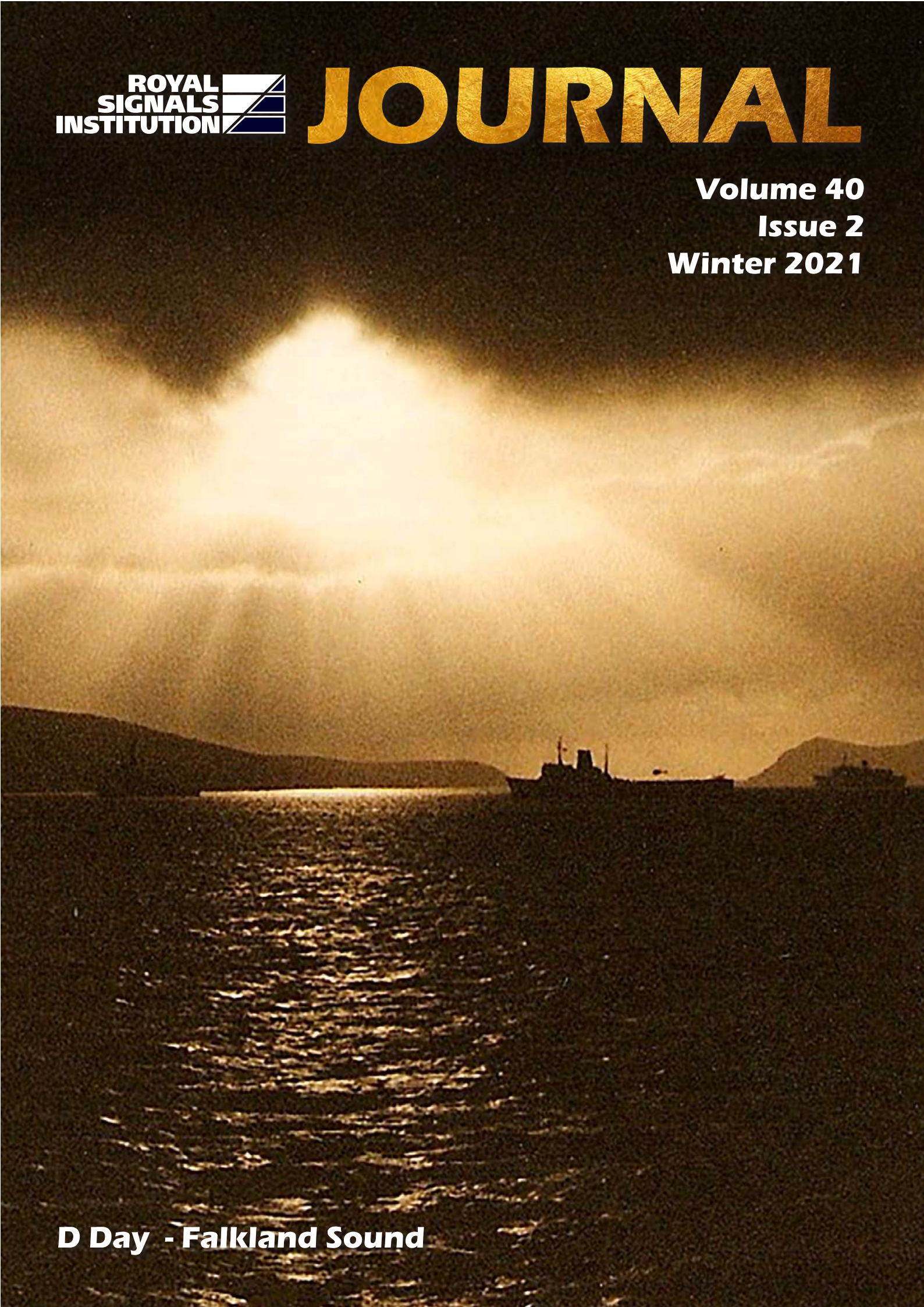
ROYAL SIGNALS INSTITUTION

JOURNAL

Volume 40
Issue 2
Winter 2021



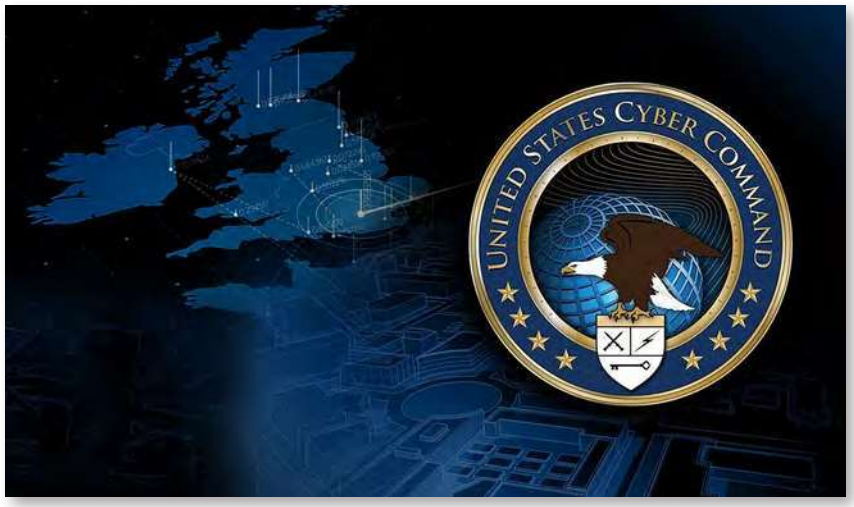
D Day - Falkland Sound

IN THIS ISSUE

RSI CHAIRMAN'S REPORT 4

Brigadier Greg Wilson

RSI NEWS, HONOURS & AWARDS 5



THE TEMPORAL DIMENSION OF 'DEFENDING FORWARD' 12

Alan Mears and Joe Mariani

C2 OF THE POST-DIGITAL HYPER-WAR 20

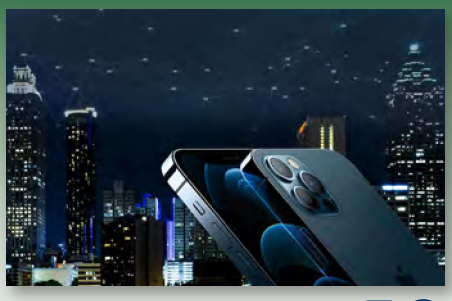
Captain Martin Crilly

FALKLANDS - A DAMNED CLOSE RUN THING 26

Colonel RDK Thompson ...and many others.

