Defence Research and Development Canada
Recherche et développement pour la défense Canada

CAN UNCLASSIFIED

DRDC | RDDC
technologysciencetechnologie

On blockchain technology and its potential application in tactical networks

T.J. Willink
DRDC – Ottawa Research Centre

Defence Research and Development Canada
Scientific Report
DRDC-RDDC-2018-R033
April 2018

CAN UNCLASSIFIED

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by DRDC using the Schedule to the *Defence Production Act.*

Disclaimer: Her Majesty the Queen in right of Canada, as represented by the Minister of National Defence ("Canada"), makes no representations or warranties, express or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

Endorsement statement: This publication has been peer-reviewed and published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada. Inquiries can be sent to: Publications.DRDC-RDDC@drdc-rddc.gc.ca.

Abstract

Awareness of blockchain has soared in recent years with the emergence of cryptocurrencies, but the technology has existed for much longer. The linking of blocks, containing cryptographic functions of transactions and data, means that tampering with their contents becomes increasingly difficult as the chain grows – this concept was exploited for document timestamping applications more than a decade before cryptocurrencies became reality. In many implementations, blocks are confirmed by, and stored at, many nodes in different locations, providing a high degree of data integrity. There are, however, many challenges for applying blockchain technologies in tactical networks, particularly due to the constraints of the platforms, the limited bandwidth available among them, and the impact of network partitioning. In this report, the development and principles of blockchains are presented, along with an overview of their weaknesses and vulnerabilities. There is a huge level of interest in this technology across many sectors, and this is reflected in the breadth of the referenced material. Weaknesses in design and implementation can make blockchains vulnerable to attack, and their interfaces are particularly at risk. A range of possible applications in tactical networks is explored, from supply chain management, to network management and application data immutability. Finally, a simple blockchain architecture for mobile tactical networks is developed, to illustrate the potential and challenges of this technology. Overall, it is clear that blockchain technology provides a potential avenue for solving some problems in the tactical network context, but it is not yet clear whether it is the best such solution.

Significance for defence and security

Maintaining data integrity in defence systems is a key component of security processes, from supply chain and asset management to situational awareness and command and control information tracking. Blockchain technology is a potential solution to achieve data integrity, relying on cryptography and duplication or witnessing to provide tamper-resistance. The immutability of data in a blockchain is strongest when the chain is long, and the number of witnesses is large: this is is a challenge in tactical networks when processing power, memory and bandwidth are limited. However, there are ways in which blockchain might be applied to provide data integrity where it is not currently a significant consideration, which may support future cyber operations by providing auditing, resource management and authentication functions.

Résumé

L’intérêt à l’endroit des chaînes de blocs s’est accru de manière fulgurante durant les dernières années avec l’arrivée de la cryptomonnaie. Pourtant, cette technologie existe déjà depuis un bon moment. L’enchaînement de blocs qui contiennent des fonctions cryptographiques des transactions et des données a pour effet de rendre plus difficile la falsification du contenu des blocs à mesure que la chaîne s’allonge. Ce concept a été exploité dans les applications d’horodatage des documents plus d’une décennie avant l’apparition de la cryptomonnaie. Dans bon nombre d’applications, les blocs sont confirmés par de nombreux noeuds et entreposés à différents endroits, ce qui permet un niveau élevé d’intégrité des données. L’application de la technologie des chaînes de blocs aux réseaux tactiques pose beaucoup de problèmes particuliers cependant, surtout en raison des contraintes des plateformes, de la bande passante limitée disponible entre les plateformes et des répercussions du partitionnement du réseau. Dans le présent rapport, l’auteur présente l’élaboration et les principes des chaînes de blocs, de même qu’un aperçu de leurs désavantages et de leurs vulnérabilités. Cette technologie suscite un très grand intérêt dans un grand nombre de secteurs, comme en témoignent les différents documents de référence. Des faiblesses dans la conception et la mise en oeuvre peuvent rendre les chaînes de blocs vulnérables aux attaques ; leurs interfaces sont d’ailleurs particulièrement à risques. L’auteur explore un éventail d’applications possibles dans les réseaux tactiques, de la gestion de la chaîne d’approvisionnement à celle des réseaux et à l’immuabilité des données d’application. Enfin, l’auteur élabore l’architecture simple des chaînes de blocs d’un réseau tactique mobile afin d’illustrer le potentiel et les difficultés de cette technologie. Dans l’ensemble, la technologie des chaînes de blocs offre manifestement une avenue possible pour régler certains problèmes dans le cadre des réseaux tactiques, sans qu’on ait établi clairement jusqu’à maintenant qu’elle constitue la meilleure solution.

Importance pour la défense et la sécurité

Le maintien de l’intégrité des données des systèmes de défense représente la principale composante des processus touchant la sécurité, de la chaîne d’approvisionnement et la gestion des ressources à la connaissance de la situation, en passant par le repérage de l’information du commandement et contrôle. La technologie des chaînes de blocs pourrait être une solution au maintien de l’intégrité des données, car elle dépend de la cryptographie, de la duplication et de témoignages pour prévenir la falsification. L’immuabilité des données d’une chaîne de blocs est la plus grande lorsque celle-ci est longue et que le nombre de témoins est élevé. Cette caractéristique constitue un problème pour les réseaux tactiques, où la puissance de traitement, la mémoire et la bande passante sont limitées. Il existe cependant des façons d’utiliser les chaînes de blocs pour assurer l’intégrité des données là où celle-ci ne constitue pas actuellement un facteur important. Cette technologie pourrait alors soutenir de futures cyberopérations en offrant des fonctions de vérification, de gestion des ressources et d’authentification.

Table of contents

List of figures

This page intentionally left blank.

1 Introduction

Blockchain is a relatively new term in popular vocabulary, and has elicited interest from many domains including finance, supply chain management, shipping logistics, identity management and others. This excitement arises from the hype surrounding the cryptocurrency Bitcoin [1], which was proposed in 2008 [2] and continues to attract headlines today.

In fact, blockchain concepts pre-date cryptocurrencies. They were developed for the purpose of time-stamping documents to assert priority, and several proposals based on linkages or chains of document properties were put forward in the 1990s [3–6]. Two approaches were considered for ensuring the authenticity of the timestamps: a central trusted authority and distributed trust. In digital timestamping work prior to 2000, the idea of fully distributed trust was largely dismissed in favour of a central trusted authority. As noted in [6], "We believe that techniques based on distributed trust are not really workable in a professional environment. . . ".

Around the world, trust in the establishment, in government, media and public institutions, has been decreasing [7, 8]. This has been reflected in the rise of the so-called "sharing economy", in which individuals make a choice to do business with other individuals, ostensibly bypassing traditional established economic relationships [9]. While some of these microeconomic systems are based on trust in individuals, more widespread sharing arrangements, such as the rental marketplace Airbnb [10], are based on a concept of trust embedded in the application, in which user profiles and public reviews provide a sense of comfort [11]. This concept of distributed trust, which is really lack of trust in individuals but trust in a community, is fundamental to current blockchain implementations.

Interestingly, despite this trend away from trust in governments, many of them are investigating blockchain as a means to improve secure identity management. Estonia invested heavily in secure digital technologies since a nationwide hack in 2007 and started testing blockchain in 2008; it has been in use since 2012, supporting health, judicial and security systems [12]. The Government of Canada announced in January 2018 that it would develop a pilot project for a prototype "Known Traveller Digital Identity", based on biometrics and blockchain or similar technologies [13]. In the US, Congress has ordered reports on the applications of blockchain [14], and several government departments, including Defense, Energy and Homeland Security, are investing in blockchain technology [15–20]. The United Nations is also investigating the use of blockchain to provide a range of services, with 15 initiatives underway [21] and a blockchain commission established [22]. Ukraine, Sweden, Dubai and Georgia are all undertaking studies and pilots [23], and blockchain has been proposed as a solution to managing the customs border between a Britain separated from the EU [24].

In financial transactions, a key part of the trust challenge is to ensure that users of a currency actually own the funds they are spending, in particular, that they are not spending the same currency unit two or more times. This has traditionally been overseen by a central trusted authority, namely, the banks. The Bitcoin approach eliminates the requirement for a central trusted authority, using a peer network to prevent double spending by time-stamping validated transactions.

A blockchain is essentially a ledger of transactions or information, where each block, containing the transactions, a timestamp and a link to the previous block, is cryptographically protected. The openness of the ledger, either by distribution or periodic publication of its state, prevents undetected modification of previously incorporated information. The blockchain technology thus provides a tool for increasing data integrity using a combination of cryptography and consensus. A more detailed description of blockchain is given in Section 2.

