WHITEPAPER

TACKLING CRYPTO-CURRENCY FRAUD

» and monitoring market abuse on blockchains

TABLE OF CONTENTS

01 **ABSTRACT** 5

02 **EXECUTIVE SUMMARY** 6

03 **BLOCKCHAIN AND BITCOIN BACKGROUND** 7

04 **BLOCKCHAIN AND BITCOIN MARKET ABUSE** 8

05 **THE ROLE AND BENEFITS OF AUTOMATION** 10

06 **THE FUTURE FOR BLOCKCHAIN SURVEILLANCE** 12

07 **ABOUT B-NEXT** 14

The blockchain revolution is developing rapidly and is garnering significant interest in the financial sector. However, a lack of regulation or standards leaves blockchains exposed to market manipulation. This paper explores how blockchain surveillance can be achieved and how blockchain ‘safe’ areas can be identified, protecting participants from market abuse.

01
EXECUTIVE SUMMARY

How can you tackle crypto-currency fraud and market abuse on blockchains?

The blockchain revolution is developing rapidly and is garnering significant interest in the financial sector. However, a lack of regulation or standards leaves activity on blockchains exposed to fraud. Crypto-currencies including Bitcoin run on blockchains and reports of fraud and manipulation have led to the launch of criminal investigations. Such reports have highlighted a need to monitor for market abuse on blockchains.

The task of monitoring blockchains, however is fraught with complexity. The anonymity inherent in blockchains makes it difficult to trace individuals and to identify safe areas. Other vulnerabilities include exposure to market manipulation due to poor understanding of the risks involved in trading crypto-currencies. In addition, many exchanges used to store Bitcoin have been shown to be highly vulnerable to hacking and theft.

This is where automated surveillance has a valid role to play. This paper explains how automated surveillance systems offer an efficient and practical means of monitoring blockchains.

This can be achieved in two stages:

- Rating engines can be used to help market participants to identify the most reliable entities on blockchains.
- Surveillance systems can be combined with rating engines, allowing you to monitor fraudulent activity on blockchains by generating alerts on trading frequencies, holding periods and watchlist/restricted lists.

This form of surveillance helps to protect participants from fraud on blockchains, while making transactions on blockchains safer.

02
BLOCKCHAIN AND BITCOIN BACKGROUND

Blockchain technology is attracting significant attention in the capital markets and is now drawing attention from regulators. However, despite widespread awareness of blockchains, they are still poorly understood[1].

What is a blockchain?

Blockchain technology is perhaps one of the most innovative inventions since the internet. It is the technology upon which Bitcoin and other crypto-currencies are run. A blockchain is a distributed ledger technology that records and verifies blocks of digital information. Transactions are recorded by adding new 'blocks' of data to the existing 'chain' of data creating a permanent chronological record of transactions. This makes blockchains resistant to tampering.

Such is the interest in the potential of this technology, accelerated demand is forecast and worldwide spending on blockchain is set to reach $9.2bn by 2021 with a compound annual growth rate of 81.2 %[2]. Research agency IDC, expects accelerated demand for blockchain technology in the regulated financial services industry, due to central banks' interest

What is Bitcoin?

Bitcoin is a digital crypto-currency launched on the internet in 2009. Its inventor is purported to be an individual called Satoshi Nakamoto. Bitcoin runs on blockchains and due to the anonymous nature of transactions, Bitcoin has earned a reputation as the preferred currency for purchasing illicit goods. Bitcoin has experienced significant price volatility making it the subject of much speculative investor activity. While blockchains are inherently secure, activity on blockchains involving Bitcoin transactions, is exposed to manipulation and may be vulnerable to significant market abuse. Blockchains won't disclose the identity of the person you are transacting with. Its anonymity opens up a significant window of opportunity for those intent on fraud or money laundering.

Consequently, there is an urgent need for surveillance to make activity on blockchains safer for legitimate users and to prevent instances of market abuse.

[1] HSBC Trust in Technology (www.hsbc.com/-/media/hsbc-com/newsroomassets/2017/pdfs/170609-updated-trust-in-technology-final-report)

[2] IDC Blockchain Spending Guide (https://www.idc.com/getdoc.jsp?containerId=prUS43526618)

03
BLOCKCHAIN AND BITCOIN MARKET ABUSE

Although blockchains are resistant to tampering this does not make the crypto-currencies that run on them, invulnerable to the many forms of market abuse and manipulation that are familiar among other asset classes.