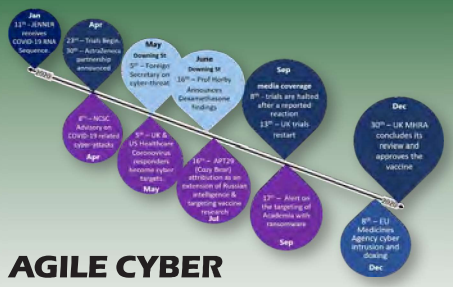
COLD WAR TO HOT PEACE 40

Group Captain Alan Matthews



COVID-19 and UK Networks 52

Simon Saunders, Huw Saunders and Nick Evans



AGILE CYBER REQUIREMENTS FOR VACCINES & THERAPEUTICS 60

Graham Ingram

RECCE OFFICER'S LAMENT 64

Begone Dull Care

CRYPTOCURRENCY ANALYTICS 66

Jonathan Francis Roscoe

STILLE NACHT - tribute to our dead grouse 72

Lieutenant Colonel Guy Meakin

VERY EARLY USE OF WIRELESS IN WWI 74

Andrew Webster

RECOLLECTIONS OF A DIFFERENT SERVICE CAREER 82

Major David Williams

SILVER AND SILVERSMITHING 94

Lieutenant Colonel M S Norbury

CHRISTMAS IS COMING – HEAD FOR ALSACE! 100

Tastevin

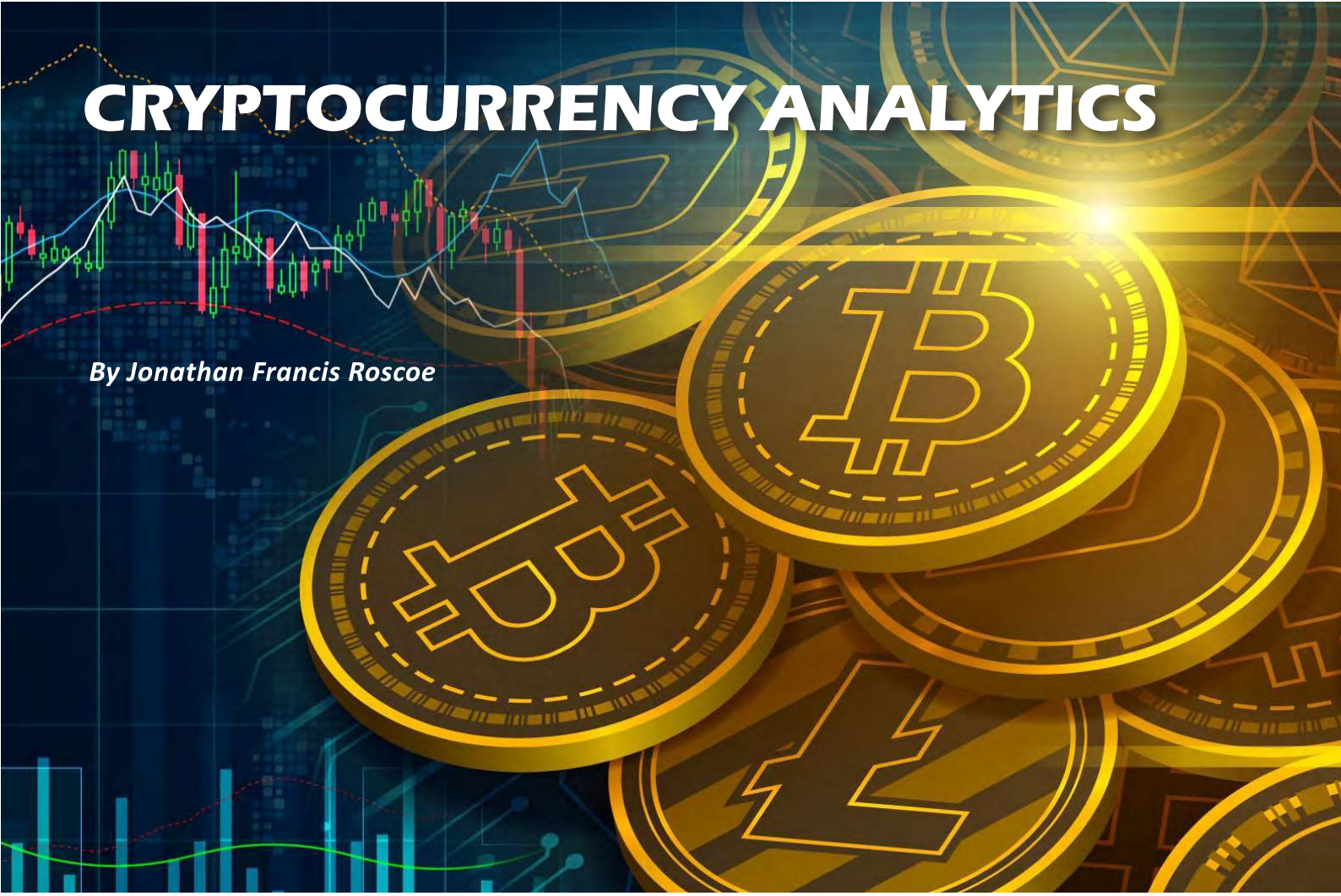
Other Articles

Book Reviews 104

Remembrance 111

HQ Royal Signals 112

CRYPTOCURRENCY ANALYTICS



By Jonathan Francis Roscoe

Dr Jonathan Francis Roscoe is a research manager in the Emerging Security Paradigms group of BT Applied Research where he has worked on developing next generation security mechanisms for enterprise applications. Jonathan has a PhD from Aberystwyth University in statistical methods for prostate cancer detection with TRUS/MR imaging.

His areas of interest include machine learning, open source intelligence and visualisation. His work in blockchain analytics was awarded the TEISS award for Information Security and the Institute of Telecommunication Professionals Innovator of the Year award.

Introduction

It has been over 10 years since Satoshi Nakamoto introduced blockchain technology in the form of Bitcoin, a decentralised, tamper-resistant and cryptographic digital currency. Although usage has remained modest it spawned a whole ecosystem of cryptocurrencies, reaching a peak market value of 800 billion USD.

Blockchain is a form of distributed database that resists tampering and enables trustless transactions between multiple participants, first discussed in the Institute of Telecommunication Professionals' Journal in 2017 [1]. Transactions between participants are conducted through cryptographic signatures to securely and verifiably record exchanges.

One of the biggest misconceptions around blockchain is that it is an anonymous means of conducting financial transactions. This article looks at the how the blockchain can be unravelled to provide insight on the activity within and also, explores some notable incidents, highlighting work that was done to assist law enforcement investigations.

What is Bitcoin and why is it relevant?

