold in 2009, and subsequently Liberty Reserve in 2013, has resulted in a growing level of distrust in centralised schemes as cyber criminals are increasingly adopting cryptocurrencies. Bitcoin is beginning to feature heavily in police investigations, particularly in cases of ransomware and extortion."

Bitcoin-stealing malware has become a blood sport for both personal and corporate users. During the period of rapid bitcoin appreciation in 2013 in particular, new bitcoin-stealing malware boomed, with attacks most commonly aimed at bitcoin wallets and the compromise of private keys. Other common malware hijacks computing resources for mining bitcoins, which earn bitcoins as payment, though the yield for that type of exploit appears to be on the decline.

Hacks like those at Mt Gox, Flexcoin and Sheep Marketplace have all resulted in the disappearance of bitcoins valued in the hundreds of millions of dollars. In the case of Mt Gox, the exchange itself collapsed into insolvency, leaving creditors (including financial institutions) and account holders carrying the loss. In some cases, the precise beneficial ownership of the exchanges has been unclear, and in some circumstances the 'hackers' conducting the theft, and the 'beneficial owners' of the exchange being attacked, could be one and the same.

How to protect your financial institution

For financial institutions, bitcoin and the underlying blockchain technology carry a mix of opportunity and risk.

Many financial institutions adhere to the recommendations of the European Banking Authority, are waiting a comprehensive regulatory framework. Others follow the guidance of the New York State Department of Financial Services, which provides sensible protections for financial institutions and their customers and clear requirements for virtual currency business.

There are a few essential takeaways that financial institutions should take to heart:

- **Implement risk models** associated with bitcoin and other cryptocurrency entities, spanning direct and indirect exposure to AML, fraud and cyber risk

- **Conduct ongoing monitoring** of bitcoin regulation and best practice requirements in all relevant jurisdictions. Such a monitoring program should include:

    - Vigilance on counterparties regarding corporate customers accepting business from bitcoin entities and financial counterparties or intermediaries accepting bitcoin deposits
    - Monitoring of funds flows through customers and counterparties

- **Monitor public lists** of licensed bitcoin exchanges, which will help recognise unlicensed exchanges, and help in identification of Beneficial Ownership

- **Build robust KYC/CDD** on licensed bitcoin entities, including beneficial ownership

    - For example, determine whether these counterparties perform risk assessment of the public bitcoin Ledger (i.e. perform risk assessments on the source [history] or destinations of bitcoins held by depositors)

- **Undertake risk media monitoring** of bitcoin entities, beneficial owners and corporate customers accepting bitcoin

- **Evaluate cyber threat readiness** of corporate business accepting bitcoins

Conclusion

Cryptocurrency and the enabling distributed ledger technology (DLT) that comes with it are potential game changers, not just in payments and transaction banking, but across a growing set of market instruments including Lending, Securities and Trade Finance.

Bitcoin, the best known, and most widely accepted, of the 200 currently available cryptocurrencies is still only regulated in a small minority of countries. It is a stellar international business opportunity but it is also a systemic target for criminals both online and offline and continues to pose complex risks for any who wish to embrace its undoubted opportunity. Cases such as E-Gold, Liberty Reserve and The Silk Road and others have given us clear direction on how this narrative can evolve without adequate safeguards. They also demonstrate how risk can rapidly move from one means of exchange to another, and potentially from one cryptocurrency to another in the future.

These cases expose the vulnerability of the financial system to misuse, particularly at the point of exchange. They show how small risks on the financial system, can quickly evolve to material risks, as organised criminals appropriate and launder billions of dollars through the financial network, and countless borders, with astonishing speed and ease.

Financial institutions need to prepare and protect themselves against both direct and indirect vulnerabilities. By understanding the AML, fraud and cyber risks associated with cryptocurrency and by monitoring the evolving guidance, registers (for example of licensed bitcoin businesses), and attack vectors. By integrated monitoring of social and risk media in relation to the activity of their own account holders – a financial institution can more effectively mitigate cryptocurrency risk.

Prevention is better than cure, and in some cases discretion may yet remain the better part of valour.

"Fortune favors the prepared mind" Louis Pasteur

We are BAE Systems

We help nations, governments and businesses around the world defend themselves against cyber crime, reduce their risk in the connected world, comply with regulation, and transform their operations.

We do this using our unique set of solutions, systems, experience and processes - often collecting and analysing huge volumes of data. These, combined with our cyber special forces - some of the most skilled people in the world, enable us to defend against cyber attacks, fraud and financial crime, enable intelligence-led policing and solve complex data problems.

We employ over 4,000 people across 18 countries in the Americas, APAC, UK and EMEA.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
Arjaan Office Tower
Suite 905
PO Box 500523
Dubai, U.A.E
T: +971 (0) 4 556 4700

BAE Systems
1 Raffles Place #23-03, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST

CESG Certified Service
Cyber Incident Response

CPNI
Centre for the Protection of National Infrastructure

BAE Systems, Surrey Research Park, Guildford Surrey, GU2 7RQ, UK
E: learn@baesystems.com | W: baesystems.com/businessdefence
linkedin.com/company/baesystemsai
twitter.com/baesystems_ai