Currently, there are huge investments in blockchain technology by both established consulting companies such as IBM [25] and Deloitte [26], and by more recent entries such as Peer Ledger [27] and EncryptoTel [28]. A new high level programming language, Solidity, has been released for applications based on blockchain [29] as part of the Ethereum project [30]. The Linux Foundation has also developed software specifically designed for blockchain applications [31]. ING Wholesale Banking [32] developed the Easy Trade Connect blockchain in partnership with Société Générale Corporate & Investment Banking [33]; in January 2018 this technology was used in the first international agricultural trade supported by blockchain – a cargo of soybeans sent from the US to China [34].

Of course, there are many academic researchers exploring the potential of blockchain, spanning a continuum of study among technology, business and societal impact [35–39]. This technology concept is advancing so rapidly, much faster than can be handled by the current peer-review process, that there is a significant volume of opinion and information available on the Internet, and relatively little useful formal, conventionally peer-reviewed, academic literature (for example, there were fewer than 250 papers indexed under 'blockchain' in IEEEXplore in November 2017). Many of the references herein, therefore, are non-traditional citations to online resources. It is anticipated that an avalanche of academic research in blockchain will appear in the next couple of years, but care must be taken in interpreting the analytical and theoretical results therein, as they will likely be closely tied to the assumptions and models used, which may not be generalisable or applicable to the circumstances of interest in practice.

Amid the hype, there is some scepticism about the application of blockchain [40–43]. With the exception of cryptocurrencies, which have already gained a firm foothold in the financial world, blockchain remains a technology solution in search of a problem.

This report is written in response to interest expressed by project clients and stakeholders about the potential for applying blockchain concepts to cyber security problems. It is focussed on tactical networks, where security is becoming increasingly important but is challenged by limited bandwidths, limited processing capability and limited power capacity.

Blockchain technology is developing rapidly, being driven by many different players with different objectives, and there is not yet a common vision. A summary of blockchain technology is given in the next section. Emerging directions, addressing challenges and opening new opportunities, are discussed in Section 3. A variety of vulnerabilities, from weakness in design and implementation to blockchain interfaces, is outlined in Section 4. The mobile wireless environment poses particular challenges that do not dominate in conventional wired networks. In consideration of these, the possible roles for blockchain technology in tactical networks are considered and a possible architecture for blockchain use is presented in Section 5. Conclusions are summarised in Section 6.

2 Blockchain technology

Blockchain technology existed before the excitement of cryptocurrencies pushed it into common parlance. The underlying concepts include cryptography and timestamping to establish tamper-resistant provenance. Modern blockchain principles are based on consensus mechanisms that have been around since distributed processing became a subject of academic interest in the 1980s. Today, a number of large scale implementations are available to support new applications and experimentation.

2.1 Evolution

The person or persons[1] who authored [2] are often credited with inventing or conceptualising both cryptocurrencies and blockchain. In fact, cryptocurrencies were proposed earlier [44], and more formally in [45,46], and the idea of requiring proof-of-work to be allowed to access a shared resource was considered in [47], as a means to reduce the volume of junk email. Blockchains themselves were based on earlier efforts in timestamping to provide verifiable proof of existence and priority of claim.

In the 1990s, efforts to provide tamper-proof timestamping resulted in both distributed and centralised approaches. While distributed trust was an early candidate for this requirement [3], it was noted that this approach required that others maintain records, be identified in a shared list, and be available and willing to perform work in a timely fashion. The practicality of those expectations was questioned in [6], so in many early implementations, the blockchain relied on a central trusted authority (CTA).

In centralised timestamping, clients submitted their documents to the CTA for timestamping and received in return a certificate containing sufficient information to validate their time claims. As discussed in [5], three main approaches to timestamping were considered, based on linear linking, Merkle trees and random witnessing. To reduce the sheer volume of data that must be stored, the documents themselves were replaced by the outputs of their hash functions. These fundamental concepts are briefly described below.

[1] The identity of the author, or group of authors, known as Satoshi Nakomoto who wrote the iconic cryptocurrency paper [2] is unknown.

2.1.1 Hash functions

Throughout the evolution of the blockchain concept, the process has relied on hash functions to cryptographically compress strings. Hash functions were developed in the 1970s [48–50] as a means to authenticate large files using a small data string.

A hash function takes an arbitrary-length input string x, such as a document file, and maps it to a fixed length string $h(x)$, known as the hash value or hash [51, Ch. 2]. The hash function is designed such that it is computationally very hard to:

- determine the input string x from the hash value, i.e., to find a string y such that $y = h(x)$;
- find a different string x' that results in the same hash value, i.e., find x' such that $h(x') = h(x)$; and
- find two strings z and z' that produce the same hash value, i.e., $h(z) = h(z')$.

2.1.2 Merkle trees and roots

A tree approach, based on Merkle trees [52], was proposed in [3] to reduce the overall effort imposed when many documents of low importance would be submitted for timestamping. Each client, i, $i = 1,\ldots,N$, would submit the hashed value $y_i = h_i(x_i)$ of their document x_i, using their own personal hash function h_i. These become the leaves of the tree. Pairs of hash values would be hashed together, successively, moving down the branches of the tree, as illustrated in Figure 1, each pair yielding a single fixed-length hash value. When the root of the tree is reached, the final hash value known as the Merkle root, y_{1N}, is published (for example in a newspaper), thereby establishing a timestamp.

To prove that their document originated before the published timestamp, a client must retain their own hash value, as well as the hash values with which theirs was paired at each stage in the tree, and the 'left' or 'right' position in each pairing. For example, client ID_3, with document hash h_3, would retain the values y_3, (y_4, *left*), (y_{12}, *right*), . . . to ($y_{N/2+1,N}$, *left*).

2.1.3 Linear linking

The significance of linking, or chaining, data produced from successive transactions, or documents, was noted in [3]. The linear linking approach is summarised in Figure 2. At event n, the client, identified as ID_n, submits the hash value, y_n, of their document to the CTA. This is combined with the timestamp, t_n, and linking information from the previous event, L_n, to produce a certificate $C_n = (n, t_n, ID_n, y_n, L_n)$ that is returned, signed as $s_n = \sigma(C_n)$, to the client. The hash value produced by the CTA function H is combined with the timestamp and client input to produce the linking information for the next event, $L_{n+1} = (t_n, ID_n, y_n, L_n)$. Once the next event has been processed, the client identifier for the next event, ID_{n+1}, is also returned to the client of event n. Thus, a challenger of client ID_n's document can ask client ID_{n+1} for their signed certificate, which incorporates ID_n's

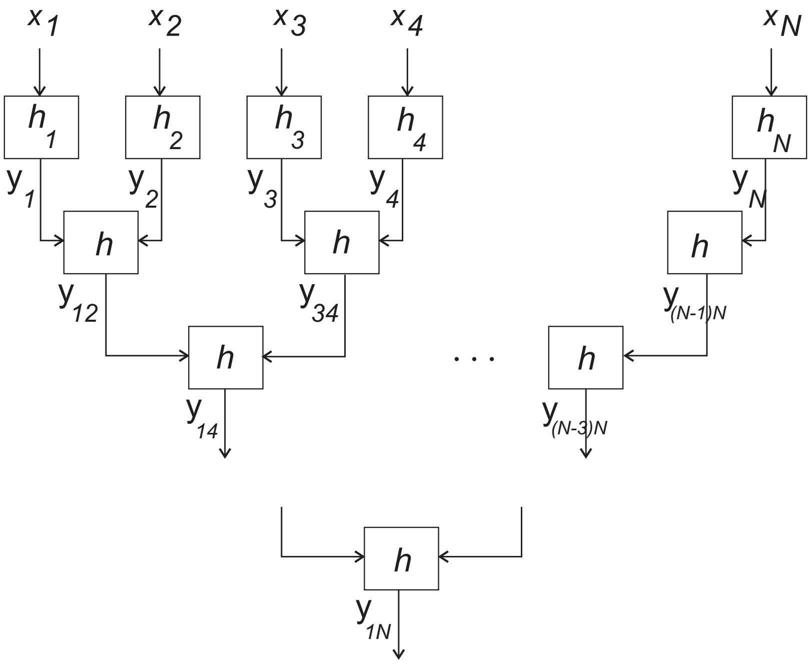


Figure 1: *Merkle tree for timestamping.*

hash value in the linking information. In this way, the challenger can move forward through the chain until they are satisfied about the veracity of ID_n's timestamp.