Bitcoin was a response to the role of banks in the financial crisis whose centralised and opaque behaviour were seen as a significant weakness of traditional banking. The solution provided by Bitcoin is a decentralised system that doesn't rely on trust in authoritative entities.

It was the first example of blockchain technology – which utilises cryptographic techniques to ensure no single entity can gain control of the network. It is a public, permissionless peer-to-peer system.

Bitcoin now compromises just half of the global cryptocurrency market cap, as competing alternatives with different technical characteristics that promise different functionality such as computational efficiency, security, anonymity and capability. These alternatives number in the thousands, though just a handful are used in any scale.

It should be noted that not all blockchains are the same and not all of them are intended to replace currency. For an overview of the technology behind blockchain in its various forms, see the National Institute of Standards and Technology (NISTIR 8202) technology overview [2].

Cryptocurrencies in Cyber Security

Cryptocurrencies are now of major significance to cyber security. For the operators of ransomware, Bitcoin is a desirable payment option due to the ease of access for victims. Cryptocurrencies are now easily purchased through mainstream exchanges with credit card and mobile apps.

Similarly, dark net markets often utilise Bitcoin and other cryptocurrencies as unlike other payment methods, the censor-resistance of the technology means it is not possible for law enforcement to shut down payments.

These markets are known for the sale of a variety of illicit physical goods such as narcotics and stolen merchandise as well as virtual goods or services such as confidential data leaks, malicious software and botnet rental.

Whilst Bitcoin lacks anonymity, it is relatively easy and cheap to obfuscate the source and destination of funds by making a series of convoluted transactions. The presence of unregulated exchanges also enables easy conversion to fiat currencies without appropriate checks.

However, despite negative media perceptions, there are many legitimate businesses utilising cryptocurrencies. For these organisations, ensuring they perform due diligence with regards to anti-money laundering and related regulation is a significant challenge. Analysis of incoming funds can allow them to identify proceeds of crime and understand the level of risk for associated users.