Market manipulation

Blockchains are vulnerable to manipulation from anonymous fraudsters posing as legitimate participants. Bitcoin, the crypto-currency, runs on a blockchain, however the relatively small Bitcoin market of c.$100 bn[3] can be manipulated by cash rich individuals with ill intent. Inexperienced traders and investors are jumping onto the cryptocoin bandwagon and through lack of expertise, are taking risks on cryptocoins they wouldn't take on other asset classes. Blockchains are at their core, linear databases just like a ledger. While the ‘ledger’ and its copies are secure and exceedingly difficult to hack or tamper with, this does not rule out the possibility of manipulation.

Markets are vulnerable to hacking and theft

The exchanges used to store Bitcoin have been shown to be highly vulnerable to hacking and theft. There have been many instances of Bitcoin being stolen; a recent high profile case involved the theft of over 4,700 Bitcoin worth $64 m from the Slovenian-based Bitcoin mining marketplace NiceHash[4]. The theft involved a sophisticated hack and shortly after the crime, a new Bitcoin wallet containing 4,736 Bitcoin appeared, raising speculation that it contains the missing Bitcoin, however the anonymous nature of the wallet means the owner cannot be easily traced, if at all.

Lack of regulation and possible market abuse scenarios

A general lack of regulation and expertise of the range of possible market abuse scenarios adds to the vulnerability of crypto-currency markets.

Aside from the serious crime of theft, the price of Bitcoin and other crypto-currencies is vulnerable to the same forms of market abuse we have seen in equities and futures markets. Bitcoin wallets are anonymous providing an opportunity to store funds from non-compliant activity covertly or to conceal proceeds from personal account dealing. A lack of regulation to date and price volatility are among the reasons for such

[3] https://coinmarketcap.com
[4] https://www.telegraph.co.uk/technology/2017/12/07/52m-Bitcoin-stolen-crypto-currency-exchange-heist/

vulnerability. With minimal monitoring of Bitcoin trading activity taking place and amid growing concerns small investors in Bitcoin will become victims of market abuse, the US Justice Department has now launched a criminal probe to find out whether manipulation is taking place[5].

The market abuse techniques that may be used to manipulate the price of Bitcoin include:

» Wash trades

These transactions are executed without a change in beneficial ownership or market risk. Such fictitious transactions can send misleading signals to the market regarding demand or supply of a financial instrument. Wash trades can be part of a larger trading strategy aiming to manipulate Bitcoin. Wash trade surveillance should include detection of suspicious activities that are:

- By a certain customer
- By a certain trader
- At a certain venue
- Across multiple venues
- Carried out in a short period of time involving multiple market members (circle trading)

» Spoofing

Spoofing involves placing and cancelling orders quickly before they are executed. Spoofing alters market price spreads by targeting the placement of orders, followed by executing transactions on the opposite side of the market, thereby taking advantage of movements in the price of Bitcoin.

» Layering

Layering creates an artificial market price by placing orders which enhance the order book without the intention of execution.

» Ramping

Ramping scenarios are characterised by the manipulation of the market price which is achieved by executing a large number of transactions or material volume in a short period of time.

[5] https://www.bloomberg.com/news/articles/2018-05-24/Bitcoin-manipulation-is-said-to-be-focus-of-u-s-criminal-probe

04
THE ROLE AND BENEFITS OF AUTOMATION

Automated Surveillance Systems

Automated surveillance systems can alert compliance officers early on by identifying suspicious situations based on a number of pre-defined scenarios. In the case of blockchain surveillance two phases can be applied to identify market abuse:

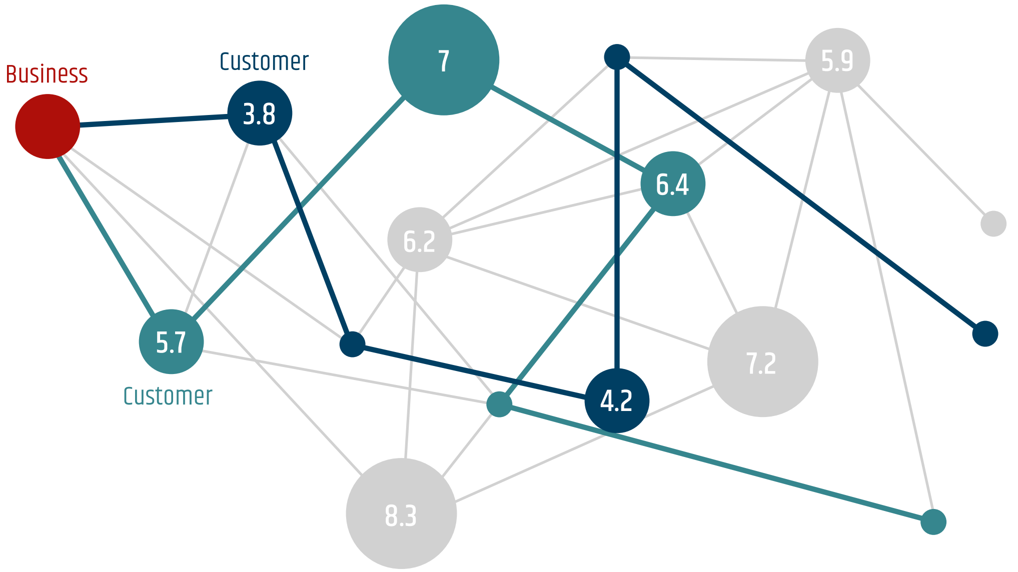


Fig. 1: Blockchain ratings

» BLOCKCHAIN RATING ENGINES

Rating engines have been developed which can be used to shine a light on the legitimacy of anonymous entities on blockchains. With rating systems from providers such as Whitestream[6] an algorithm analyses blockchain traffic to map the Bitcoin network and find blockchain "safe" areas. The system can identify reliable wallets or market participants, while highlighting untrustworthy entities. A rating system is then applied, scoring Bitcoin wallets to help market participants to identify the most reliable entities on blockchains and protect themselves from reputational risk.

» BLOCKCHAIN SURVEILLANCE

Blockchain Surveillance systems such as b-next's CMC:Blockchain Surveillance allows you to monitor fraudulent activity on the Blockchain by generating automatic alerts on trading frequencies, holding periods and watchlist/restricted lists based on the Blockchain rating analysis.

Automated solutions of this kind will typically provide alert analysis including market data, covering trading activity aggregating and analysing data from across all time zones, allowing for cross linking between all parts of a global institution.

[6] https://whitestream.io

The Benefits of Automation

Such is the complexity, magnitude and dynamic nature of the surveillance task, automation is emerging as a viable and practical solution.

The benefits of implementing automated solutions are wide reaching and can include:

- The ability to respond quickly to regulatory changes and reporting requirements
- A reduction in workload and associated costs
- Proactive management of suspicious trends
- Improvements to the quality of market abuse monitoring
- Improvements to risk management and visualisation of compliance oversight
- Increased competitive advantage
- Reduced exposure to risk
- Global monitoring of market abuse and insider dealing behaviour
- Flexibility and scalability to cope with future changes to regulation and new scenarios of market abuse
- Early automated alerts and deep insights into potential incidents
- Unique market and business insights via data held in a harmonised database
- Fast, easy roll-out and go-live
- Intuitive system operation