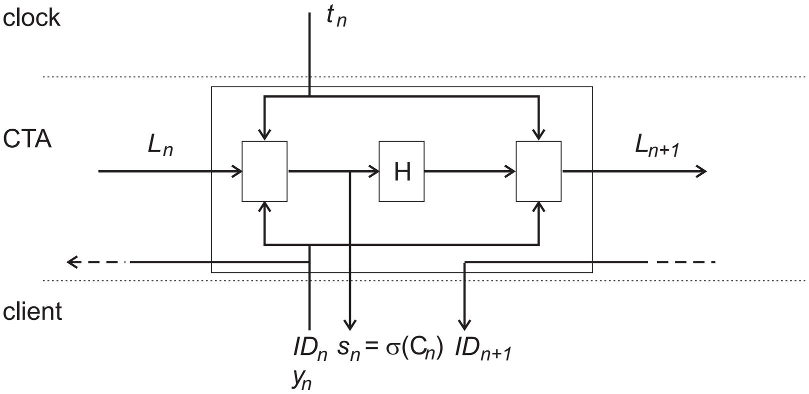


Figure 2: *Linear linking for timestamping.*

2.1.4 Witnessing

The concept of distributed trust was considered in [3], whereby k witnesses, randomly selected from a list of all clients, perform the timestamping service and return signed messages to the requestor containing their timestamp, the requestor's ID and the original hash value. This would produce a believable timestamp, as the random witnesses would have to collude to produce a false yet valid value. This requires a large pool of available witnesses, who have sufficient independence from one another that it can be safely assumed that the k selected ones are not all corruptible.

In [5], it was noted that the act of publishing of the root of the tree in Figure 1 created a pool of witnesses, namely, those that see the publication.

2.1.5 Distributed ledgers

A trusted central authority must not only maintain the trust of its clients, it must also provide the necessary resources to maintain and update its database, or ledger. In the absence of such a willing and trusted authority, the ledger may be held in a distributed fashion[2], where every node in the peer network shares control of the data. Peers agree to a common set of rules to determine the validity of ledger data: if they break these rules then the other nodes will not accept their inputs to the ledger.

The lack of mutual trust among peers means that each must check every piece of data, or transaction, it receives to ensure the rules are followed. Some form of consensus among the peers (defined by the rules of the distributed ledger) is required before the new transaction can be accepted. Once validated, these transactions are propagated through the network and added to each local copy of the ledger. In this way, distributed ledgers are maintained as “authoritative systems of record” [54].

Note that a distributed ledger is not necessarily a blockchain. A blockchain is a form of ledger[3] in which transactions are cryptographically linked to form a (theoretically) immutable and incorruptible record of transactions, in the sense that tampering or modifications of one block would be detectable by looking back through the chain.

2.2 Blockchain principles

The purpose of a blockchain is to maintain a trusted record of transactions, which are usually thought of as records of exchange of goods, funds or data, but may also be documents or data that require proof of existence, as in the timestamping application. They are usually digitally signed by the user submitting the transaction to allow verification by others.

The construction of the blockchain is similar regardless of its purpose and participants: this will be described in Section 2.2.1. Public blockchains, known as ‘permissionless’, allow any participants to join the blockchain network and take on different roles. Permissionless blockchains are also trustless, i.e., the participants have no reason or need to trust each other; rather, they are able to agree on the current state of the common record using a consensus mechanism (see Section 2.2.2).

[2] Note that the term “distributed ledger” has become standard usage, although it is more accurate to call these “decentralised ledgers” as the former suggests that the ledger contents are spread amongst many nodes, while in fact copies of the ledger are held at each node. This distinction is made in the technical whitepaper released by Corda [53], which is a platform for managing business agreements.

[3] A blockchain need not be a distributed ledger, but having copies held in many, distributed independent nodes gives it its immutability in a trustless environment.

In a typical permissionless blockchain implementation there can be users, nodes and miners. Users are the clients of the blockchain, but the nodes and miners play an active role, and are accorded read and read/write permissions, respectively. The process will be along these lines:

1. A user submits their signed transactions to a node.
2. The node propagates the transaction around the network to the other nodes.
3. Each node verifies those transactions; this will typically involve checking the digital signatures and that the structure of each transaction is correct.
4. Miners gather groups of verified transactions, validate that each user is the owner of the goods or funds in the transaction, and process them to generate blocks, according to the rules of the blockchain.
5. When a miner completes a block, it propagates it around the network.
6. The network nodes validate the block, according to the consensus mechanism.
7. When the network nodes agree the block is valid, it is appended to the blockchain.

The costs of verifying and propagating transactions, mining blocks and achieving consensus must be borne by the users, so permissionless blockchains usually contain some kind of token for payment. While tokens are usually considered to be some form of currency, they may also represent other assets of value, such as votes or credits. Some permissionless blockchains exist purely for the purposes of these tokens, particularly cryptocurrencies, for example Bitcoin [1], while others such as Ethereum [30] allow other types of record keeping and processing.

'Permissioned', or consortium, blockchains are sovereign – they are not open to the public; rather, the participants are typically defined in the rules establishing the blockchain, which also specify who has read and write permission. This changes the trust dynamic among participants, which may alter the roles of the participants and the demands on the consensus mechanism, see Section 2.2.2. These blockchains may be used, for example, for supply chain management, or recording of business-to-business transactions or record exchange. In these implementations, there may be only one class of user node, and the process may be similar to this:

1. A user node signs their transaction and submits it to the blockchain network.
2. One selected node (maybe the user node) generates a block and propagates it around the network to the other nodes.
3. Each node validates the block, by verifying the signature and checking the transaction.
4. The nodes apply the consensus mechanism rules to agree the block is valid, and it is added to the blockchain.

In this case, the nodes share equally in the blockchain's benefits, so the blockchain need not include any form of payment token. Sometimes, permissioned chains are considered to be a subset of private blockchains, in which one organisation is trusted to authorise block additions to the chain; in this report, these private and permissioned blockchains are not distinguished, as they differ primarily in the consensus mechanism used.

Some of the higher-profile blockchain implementations are discussed in Section 2.3. As discussed below, the introduction of permissioned blockchains, for example as service offerings from information technology (IT) providers, is opening up new blockchain application opportunities (see Section 3.4).

2.2.1 Construction

Each block in the blockchain contains the block number, a header, and the transactions contained in the block. The blocks are joined via their headers, which are chained together as illustrated in Figure 3. The mining process selects the transactions to be included in the block, generating their hash functions and deriving their Merkle root (Section 2.1.2).

The header contains the Merkle root derived from the included transactions, a timestamp and the hash of the previous block header (except in the case of the first, or genesis, block). This linking provides the immutability of the blockchain: the only way to successfully tamper with a block is to regenerate all blocks from the genesis block forward, which is a gargantuan task for a blockchain of any substantial length.

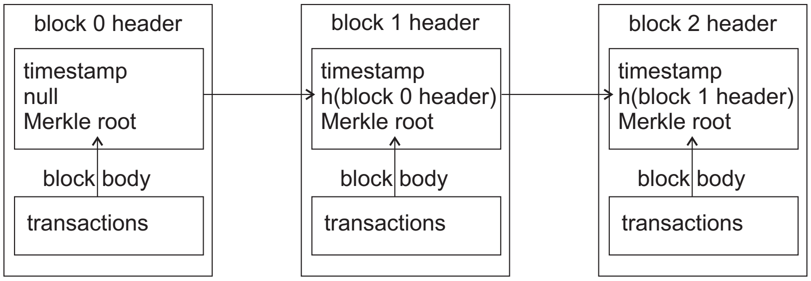


Figure 3: *Chaining of block headers.*

2.2.2 Consensus mechanisms

When blocks are generated, the network must agree that they are valid and should be added to the chain. This is achieved through a consensus mechanism, which is defined in the rules of the blockchain. As noted above, the type of consensus mechanism used is specific to the requirements of the blockchain, and new ones are being developed as blockchain applications expand. An overview of the main consensus mechanisms currently in use is given here.

The most commonly known consensus mechanism is proof-of-work, which is used by Bitcoin (Section 2.3.1). In this protocol, the miner must find a nonce[4] that, when included

[4] A nonce is a number, in this case, with a fixed length, that is generated and used once.

as part of the block's header, results in a hash value that is less than some predefined, common target[5]. This hash value computed is called the "proof-of-work" – it is computationally intense to produce but easily validated by other nodes, which makes it appropriate for trustless, permissionless blockchains. However, as observed below, this is an extremely energy-intensive process.

Proof-of-stake is widely considered as an alternative to proof-of-work as it does not require specialist hardware for mining, and consumes far less energy than proof-of-work. In a typical proof-of-stake protocol, a set of validator nodes is established, based on their stakes in the blockchain [55]. In one version of the proof-of-stake protocol, a validator node is selected randomly to provide the next block – the node combines the transactions and links to an existing block, usually the most recent one in the longest chain, to generate a new block. In an alternate version, selected nodes are allowed to propose a block, but all the validator nodes then vote on which block will be accepted into the chain. The Ethereum blockchain (see Section 2.3.2) is preparing to make a switch from proof-of-work to proof-of-stake in its new release, Casper [56].

Under a proof-of-stake algorithm, nodes with small balances will very rarely be given an opportunity to generate blocks. In the delegated proof-of-stake variant of this algorithm, these small players may lease their holdings to other nodes, increasing those nodes' chances of being selected and when they are, a portion of the reward may be shared.