Variants of blockchain, more broadly referred to as distributed ledger technology (DLT) are also being trialled in a number of industries. Applications such as supply chain management, document verification, intelligence sharing, and licensing make it a compelling technology in all sectors. These enterprise blockchain solutions are private and more restricted variants of the technology that provides the same security that Bitcoin offers, with a lower overhead and greater governance.

This presents a broad variety of needs around being able to understand the activity on distributed ledgers, to support cyber security investigators and protect users.

Deanonymising the blockchain

The blockchain contains a public record of all transactions, each transaction shows the source and destination of any funds. The entire history of a coin can be retrieved and cryptographically verified, this prevents counterfeiting and fraud, but also introduces a major privacy concern. Each transaction must reference the output of a previous transaction, resulting in a chain that provides a lineage for every coin as shown in Figure 1.

Transactions specify inputs (in the form of signed references to previous outputs) and outputs (in the form of one or more public keys). These public keys don't necessarily have a 1-to-1 mapping to individuals, and privacy conscious users will use many keys to try and hide their activity.

Visualising transaction activity

Working with several security teams, Applied Research has developed Nexus, a new graph visual analysis tool backed by state-of-the-art machine learning algorithms to provide novel insights to investigators. The tool has already been deployed for internal BT cyber threat hunting operations.

Graphs (not to be confused with charts) are made up of nodes and edges and can be configured to model potentially any aspects of data. There may be multiple types of nodes and edges and each can have unique sets of attributes. An edge represents a relationship of some form between a pair of nodes, for example traffic from Node A to Node B in the case of a computer network, or an affiliation between Person A and Person B in a social network.

Many algorithms exist to efficiently analyse such graph structures, for example to understand the paths between two points, the connectivity, or identifying communities of nodes.

Graph analytics can be used to focus analyst attention on particular subsets of data which are of interest through explicit user-driven filtering, as well as filtering and prioritisation based on calculated graph metrics. Through graph styling, the interactive visualisations produced by Nexus also offer an effective means for analysts to explore large scale data sources, expanding their hunt if required.

Using Nexus, a model of the connections between datapoints can be generated. This enables useful visualisation of key relationships and interactions. Nexus was used in cryptocurrency investigations here to visualise the flow of transactions from the blockchain ledger. This can help provide attribution and confirm the source and destination of funds.

From the ledger, graphs can be built showing the flow of funds between these addresses. To do this, a bipartite graph that links address nodes to transaction nodes is used. However, transactions may be more complex than shown in Figure 1, with multiple inputs and outputs. This results in complicated patterns of activity and, depending on the objectives of the user, a variety of patterns in the graph visualisation stand out. These patterns are known as graph motifs and serve as unique indicators for particular activities Different graph motifs, corresponding to different categories of activity are a powerful way of classifying different types of activity by users on a blockchain are shown in Fig 2 (see page 68).

Figure 1: References between transactions

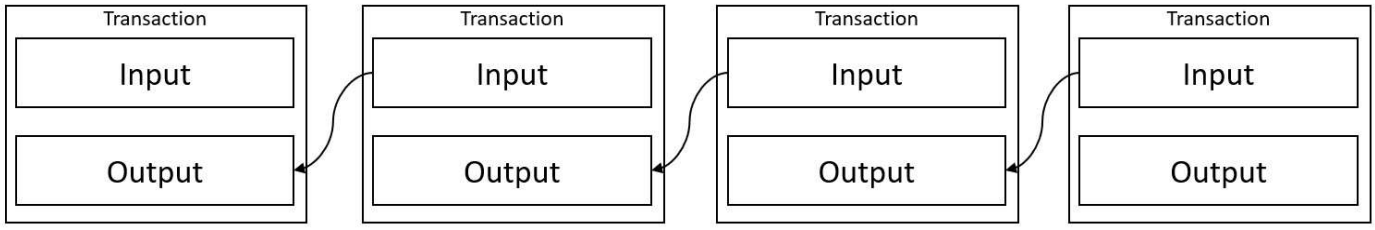
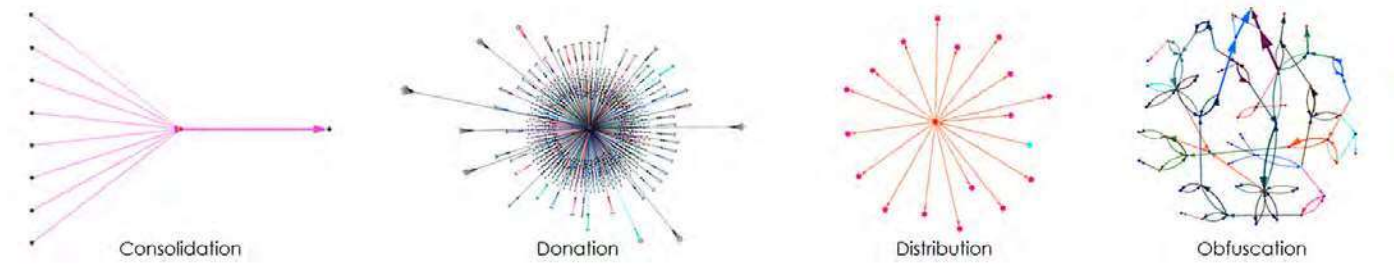


Figure 2: Categorisation of blockchain activity by graph motif



There are a wide variety of cryptocurrency users such as exchanges, marketplaces, private vendors/purchasers, microtransaction, payment processing, etc. The way these users interact with one another can become a tell-tale characteristic for identifying common activities and attributing chains of transactions to entities.