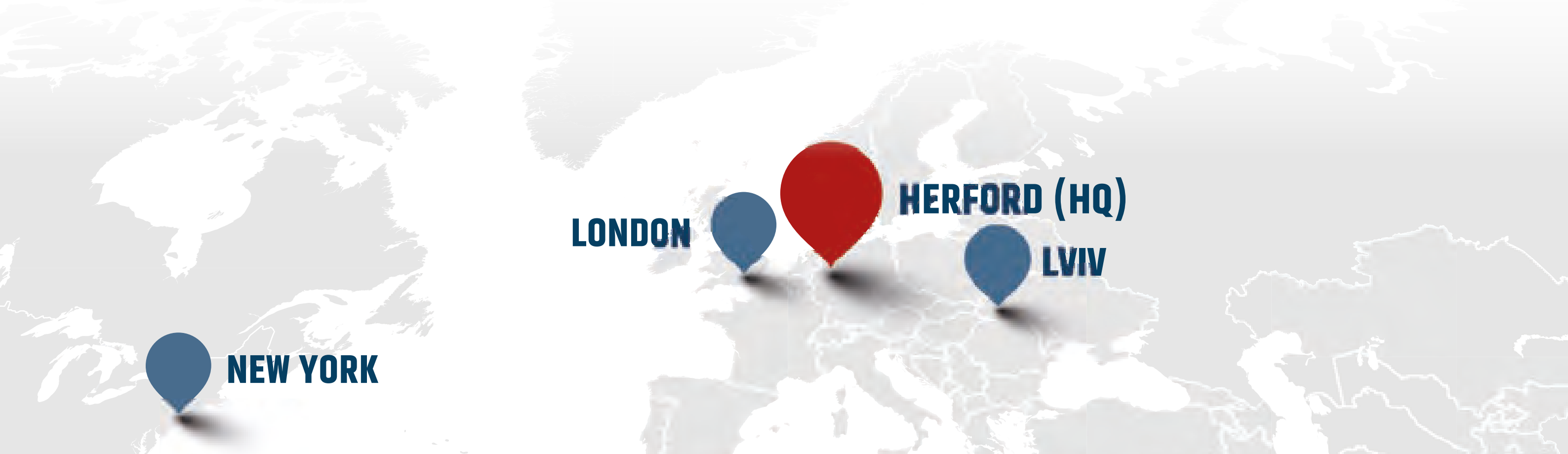
Market abuse is an ongoing threat to legitimate entities on blockchains and while the market waits for regulatory measures, automated surveillance offers a solution and a degree of protection to participants trading Bitcoin and other crypto-currencies on blockchains.

06
THE FUTURE FOR BLOCKCHAIN SURVEILLANCE

Blockchain and Bitcoin market abuse is beginning to come to the attention of regulators. As scrutiny tightens and the full force of regulation and scrutiny is felt, it will become harder for illegitimate entities to conduct market abuse on blockchains. Automated surveillance and rating solutions are ideally suited to the complexity and magnitude of blockchain surveillance tasks. The combined effect of regulation, surveillance and rating systems, will make blockchains safer places for legitimate entities to trade and conduct transactions. And, those intent on manipulation of Bitcoin or other crypto-currencies on blockchains, will have increasingly fewer weaknesses to exploit and fewer places to hide.

ABOUT B-NEXT

b-next is a specialist provider of proven multi-venue, multi-asset class, Capital Markets Surveillance and Compliance software solutions to meet regulatory mandates, manage risk and drive trading efficiencies. The b-next Capital Markets Compliance (CMC) solution is a single integrated compliance platform for **detection of Market Abuse**, **Insider Trading**, **Conflicts of Interest**, **Derivatives/OTC Monitoring**, **Best Execution reporting** and **monitoring of trading activity**. b-next provides clients with options for an onsite or Thomson Reuters Elektron hosted solution. Both offer rapid deployments with pre-built integration for Thomson Reuters Market Data and low monthly investments.



120+
SCENARIOS

b-next's CMC:eSuite solution offers a single integrated compliance platform with over **120 DIFFERENT SCENARIOS** for the detection of market abuse, insider trading, conflicts of interest, FX benchmarking, derivatives/OTC monitoring, best execution monitoring and reporting of trading activity. It supports a diverse range of global clients including banks, brokers, asset managers, exchanges, regulators, funds and energy utilities.

25+
YEARS

A highly focused provider of capital markets solutions for more than 25 years, b-next has a growing international client base, supported by offices in Europe and the US. Our proprietary development team and strong client centric approach ensure that our solution set remains at the leading edge of regulatory change and market best practice.

FOR MORE INFORMATION

VISIT WWW.B-NEXT.COM

Germany
Bielefelder Strasse 12 – 14
D-32051 Herford
+49 5221 99 280 0

UK
80 Coleman Street
London, EC2R 5BJ
+44 20 7489 6430

USA
80 Pine Street, Floor 24
New York, NY 10005
+1 646 437 1026

Ukraine
77/38 Heroiv UPA #401
Lviv 79015
+49 5221 99 280 0

Singapore
2 Marina Boulevard #17-01
Marina Bay Financial Centre Tower 3
Singapore 018982
+65 6809 5217

www.b-next.com