Proof-of-work and proof-of-stake have been combined into a hybrid in Peercoin [57]; in this hybrid, proof-of-work is used mainly for minting, i.e., generating new currency units, while proof-of-stake is used for securing the blockchain, which removes much of the high energy requirements.

The practical Byzantine fault tolerance (PBFT) algorithm was introduced in the late 1990s [58], to address the challenge of reaching consensus among a group of distributed agents, when they cannot be trusted to give honest answers. Several flavours of the PBFT consensus mechanism have been developed, and are used in Hyperledger [31] and Tendermint [59].

Backfeed is a reputation-based protocol using proof-of-value [60]. In this approach, a peer node's reputation is gained by making contributions and by evaluating other nodes' contributions; when a majority of reputation in the network acknowledges that a contribution is valuable, i.e., the block is accepted, that contributor is rewarded with an increase in reputation and their block is added to the chain.

For permissioned blockchains, the enhanced level of trust removes the need to compete for block generation. Consensus mechanisms such as round-robin, where nodes take turns generating blocks [61], might be appropriate. Intel has proposed a proof-of-elapsed-time algorithm, which operates in a trusted execution environment (TEE) such as the SGX-enabled CPU [62], in which code and data are protected and cannot be modified or accessed.

[5] The size target is used as a simple way to apply a restriction to an otherwise random number, thus ensuring that each miner must 'work' to find a suitable nonce and thereby generate a block.

In this approach, a node is selected at random based on a counter within SGX and it provides the next block. This counter uses a minimal amount of power, but does require that all nodes are using the same TEE. The TEE was also exploited in [63] to implement a PBFT algorithm; this implementation is claimed to be "the fastest and most scalable BFT protocol to-date".

2.2.3 Forks

In a large blockchain network, transactions and blocks take time to propagate to all nodes. Miners therefore may operate on different sets of transactions and generate blocks at almost the same time, and there be multiple blocks circulating in the same interval. It is therefore possible that at any given time, the blockchain diverges and contains two or more leading blocks. This is referred to as a fork.

One of the principles of the blockchain is that blocks are added to the longest chain, therefore generally so-called soft forks are resolved quite quickly as one tine grows faster than the other(s). In this case, the shorter chains are abandoned, and the transaction contained in the dropped blocks, if they are not included in blocks on the maintained chain, will be offered up for mining again.

Forks are also imposed on the blockchain when there is a change in the rules. As with most blockchain features, there are differing opinions on the definition of a fork. Generally, a hard fork occurs when the rules are not backward compatible, for example, if a new consensus mechanism is introduced. In this case, the blockchain will split permanently; the old blockchain may cease to grow, or the two may continue independently.

2.3 Implementations

As noted above, there are different types of blockchain, which depend on the community they serve and their purpose. Some of the more established implementations are summarised here.

2.3.1 Bitcoin

Bitcoin is probably the most well-known of the cryptocurrencies in use. It is a public distributed ledger of financial transactions in the form of a blockchain, proposed in 2008 by the person or group going by the name Satoshi Nakamoto [2]. While bitcoins are used by clients for an increasing range of everyday financial transactions, at the core of the blockchain are the 'miners', or nodes that compute and validate new blocks.

Sums of bitcoin have public and private keys associated. When client A owns bitcoins, what they really hold, stored in their electronic wallet, are the cryptographic keys of one or more sums of bitcoin that have previously been transacted. The public key specifies the address to which that sum was sent most recently (belonging to A), and the corresponding private key authorises that sum to be forwarded to another client. This is known as an unspent transaction output (UTXO) scheme.

Transactions are incorporated into the Bitcoin blockchain more-or-less as described in Section 2.2; every block interval, currently 10 minutes, each miner starts a new block generation attempt, based on the unprocessed transactions available. Each transaction must be validated, which requires searching back through the blockchain to find the prior transaction history of the bitcoin being spent; as the blockchain gets longer (the number of unspent transaction outputs exceeded 60m in early December 2017, up from 44m a year earlier [64]), this search process becomes increasingly onerous. Near the end of December 2017, there were almost 120,000 unconfirmed Bitcoin transactions – in mid-May 2017, this number spiked above 200,000 [64]. This backlog contributes to a latency in transaction processing, which ranges from approximately 35 minutes to a peak of over 3500 minutes during December 2017 [64]. Once the current transaction is validated, the miner can include its hash in the computation of the Merkle root contained in the header. Bitcoin uses a proof-of-work consensus mechanism, in which each miner competes to find a nonce that, when combined with the rest of the block header, produces a hash that is less than a publicised target.

At the end of November 2017, the Bitcoin blockchain was almost 170 GB [65]. Blocks were averaging 1 MB each, and at the time of observation, there were over 13,000 transactions waiting to be incorporated into the block, accounting for approximately 34 MB. On average, there were over 300,000 transactions per day, with an average transaction value of more than $60,000 USD (median $535 USD). Miners were rewarded over $125,000 USD per successful block.

It has been estimated that 500–700 MW are required to power Bitcoin processing, worldwide, enough to power 325,000–450,000 average US homes [66]. This is particularly wasteful when it is observed that almost 25% of blocks mined were empty, i.e., contain no transactions, between 2009 and 2015 [67]; this rate has decreased since, but as miners are given large rewards for mining blocks and only receive small transaction fees, the incentive to include few transactions and produce a block faster remains.

2.3.2 Ethereum

Another major blockchain player is Ethereum, from the Ethereum Foundation [30]. Ethereum was launched in 2015, and already completes over 1 million transactions per day, compared to approximately 400 thousand for Bitcoin [65]. It has its own crypto-token, Ether, but also provides a public blockchain for use in other applications such as smart contracts (see Section 3.2); the Ether token is used to pay transaction fees in those applications. Developers can use the platform provided to write their own blockchain code to implement smart contracts, create new asset registries, or release new trading concepts, without building or maintaining the underlying blockchain.

Ethereum is an account-based blockchain, so unlike the Bitcoin UTXO approach, the total balance of each client account is stored. Each block contains the Merkle root, the hash of the root node of the Merkle tree of account balances (see Section 2.1.2), to record the global state of all the accounts at the time the block is generated, as well as the previous block hash and the hash computed from the mined transactions.

Ethereum currently uses the proof-of-work stake, but as with Bitcoin, the amount of energy required to mine blocks is huge. A hard fork is expected in the near future, in which the consensus mechanism will be switched to proof-of-stake. Although this is a major event for a blockchain, it is not unheard of: a hard fork was planned for Ethereum to upgrade the network, and occurred, seemingly without significant disruption, on October 16, 2017, when the software upgrades were activated.

2.3.3 Hyperledger

Hyperledger [31] is an open-source collaboration producing a growing set of blockchain frameworks and tools, initiated by the Linux Foundation in 2015. It claims as members a large number of small and large enterprises, spanning finance and banking, information technology, manufacturing and supply chain logistics, and university labs. Its projects include Hyperledger Sawtooth and Fabric, which are frameworks for modular blockchain development, and Hyperledger Indy, for decentralised management of self-sovereign identity, i.e., users store their own digital identities on their own devices, but stored as ‘transactions’ in the blockchain, maintaining privacy while enabling trust.

Despite the many consortium members, uptake of Hyperledger’s products is slow [68]. Known use cases are IBM’s use of Hyperledger Fabric [25], and CLS Group’s application to foreign exchange [69].

2.3.4 Corda

R3 Corda is a distributed ledger designed to support financial services industries [70, 71]. Note that is is not described as a blockchain, but rather ‘blockchain-inspired’ and a ‘decentralised global database’. However, it shares many of the same principles. Its consensus mechanism is built around notaries, which are clusters of nodes authorised to verify the structure of each transaction and validate it, ensuring that the same assets are not transferred twice. The notary nodes may be trusted or not, and run a consensus algorithm such as PBFT to approve transaction blocks to the ledger.

3 Emerging directions

As blockchain concepts evolve, there are a few emerging directions that might be relevant to their application in defence applications.

3.1 Scalability

As blockchains become larger, the data in older blocks becomes more resistant to tampering (Section 5.3.6), but other problems arise. Validating transactions may require searching back over thousands of blocks, which slows the mining and consensus processes; in the Bitcoin blockchain, on-line indexing services are necessary and available [64], even though this is counter to the trustless and distributed philosophy of blockchain.

The consensus mechanism may also be a barrier to scaling. The proof-of-work consensus, used in Bitcoin, scales poorly [72] as its latency increases and throughput decreases with an increasing number of transactions. The massive power demand was also noted in Section 2.3.1.