However, for a human analyst investigating the blockchain, these patterns may not be readily apparent due to the drastically increasing complexity of interactions, as can be seen in Figure 3 which shows a graph of funds sent between different Bitcoin addresses.

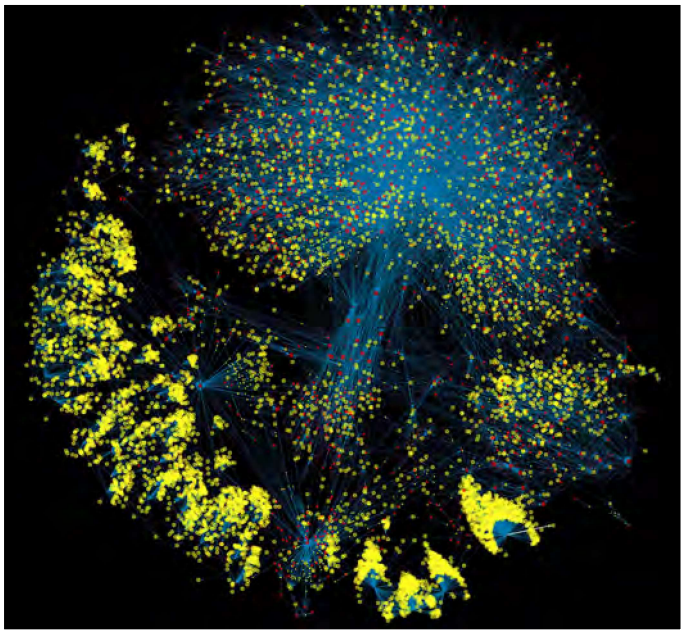


Figure 3: Graph representing funds sent between different Bitcoin addresses

This is where machine learning has a role in automatic identification of suspicious activity. If an analyst has identified initial blockchain activity of interest (such as an address belonging to a darknet market), then unsupervised techniques such as clustering are a powerful mechanism for identifying similar activity [3].

Supervised learning (machine learning with training data) is difficult to apply to cryptocurrency due to a lack of ground truth (data known to be correct through prior observation). By utilising open-source intelligence freely available data from the public Internet and manually interacting with service providers analysts can construct a database of known addresses. This technique has been proven in literature to be effective for deanonymizing transactions [4]. Unfortunately, these databases are often sparse and with almost 500million addresses in use and only approximately 37% of economic relevance [5], supervised learning remains a difficult task. However, open-source intelligence does enable us to identify clusters of the blockchain closely linked addresses that have at least one known association with a specific service or actor. This is vital for analysis of cryptocurrencies.

Case Studies

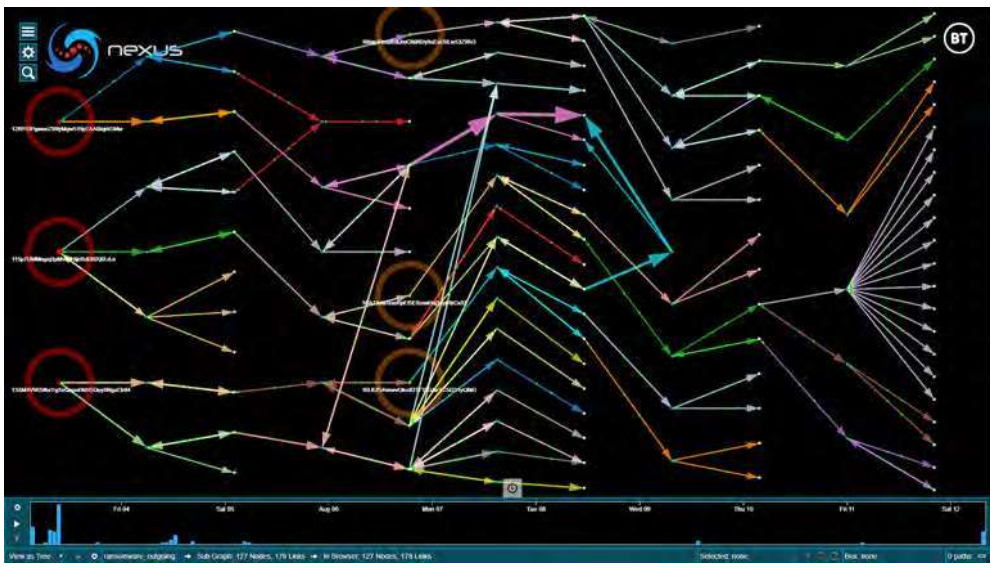
These analytics capabilities have been applied to a number of real-world use cases, supporting threat investigators and law enforcement in their fight against cybercrime.

WannaCry

During the 2017 WannaCry attack (known in the UK for its severe impact on the NHS and countless other organisations worldwide) Nexus was used for real-time monitoring, allowing analysts to visualise frequency and size of ransom payments to perform threat assessment.

In the initial days of the attack, a large number of payments to addresses identified by intelligence teams was observed. Comparing the transaction data to revelations regarding affected organisations, it is clear that only a fraction of infected machines led to a payment. Figure 4 shows a visualisation of funds being moved

Figure 4: Visualisation of the movement of funds during the WannaCry attack



CGI

Advise, build, operate

CGI helps defence clients deliver secure, mission-critical IT solutions from the back office to front-line operations.

CGI is committed to supporting our Armed Forces and are proud to hold a Gold Award in recognition of our support of the Armed Forces Corporate Covenant.

ARMED FORCES COVENANT

EMPLOYER RECOGNITION SCHEME

GOLD WINNER 2019

For more information on CGI in defence please visit
www.cgi-group.co.uk/space-defence-intelligence

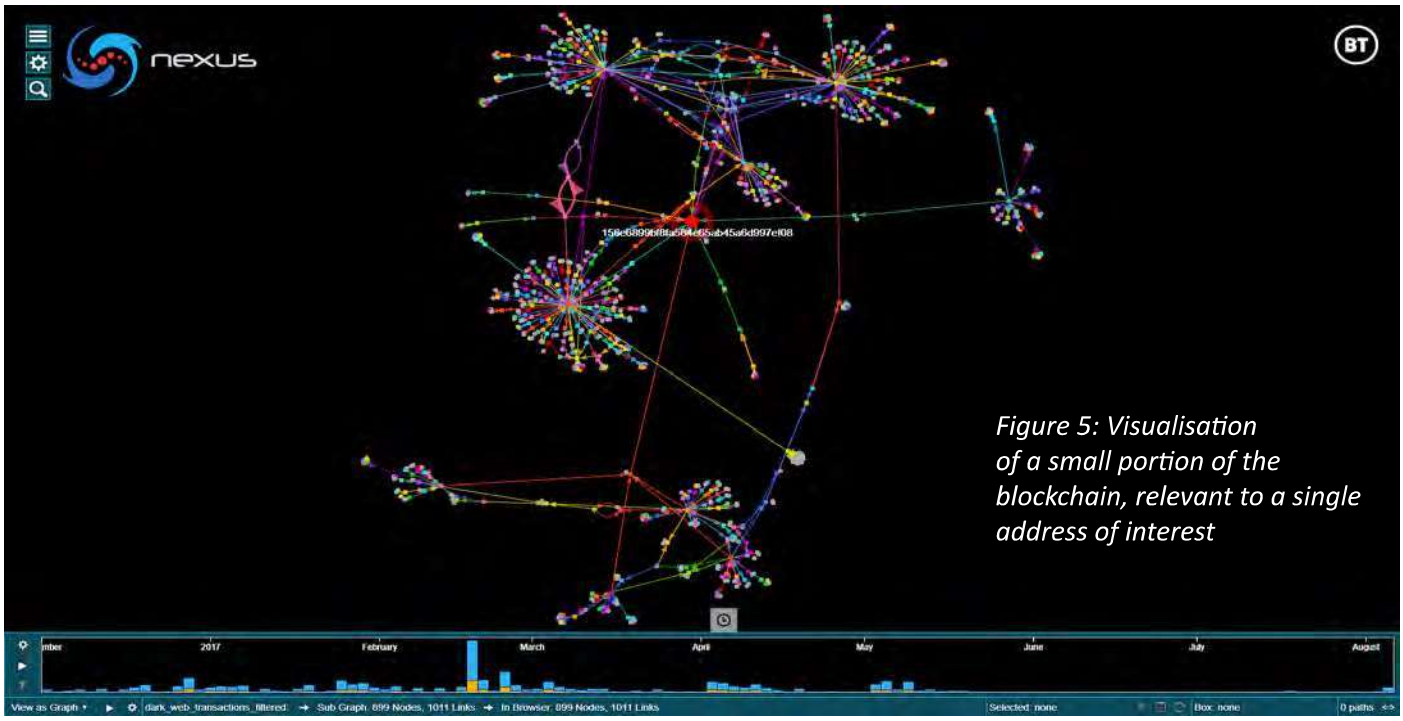


Figure 5: Visualisation of a small portion of the blockchain, relevant to a single address of interest

from WannaCry addresses to identified cryptocurrency exchanges. On the far left, the three addresses operated by the perpetrators of WannaCry are highlighted red. The initial distribution of funds to currency exchanges (highlighted orange) and final distribution amongst other users (on the right) is clearly visible. In this case, the malware was rendered ineffective after a few days, but a small number of payments were still seen.

Once the analyst identified nodes of interest, a clustering algorithm was applied to identify similar nodes based on features (such as transaction frequency, value, etc). In Figure 5, three other nodes (blue) were identified as being in the same category as the target.

Later, when the payments were moved from the ransom wallets, a network of transactions as the funds were mixed between linked accounts in some form of money laundering was seen. This pattern, visualised in Figure 6, enabled us to inform those who may be in receipt of the malware funds.