Permissionless blockchains, in particular, are limited in their ability to scale, because every participating node must deal with every transaction submitted to the network, and must maintain a copy of the entire blockchain. This can be avoided in permissioned blockchains, although restricting the number of nodes supporting consensus weakens the fundamental security of the blockchain technology. Although the security of the network grows with the number of processing nodes, the weakest node in the network defines the limit on the rate of transactions that can be processed. The latency of the propagation of transactions and blocks in the consensus mechanism increases as the number of nodes in the network increases, which tends to increase the number of forks.

Several innovations have been proposed to deal with scalability issues, including sidechains and sharding, although each introduces its own challenges.

Sidechains

A sidechain is an offshoot of a blockchain that operates separately, but is pegged to the main blockchain, so assets can be moved between them. In a cryptocurrency, this would enable users to transfer coins securely from one blockchain to another, where they can be exchanged under the sidechain's protocols, for example, as a new or experimental cryptocurrency or as a smart contract (see Section 3.2) [73]. Ethereum [30] and Lisk [74] are blockchains that are designed for developers to create their own sidechains, taking advantage of the security and protocols of the main blockchains to build applications. Fees are paid per transaction, as established by the main blockchain owner.

Several criteria for establishing sidechains were defined in [73], including the firewalling of sidechains such that they are fully independent and do not require users to monitor the parent blockchain, and security regarding the transfer of assets from one blockchain to another. However, the consensus power available is reduced as the number of sidechains increases, increasing the overall vulnerability.

The Cosmos network [75] takes the concept of sidechains much further, connecting separate, independent blockchains through blockchain-based hubs, to address scalability and interoperability issues. When the load on one of the blockchains becomes excessive, a new blockchain instance is added to the hub, to process some of the transaction load, while the hub maintains synchronisation among the blockchains.

Sharding

There are two main bottlenecks impinging scalability: the need for nodes to process all transactions, i.e., to verify the signatures and validate transactions, and to process the network state, i.e., the accounts. Dealing with scalability requires tackling both of these; this can be achieved with sharding [76]. A simple sharding scheme would split the accounts into a number of disjoint sets, or shards, then nodes assign themselves to shards and process only the transactions submitted by the accounts in that shard. Some kind of cross-shard exchange is necessary when transactions occur across shard boundaries. An early proposal for implementing sharding in Ethereum is given in [77]. It was recently announced that sharding is part of the 5-year plan for Ethereum [78].

A version of sharding, tree chains, was proposed for addressing the scalability of Bitcoin [79]. In this scheme, a tree of blocks would be used in place of the chain, where the leaves (see Section 2.1.2) are groups of transactions, and blocks further down the tree structure simply combine the two hash functions generated above. This allows miners to work in parallel, mining as many different sets of leaves as they have capacity for. This deals with the processing limitations, but actually appears to worsen latency, according to [80], as each transaction must be communicated among the leaves to ensure it is only processed once. The tree chain concept has since been adopted into the Viacoin cryptocurrency [81], but does not appear to have achieved much traction in the broader community.

3.2 Smart contracts

Smart contracts are currently emerging as a viable use of blockchain technology [82,83]. The underlying concepts of smart contracts were originally discussed in the mid-1990s [84]. Simply, a smart contract is a set of self-executing and self-enforcing instructions, implemented in software and stored in a blockchain, such as Ethereum [30].

Smart contracts are essentially accounts held in the ledger maintained by the blockchain, alongside the user accounts. While the user accounts hold records of assets and transactions, and are controlled by specified users, the contract accounts are controlled by their self-executing software, i.e., the smart contract. These contracts are agreed by the relevant parties prior to being added to the block chain, and execute when the contract account is sent a transaction by a user account. For example, consider a rental agreement contract:

- renter and owner agree terms, which are written into the contract, specifying rent and start date;
- renter pays the agreed initial rent in cryptocurrency to the contract account, which provides a receipt to owner;
- owner provides a digital key to the contract account;

- if the rent and key are provided by specified dates, the contract account releases the key to renter and the currency to owner; if not, the contract account releases a refund to renter.

Even though this is a simple example, it illustrates that the transaction is completed rapidly and in strict agreement with the contract terms; it is witnessed by many virtual bystanders, reducing the requirement for personal trust or faith in the other party; the contract cannot be lost or altered by either party as encrypted copies are held at many distributed nodes; no middle agency is required, although fees would typically be required for participating in the blockchain.

Another challenge to the implementation of smart contracts arises from one of their key selling points, *viz.* they are processed independently on many distributed nodes in the blockchain network. This means that any reliance on external data sources, such as stock market values, can result in disagreement amongst the nodes, which may access those sources at different times. The workaround for this is that a single, trusted entity must provide a single view of the external data to all nodes but this is counter to the concept of a trustless, decentralised system, and is vulnerable to loss or attack.

While transparency of the smart contract is sold as a benefit, in fact, there is a risk of exposing confidential information because each contract is held on many different nodes [85]. Any node owner could extract that information relatively easily.

Smart contracts via blockchains are being adopted in a range of industries. Kodak announced the launch of a photo-rights management blockchain, KODAKOne [86], with an integrated cryptocurrency, KODAKCoins, to ensure that photographers are paid when their images are used. Other companies in this market include Po.et [87], Photochain [88] and COPYTRACK [89]. The better-known Spotify acquired a blockchain company early in 2017 to manage copyright and payments [90]. Somewhat bizarrely, Long Island Iced Tea [91], which manufactures soft drinks, changed its name in December 2017 to Long Island Blockchain [92], announcing it would invest in developing blockchain technology, and sending its share price soaring.

The US Department of Energy's National Renewable Energy Laboratory announced in January 2018 that it is partnering with BlockCypher [93] to demonstrate the settlement of transactions related to energy resources across different blockchains [19].

3.3 Internet of Things

Internet of Things (IoT) devices comprise mostly sensors and effectors that can exchange data with other devices and applications. Typically, IoT devices have been designed to pass data or information to, from and via the "cloud", i.e., a central computer server system. This exposes a number of vulnerabilities, including authentication and confidentiality. As reported in [94], a recent investigation of new IoT devices showed design flaws such as hardcoded passwords and coding implementation errors such as buffer overflows. Mirai malware infecting wide range of IoT devices caused a massive distributed denial of service attack in October 2016, taking the Dyn DNS servers offline for hours [95]. Other IoT vulnerabilities were highlighted in 2016, when hackers showed they could remotely infect a thermostat with malware and lock it, opening the possibility of ransom attacks [96].

Blockchain has been proposed as an enabler for peer-to-peer networking IoT devices [97–100]. Blockchain can be used as a tool to provide authentication services [101], policy implementation via smart contracts [102], secure firmware updates [103], and secure data exchange [104]. Early implementations are using the Ethereum blockchain (see Section 2.3.2), including the IBM and Samsung collaboration, "Autonomous Decentralized Peer-to-Peer Telemetry" (ADEPT) for autonomous device coordination [105]. The US Department of Homeland Security issued an award under the Silicon Valley Innovation Program (SVIP) to Factom Inc. in June 2016, for the development of blockchain technology to track IoT devices used for border security, including their provenance, update status and authorities [20].

Estimates of the number of IoT devices vary, from 8.4 billion [106] to over 20 billion [107] in 2017; at either extreme the number is vast. These devices consume a huge amount of bandwidth and connection capacity, due to their high signalling overhead [108]. In many cases, IoT devices communicate via remote servers to other devices located nearby, rendering connections via the cloud wasteful. As discussed above, blockchains often require large amounts of power and bandwidth, and processing introduces significant latency. An alternative local blockchain was proposed in [109], however this approach requires some refinement as local clusterheads, which are nodes responsible for accepting blocks, may have different versions of the blockchain: this trades some degree of security for bandwidth.

3.4 Blockchain-as-a-service

Blockchain-as-a-service (BaaS) is being offered by a number of IT providers, to allow companies to develop distributed ledger capabilities without having to invest in deploying and maintaining their own blockchain technologies [110]. Some of the large providers include Oracle [111] (as part of the HyperLedger collaboration [31]), IBM [25] and Microsoft [112], whose Azure product leverages several blockchain protocols, including Hyperledger, Ethereum [30] and Corda [70]. Hewlett Packard Enterprise will launch their new product, "Mission Critical Distributed Ledger Technology" (using Corda) early in 2018 [113]. All these products are advertised as enabling rapid development of permissioned blockchain applications using the templates and tools provided, and integrate the blockchain into other enterprise services.

There are still challenges in this new direction. The pilots to-date have been small, and it is not clear how the scheme will scale. Additionally, it was noted in [114] that integrating blockchain into other services will require the reconciliation of transactions across the interface, which will slow down the whole process.

Note that blockchain is also proposed to add capability to the cloud, in particular to provide cloud storage in peer-to-peer networks. Sia from Nebulous Inc. [115] and Storj [116] both provide services to securely store data on multiple remote, untrusted and unstable servers. Smart contracts are enforced on the blockchains between users (storage renters) and providers or farmers. To use Sia requires downloading the entire blockchain, which is about 6 GB; Storj uses the Ethereum blockchain.