Malicious software vendors

In a recent security incident, Tier-1 US banking institutions were targeted, with compromised customer accounts being accessed and modified. The IP addresses from which the attack originated where analysed a larger number of DNS requests were found. The attack was being carried out with malicious software that had a “phone home” feature for licensing purposes. From this, a website selling services and software for brute forcing passwords and modifying user credentials was identified. The site included a bitcoin address for payments.

Given the vendor’s address, several transactions were identified. From the linked addresses, features such as value, frequency and timing to capture patterns in behaviour and association were derived. K-means clustering was used to group addresses based on their transactions. This process partitions the addresses into discrete groups based on the similarity of the features.

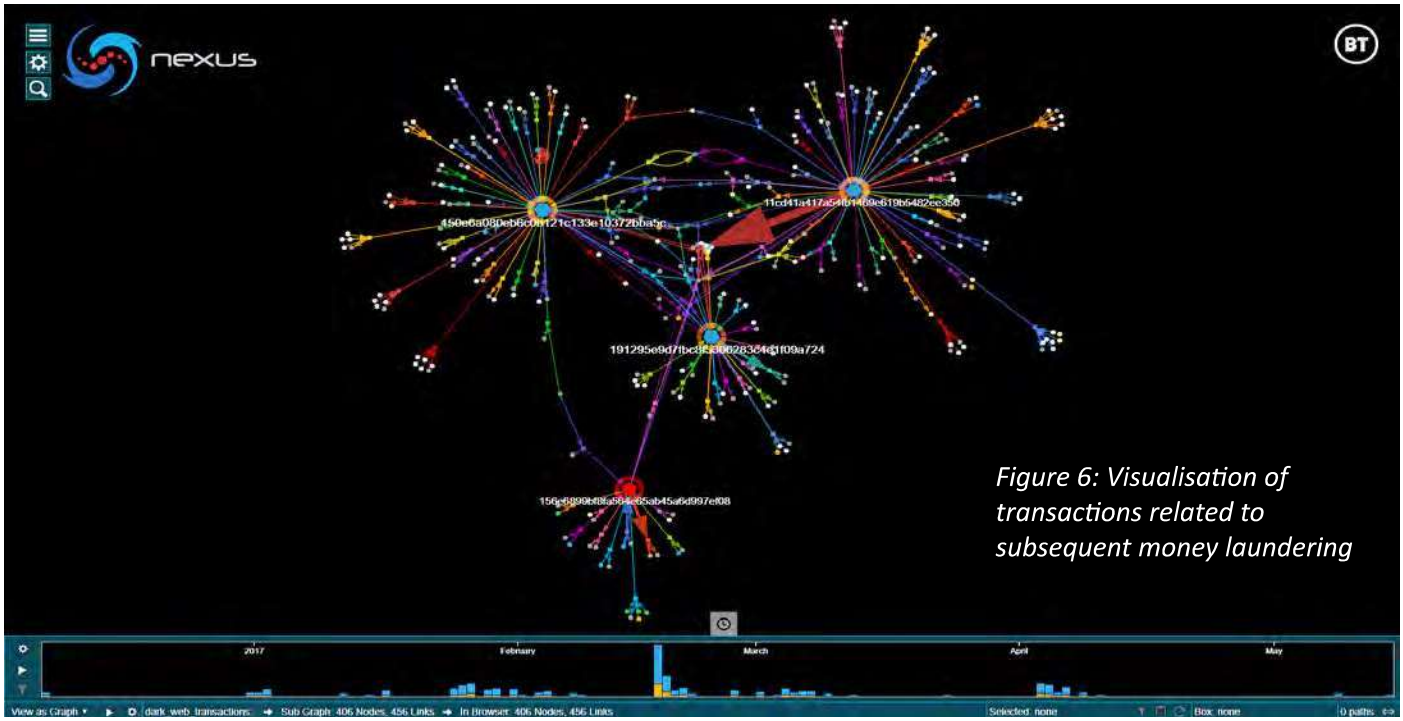


Figure 6: Visualisation of transactions related to subsequent money laundering

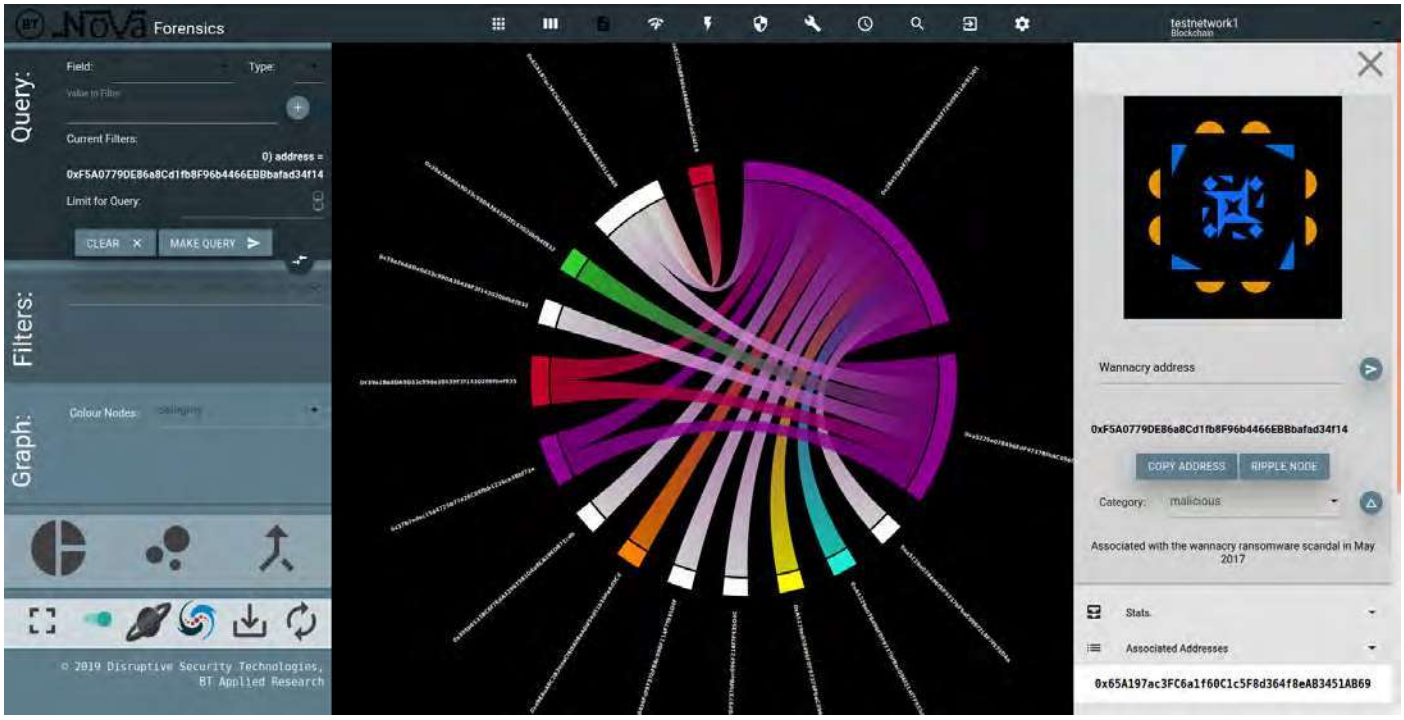


Figure 7: "Nova" the blockchain analytics dashboard

The results of clustering sorted each bitcoin address in the vicinity of the target into half a dozen distinct groups. This highlighted groups of nodes with similar behaviour, and it enabled human analysts to identify groups likely to be patrons, exchanges and money laundering services. Of significance was the group containing the initial vendor address, which contained three other addresses.

These additional addresses were investigated by intelligence teams which revealed other websites supplying the same software. Each site provided new information on the vendor and went towards building a profile of two individuals responsible for the creation and distribution of the malicious software.

The information was fed back to police cybercrime teams and formed evidence in a criminal investigation.

Blockchain Analytics for Enterprise

The blockchain analytics capability described was developed to support law enforcement in forensic analysis of cybercrime involve cryptocurrencies, however the technology has been extended work to support all manner of blockchain users.

Visualising activity can be useful in assessing the scale of events and the behaviour of individuals but also in providing a means of monitoring for enterprise blockchains. This is something particularly useful as blockchains see increasing industrial applications for access control, document management, etc.