3.5 Secure messaging

The US Defence Advanced Research Projects Agency (DARPA) has issued several blockchain-related grants [15], including one to ITAMCO [117] for "secure message on the blockchain architecture". ITAMCO, in partnership with the Center for Research Computing at the University of Notre Dame, has established SIMBA Chain [118]; in the first phase of the project, blockchain technology will be incorporated into ITAMCO's Crypto-Chat messaging application [119].

The Mercury Protocol is an Ethereum-based blockchain token system for building social media applications [120]; it is already included in Dust [121], a peer-to-peer messaging app in which messages are automatically deleted after 24 hours, without leaving a trace. The protocol introduces and uses the Global Messaging Token (GMT), so that different messaging platforms, both using the Mercury Protocol, can exchange messages securely via the blockchain. Currently, social media platforms such as Facebook monetise their activities by selling aggregated user data, and users' attention, to advertisers. Within the proposed system, users could earn GMTs by performing "incentivised actions", for example, reading posts, responding to messages and contributing positively to discussions. These GMTs could be used to attach larger files to messages, or raise the user's profile within the social media platform. As a feature of the blockchain, users can maintain anonymity, but the reward of tokens for positive contribution is aimed to reduce trolling and other antisocial behaviour.

PikcioMe [122] from MatchUpBox [123], is a new app, in beta testing as of January 2018, that claims to provide a planner, data management, internet search, financial management and secure chat. Details are light, but the peer-to-peer messaging function registers and timestamps messages and files on the PikcioChain [124]. Somewhat alarmingly, the Pikcio Whitepaper claims that users earn tokens by selling their data and the PikcioPro component of the system allows commercial organisations to buy, sell and trade users' data.

Blokcom is another blockchain-based messaging application that claims to transform untrusted environments, using "secure and trackable messaging" [125]. Little information is available, but the platform promises user authentication and certification, as well as immutability and trackability of data exchange. Yet another, also with few details, is Obsidian [126], which supports user privacy through anonymous messaging.

Crypviser [127] was launched in January 2018, and claims to be the "first encrypted unified cross-platform app on blockchain". The application provides public key distribution and validation through a blockchain, to establish secure communication sessions between users. As with most commercial blockchain offerings, it includes a cryptocurrency, which is used primarily to pay for the blockchain transactions used in authentication. In the current release, Crypviser servers are integrally involved in the authentication and key distribution process, which appears counter to the blockchain philosophy. The company's whitepaper [128] indicates that future releases will rely solely on a mobile blockchain, but details are sparse.

Blockchain-based email applications have been under development, including SwiftMail [129] and CryptaMail [130], which use the SwiftCoin and NXT [131] private blockchains, respectively, to store the emails in a decentralised fashion. Neither of these email applications appear to be actively under development at present.

3.6 Identity management

Blockchain provides verifiable data exchange, and one of the "killer apps" for this technology may be identity management, or user authentication. The US Department of Homeland Security gave four Small Business Innovation Research (SBIR) grants in 2016, to develop blockchain-based identity management capabilities. The call for proposals noted that blockchain technologies "potentially offer a flexible, resilient and potentially lower cost alternative to current Homeland Security Enterprise identity management capabilities". Pomcor [132] received one of the SBIR grants, and investigated a public key infrastructure (PKI) implemented on a blockchain [133].

Currently, users must establish multiple accounts, to engage with each of many services across government, banking, healthcare and social media. This gives wide exposure to personal information, relying on the services' own security as well as the user's ability to remember many passwords. Digital identity management has the potential to increase security and privacy, and blockchain is one possible technology to support this [134, 135]. Estonia has embedded blockchain technologies in its national identity management system, a response to the sustained distributed denial of service (DDoS) attack in 2007, which shut down the nation's access to the internet. The national e-identity cards [12] are integrated with the KSI blockchain from Guardtime [136]; note that this technology is not immune to bugs: the cards were frozen after a security flaw was discovered in 2017, and must be updated [137].

The Government of Canada recently announced it is designing, in collaboration with the Netherlands, a pilot project to use biometrics and cryptography in conjunction with distributed ledger technology for cross-border travel [13]. Several United Nations entities are investigating the use of blockchain technology to support a range of objectives [21]. A Blockchain Commission [22] was established by the Global Partnerships Forum [138], to explore blockchain applications to further humanitarian causes. Microsoft and Accenture have already collaborated to bring a biometric, blockchain-based identity system designed for refugees and other vulnerable populations [139].

Identity management systems have been introduced in conjunction with cryptocurrencies. An example was BitID [140], which operated on the Bitcoin blockchain (it is not clear if the current BitID app [141] is the same product). In this implementation, the user creates an identity token, based on a pre-existing authenticated identity, such as a bank account, which is recorded on the blockchain. Another user that wants to verify the identity then uses a BitID protocol that searches the blockchain, and confirms that the identity token exists there. Such an identity system might be used, for example, to replace Facebook sign-in to discussion sections on news websites. The user maintains their privacy, because their actual identification documents are not stored on the blockchain. BitAuth is a similar application, also operating on the Bitcoin blockchain; its launch announcement [142] noted the added security offered because no users' passwords are stored on a server – this has been a continuing source of security compromise [143].

A commercial application for enterprise clients is ShoBadge, in which users' mobile devices store their identification and share it on the blockchain [144]. Multi-factor authentication, such as passwords and biometric data, in this case facial recognition, is used to validate the user's access to the device, which then provides access to computers and workspaces. The Civic application allows a more flexible selection of validation criteria, which are confirmed by different entities such as banks and government agencies and then stored as 'attestations' on the blockchain [145]. These attestations would be for sale, using smart contracts on the blockchain, to other service providers requiring identity confirmation, who would pay using blockchain token as currency. This system is expected to be launched in late 2018.

SecureKey [146], based in Toronto, is working with IBM and a range of Canadian banks to develop a blockchain-based digital identity network based on HyperLedger Fabric [31]. The system is expected to be launched in early 2018.

3.7 Government and military cybersecurity

In December 2017, a new US Defense Bill was signed, which included a provision requiring the Secretary of Defense to provide a briefing within six months on the use of blockchain technology in defensive and offensive cyber applications [14]. In addition to the secure messaging blockchain application (Section 3.5), recent DARPA awards include one to Galois [147] to formally verify Guardtime's blockchain technology [136].

Other blockchain efforts in the US military and defence industry include the US Navy's trial to use blockchain to share data securely among the sites where it uses 3-D printers [148, 149]. Lockheed Martin announced a contract with Guardtime Federal [136] to incorporate blockchain technology into its "Cyber Aware Systems Engineering" concept, and to increase the security of its development processes in software and supply chain risk management.

The US Department of Energy is also exploring the use of blockchain [18] within the fossil fuel energy system, for example to record sensor and actuator data with the aim of detecting cybersecurity threats and hacks.

4 Vulnerabilities

While cryptographically linking blocks of protected data provides a high degree of security from malicious or ignorant players, blockchains are not immune from attack. Some attacks are specific to the consensus mechanism chosen, and others are more general.

Public blockchains are susceptible to denial of service (DoS) attacks; proof-of-work consensus, as used by Bitcoin and by the original implementation of Ethereum, is judged to be more susceptible to DoS attacks than proof-of-stake consensus [150]. Ethereum was subjected to an extended DDoS attack in September/October 2016 that caused clients to run out of memory by forcing each transaction (smart contract) to check the code of other transactions in the network. As noted in Section 2.3.2, a hard fork is anticipated by which Ethereum will convert to proof-of-stake consensus.

The proof-of-work consensus mechanism used in Bitcoin and other blockchain implementations is vulnerable to the "51% attack", in which one entity owning more than 50% of the computational resources in the blockchain can alter the history as well as the future of the blockchain, including enabling double spending. This attack was foreseen, but underplayed, in the original Bitcoin paper [2]. There is a lengthy discussion in [151] addressing many ways in which owning the consensus would undermine the integrity of a Bitcoin-type blockchain. Reports of short-term majority ownership of computing resources, or "hash power" have been reported, e.g., in [151], and it is noted that this condition can be created by creating an incentive for other nodes to divert their computing resources to mine for a different cryptocurrency temporarily. In November 2017, only four miners were responsible for creating over 56% of the almost 2500 blocks added to the Bitcoin blockchain. In a given 24 hr period observed in that month, only three miners accounted for over 50% of new blocks [152]. It would seem that collusion is a realistic risk under this scenario.

With a smaller cartel, selfish nodes can disrupt the blockchain by exploiting its longest chain rule, discussed in Section 2.3.1 as the way to recover from forks. The cartel can use its limited computing resources to generate more blocks, and keep them secret from the remainder of the mining community before revealing a longer block than the public one, which would then be accepted and used instead [153]. This "selfish mining attack" would result in mining profits going to the cartel.

An attack equivalent to the 51% proof-of-work attack is possible in a proof-of-stake consensus blockchain, if one node owns, or holds the lease to, more than 50% of the cryptocurrency [154]. Such a node can retroactively alter existing blocks - this is known as the "long range attack" or "history attack" [155]. Nodes might also increase their chance of being assigned opportunities to generate blocks by using their computational resources to manipulate the random process [155]; this is called a "stake grinding attack".

When the blockchain is forked, nodes can mine each set of blocks, which further increases the number of forks but does not risk the nodes' stakes [155]. This "nothing at stake attack" also increases the time before the network reaches consensus and eliminates sub-chains, expanding the attack surface. This is a vulnerability identified in the proof-of-stake consensus mechanism, and is also a potential vulnerability in other less popular schemes [156]. Proof-of-value consensus mechanisms may also be exploited by generating and validating false transactions to inflate the perceived contributions of the node [157].

In addition to vulnerabilities in the consensus mechanism, security issues have been found in implementations of blockchain code, for example: blockheader overflow in Ethereum [158]; timing leak in authentication in Bitcoin [158]; and buffer overflow in Dogecoin [159]. (Note that Dogecoin was founded as a "joke", but in the cryptocurrency hype, recently saw its market capitalisation exceed $2 billion [160].)

Ethereum suffered another large scale attack in June 2016, resulting from a feature of the smart contract blockchain that results in the contract code being executed exactly as written, and any errors or exception condition omissions are not correctible. A distributed crowdfunding system, the Distributed Autonomous Organisation (DAO), was created using Ethereum to provide a platform for popularity-based funding from the community of users. The DAO, in which the operations and governance were implemented in smart contracts and were run autonomously, collected $150m USD in pledges (in the cryptocurrency Ether) in a short period after start up [161]. Within a few weeks, a user exploited a bug in the contract code to extract $60m USD using transactions deemed legitimate within the contract construct.

In recent expensive incident [162], a coding error resulted in approximately $14m USD being trapped in a contract that was part of the Ethereum implementation of a bitcoin exchange, Quadrigacx [163].

Particular points of weakness in cryptocurrencies are the interfaces, rather than the blockchains themselves. For example, cryptocurrency wallets, software for users to store their keys and to communicate transactions with the blockchain, have been seen to have a variety of security vulnerabilities [164–167]. The Meltdown and Spectre exploits announced in January 2018 [168] also pose a threat to cryptocurrency wallets [169]. Wallets providing additional security to protect Bitcoin assets are available from Xapo, which stores the cryptographic keys in offline servers, physically secured, and located in underground bunkers [170].

Cryptocurrency exchanges, where crypto- and fiat currencies can be traded, have been subject to big losses due to hacking attacks, for example [171–173]. The Youbit exchange hack in December 2017 resulted in the bankcrupcy of the South Korean exchange [174]. In the largest cryptocurrency hack to-date, $530m USD was stolen from the Coincheck exchange in a January 2018 [175]. Cyber attacks on exchanges have been attributed to stated-sponsored groups [176]. Cryptocurrency exchanges have also been susceptible to DDoS attacks [177], for example, according to Reuters [178], one of the largest exchanges, Bitfinex, experienced attacks in February, June and December 2017.

5 Blockchain in tactical networks

The key feature of blockchain technology is data integrity in a trustless environment: transaction or data records included on the blockchain are timestamped, cryptographically protected and stored by many distributed nodes, reducing the risk of total loss. For a sufficiently long blockchain, with a large number of nodes, the records can be considered immutable, in the sense that any tampering will be evident. This integrity can be exploited in different ways to enhance the robustness and resilience of tactical networks, and some of these are discussed in Section 5.1.

Smart contracts, described in Section 3.2, also provide opportunities for robust resource management in tactical networks, particularly in complex operational conditions where many users interact in the electromagnetic (EM) spectrum. Possible applications of blockchain to resource management are discussed in Section 5.2.

Tactical environments pose particular challenges for the introduction of blockchain technology, as devices are constrained in size, weight and power, and there are physical limitations on node connectivity. These challenges are considered in Section 5.3.

An example architecture for applying blockchain technology to support tactical operations is described in Section 5.4, taking into account the opportunities and challenges outlined thus far.

In this section, network nodes are considered to be the devices or platforms connected to the blockchain network; these are not (just) the radio interfaces themselves, but may be auxiliary equipment such as biometric devices, weapons or communication platforms.

5.1 Integrity

Blockchains enhance the integrity of the data stored, because the linking from one block to the next makes the adversary's ability to tamper with prior blocks extremely computationally intensive (see Section 2.2.1). This feature can be exploited in several ways in military systems, as outlined below. Note that, for data records, only the document hash is stored in the blockchain, which opens the possibility for tracking data at different security levels within the same chain [179].

5.1.1 Supply chain

Under US law, the Department of Defense is required to address detection and avoidance of counterfeit electronic parts; a similar requirement for the US National Aeronautics and Space Administration (NASA) was introduced in 2014, but held up in the legislative process [180]. In Canada, counterfeit electronic components have been found in military aircraft [181] (see also the response from the Department of National Defence (DND) [182]), but no similar law has yet been introduced.

Tracking the origins of the components in any significant military asset is a massive challenge, as there are many, often long and intertwined, supply chains. In many cases, parts are replaced throughout an asset's lifespan, further complicating the problem. Blockchain provides one approach to tracking the provenance of each component, in which each manufacturer and distributor would register their ownership and safety certificates into the blockchain throughout the manufacturing process [99, 100, 157, 183].

A supply chain blockchain would be write accessible to all entities coming into contact with components throughout the asset's lifespan, but permissioning would restrict their read access to relevant records. Thus, a single blockchain could support the entire asset-registry for the whole department, or government. In this permissioned blockchain, blocks would be generated by distributed, trusted nodes, eliminating the need for high-complexity mathematical computations such as proof-of-work. All users could validate each block, verifying that their own records are included and correct.

The size of a department- or government-wide blockchain, in terms of numbers of blocks and nodes, would give it strong integrity and resistance to attacks, but the verification performed by the miners cannot ensure the accuracy of the information stored. The validity of the information recorded is dependent on the integrity of those submitting it: a rogue node submitting false documentation can provide a valid data hash, and that will be recorded in the blockchain indistinguishable from accurate and true information.

5.1.2 Updates

Networked devices periodically require firmware and software updates, and these are usually received automatically. But as noted in [184], there are incidents where "hackers have hijacked software's own immune system to deliver their infections", i.e., the act of updating is a vulnerability. In [103], it was proposed that IoT devices could increase the security of updates using blockchain technology; IoT devices would be on their manufacturer's blockchain, and the manufacturer would use smart contracts to register the (hash of) their updates on that blockchain. When the devices search the blockchain for updates, they retrieve the hash and can request the update from the network.

For tactical equipment, it is to be hoped that devices are not updated while deployed, but with the anticipated increase in the number of connected devices used in operations, ensuring they are all updated with the same, most recent firm- and software is a significant task. Utilising a blockchain, such as the one discussed in Section 5.1.1, could facilitate this task.

5.1.3 Auditing

Blockchain can be thought of as a distributed ledger, and can serve as an audit trail for a wide variety of functions in tactical operational environments. For example, data from distributed networked sensors can be timestamped and recorded in the blockchain, along with command and control messaging among effectors, providing a means for post-action analysis and battle damage assessment in, e.g., cyber EM activities (CEMA) [185]. Other auditing functions might include force position information, health status of assets and other situational awareness data. The immutability of the data provides an incontrovertable record, which should support forensic investigations of operational activities, and many distributed copies means that data loss is highly unlikely. The process of generating the blockchain generally means that the information is, within a few recent blocks, reconciled across the network nodes.

5.1.4 System integrity

Cyber physical systems, i.e., systems that integrate physical and computational components [186] such as sensors, are at risk of attacks on several fronts. The physical interfaces provide potential attack surfaces, which can be used to violate the integrity of the software, firmware and data on the device. Blockchain provides a possible technology for supporting the detection of changes to these, as suggested in [183]: the system is imaged initially, and the hash of that image is stored on the blockchain. When legitimate updates are made, the new images are stored and timestamped on the blockchain. To check the system's integrity, it is re-imaged periodically and compared to the most recent stored version: any variations should be quickly detected when the hashes do not match.

As with biometrics and other tools for identity management (Section 5.1.5), system integrity checks could be vulnerable to attackers using stored images, rather than new ones, defeating the objective of detecting changes.