For financial services, know your customer (KYC) and anti-money laundering (AML) checks are of value.

"Smart contracts" are a common feature of blockchains that facilitate the negotiation and enforcement of business logic in a verifiable manner. They are of particular interest to organisations and consortia looking to transact between a number of untrusted parties. Many incidents relating to the loss of funds in cryptocurrencies can be linked to errors in smart contracts. Understanding threats to blockchains and smart contracts that run on them is extremely valuable to enterprises looking to leverage the technology.

Recognising the challenges and risks of blockchain technology, BT has constructed "Nova", an all-in-one blockchain analytics dashboard. A typical screen display is illustrated in Figure 7. With the ability to connect to multiple blockchains (cryptocurrencies such as Bitcoin and Ethereum as well as private ledgers such as Fabric), it is suitable for use by law enforcement and enterprise developers alike. The tool combines cluster analysis with graph visualisation as well as a rich intelligence database.

Conclusions

Cryptocurrencies saw an unprecedented surge in 2017 and their use in cybercrime is an ongoing issue with an increasing need for new tools to support both businesses and law enforcement. Cluster analysis and supporting open-source intelligence are powerful capabilities that have proven value in supporting human analysts, but fully automatic approaches still need development.

One of the challenges is the increasing but understandable rise in privacy preserving cryptocurrencies (those with the verifiable nature of Bitcoin, but without the lack of anonymity) and this is compounded by the availability of cross-chain transactions that utilise a variety of cryptocurrencies to obfuscate the source and destinations of funds.

As enterprise blockchains technology is being deployed across industries for financial, access control and data management tasks it is likely that forensic capabilities originally developed for cryptocurrencies will be applicable to developing environments in managing blockchain homeostasis. Capabilities will need to be developed that analyse not just historical transactions, but also smart contract execution, peer to peer communications and social interactions.

Reproduced by kind permission of the Editor, The ITP Journal.