5.1.5 Identity management and authentication

As noted in Section 3.6, identity management and authentication may be able to make early and advantageous use of blockchain technology. Different forms of identity sources, such as biometrics and system images (Section 5.1.4), registered in a decentralised and distributed ledger, enabling user and device authentication to support data access, secure communications and trackability, militate against the need for a vulnerable centralised repository of stored identities. The use of cryptographic tools means that the identity sources themselves are not stored on the blockchain, reducing the impact of a security breach. A similar approach was proposed in [187] to support trust and authentication applications using blockchains. However, note that the blockchain should not be viewed as a fixed but distributed database, storing only identity information. The chain must continue to grow in order to maintain the integrity of the data contained (Section 5.3.6).

As discussed below in Section 5.3, wireless networks can become partitioned, and using centrally-held identity information, nodes that are unable to access that information may become partially paralysed. With distributed storage, those nodes would still have access to be able to authenticate other nodes that remain within reach, but would not have access to changes that occurred since partition, such as node revocation.

Other challenges noted in Section 5.3 include bandwidth and processing requirements for extending the blockchain. Additions to the blockchain for identity and authentication purposes should be few, during operations, although the capability to exchange or add sensors, for example, is important. An additional useful feature would be to combine or bridge blockchains, for example when a mobile unit comes within range of a sensor network or other unit, which would enable rapid acquisition of access to the users, nodes and/or data in the other network.

5.1.6 Communication

The secure communication platforms providing social media functionality, discussed in Section 3.5, might find utility for morale purposes, enabling Canadian Armed Forces (CAF) members to decompress and hold secure, off-the-record discussions with limited potential for them to be leaked to adversaries or the public. They do not, in general, appear to be appropriate for secure operational command and control communications.

The secure authentication blockchain outlined in Section 5.1.5 could be used to provide identity management and key distribution. This would support secure tactical communications, providing secure addressing and user authentication to establish communication sessions using updated cryptographic keys. Communications could be directed at specific users or devices, depending on the scenario and identities stored.

Auditing of communications could be provided by storing encrypted details on local devices, and periodically registering hash functions of those records on the blockchain.

5.2 Resource management

Managing resources involves tracking expenditures and exchanges, and ensuring that service level agreements (SLAs) are respected. There are several resource management tasks in tactical networks that might be supported by blockchain technology.

5.2.1 Network management

According to [188], blockchain technology can be applicable wherever centralised control is used for network management. For example, software defined networks (SDNs) make use of logically, if not physically, centralised control. Blockchain could be used to track and configure each network device without relying on a central controller [189], and smart contracts could be used to automatically reconfigure the network when links or nodes fail. It remains to be seen whether SDN has a useful role to play in tactical networks; work is underway within The Technical Cooperation Program (TTCP) community to investigate its potential implementation and vulnerabilities [190].

Applications in which blockchain could contribute to managing networks in coalition tactical operations were proposed in [179]. One is essentially a federated mission network (FMN) deployment [191], in which coalition members share assets; in [179], it was suggested that the blockchain could be used to record commands given by one nation to configure assets owned by another, creating an audit trail for post-mission analysis. The second application proposed in [179] is to maintain a cross-coalition inventory of assets, to track their availability and deployment. Finally, also in [179], a somewhat complicated process was envisioned in which a robot-assisted human tracks records that are transferred between networks at different security levels.

The opportunities to exploit distributed ledger technology to assist in the management of coalition tactical networks are broader than those proposed so far. The North Atlantic Treaty Organisation (NATO) FMN concept, agreed in 2012, is based on lessons learned from the Afghan Mission Network [192]. The aim is to rapidly and efficiently provide connectivity to a federated environment for forces participating in a joint operation, and the goal is to support command, control and decision making. FMN is based on an agreed set of standards, policies and doctrine, including joining, membership and exit instructions (JMEI). Trust and security criteria are agreed among the participants. All these characteristics are essentially rules and policies that could be implemented as smart contracts on an FMN blockchain, also providing identity management, authentication and addressing across the coalition. The audit function could be used to track the exchange of operation and network management information, as well as the adherence to SLAs related to resource sharing and quality of service. Gaps in current FMN proposals were identified in [191], including automated network configuration and service provisioning and cross-federation network information sharing and security provisioning; blockchain may provide a mechanism to support these functions in a distributed and secure way.

5.2.2 Policy enforcement

As noted in Section 5.2.1, blockchain smart contracts can be used to enforce network management policies, and the same blockchain can be used to provide an audit trail. Other policies maybe used within networks, for example, selecting bearers to meet requirements such as quality of service, quality of protection and user demand [193], might be enforced using smart contracts on a blockchain, simultaneously generating and storing an immutable audit trail. In a coalition environment, access to other shared resources, in particular spectrum, might be subject to agreed policies, and these can also be enforced using smart contracts.

5.2.3 Spectrum sharing

Spectrum is a limited resource, with high demand particularly during coalition activities; different approaches to spectrum sharing have been proposed, most of which are based on some form of policy framework [194]. Policies may dictate how much spectrum may be accessed, and at what times of day, as well as conditions for evacuation in favour of a higher priority user. The integrity of, and conformity to, these policies is critical to mission success, as modifications or violations may result in spectrum fratricide or inability to access the spectrum at all [195]. The integrity of the spectrum policies, and their enforcement and auditing, could be achieved using blockchain technology.

5.3 Challenges

Application of blockchain technology in tactical networks has particular challenges due to the physical restrictions on portable devices, and to the possibly dynamic and unpredictable wireless connections among the nodes. The size of the network is also a factor in whether blockchain is a useful addition to the tactical technology toolbox.

5.3.1 Platforms

Remarkable advances in processing technology have enabled highly sophisticated handheld computing devices. However, these devices have limited amounts of memory, battery life and processing power available to service an additional application such as blockchain. The power and processing limits indicate that efficient block generation and consensus mechanisms are required. Designing the system such that each node stores only its own data and transactions, and does not need to maintain records of all other nodes' transactions, will reduce the memory requirements. However, as the blockchain grows, the memory requirements at each node increase as it should store the entire blockchain to achieve the full benefits.

The most power- and processing-efficient consensus mechanisms rely on some level of existing trust, for example the round robin mechanism, in which nodes take turns, or the PBFT consensus (Section 2.2.2). The former reduces the security of the blockchain, as a rogue node would get opportunities to generate blocks, and thereby override the integrity of the data stored. The latter, while it maintains confidence in the block generation, requires a higher level of data exchange among the nodes, which is problematic when there is limited bandwidth or connectivity.

5.3.2 Bandwidth

Tactical networks are, typically, bandwidth constrained. The high demands for network connectivity to support situational awareness (SA) and command and control (C2) messaging, and the congested radio spectrum, mean that throughput is at a premium. There are different possible blockchain architectures (Section 5.4) with different data exchange requirements, but it is the exchange of information, both transactions and blocks, that provides the integrity for which the blockchain is valued. This trade-off between bandwidth and blockchain value may significantly hamper efforts to integrate blockchain into tactical operations.

5.3.3 Latency

To ensure all nodes in the network have a reasonably up-to-date version of the same blockchain (consistency), the transactions incorporated into blocks, and the blocks themselves, must be available to all nodes within a relatively small time interval. Processing in the nodes also causes latency: see [196] for an evaluation of the block computation times, including parameters such as message size and library access overhead. In general, small relative delays can be dealt with by requiring nodes to wait before processing messages, mimicing syncronicity, however this fails in the case of proof-of-work consensus [197]. Analysis of proof-of-work consensus in [198] showed that as synchronicity degrades, the security of the blockchain degrades, meaning that attackers can more easily generate and add false blocks to the chain.

One potential problem arising from low-capability platforms and limited bandwidth was identified in [199], and is known as the ‘FLP result’: *viz.* “no completely asynchronous consensus protocol can tolerate even a single unannounced process death.” The idea is that when processors take different amounts of time to receive and process messages to come to their own decisions, for example, it is impossible for the rest of the network to know whether a node has failed, or has yet to make a decision. In principle, this applies to a wireless network in which some nodes may have slow or heavily-loaded processors, and where message delivery may be delayed.

As noted above, applying analytical results to real implementations must be done with care, as the assumptions made in the analysis may be invalid in practice. Nonetheless, it is important to consider the effects of delays and lack of synchronicity in developing an architecture and selecting a consensus mechanism.

5.3.4 Connectivity

In mobile networks, or static networks where weak links may become disconnected due to changing local environments, end-to-end connectivity across a network may be lost periodically. While this causes temporary disruptions for most applications, for blockchain the partitioning of a network can be critical.

Brewer’s Theorem, formalised in [200], shows that it is not possible to achieve all three of consistency, availability and partition tolerance (these properties lead to Brewer’s Theorem’s more commonly-used name, the CAP Theorem). In the context of blockchain:

consistency means that each node has only the same, current version of the blockchain;

availability means that each node can always access any data contained in the blockchain; and

partition tolerance means that when some nodes become unreachable from the rest, the blockchain continues to function as expected.

The CAP Theorem means that the blockchain cannot provide full availability or consistency and also be tolerant to partitions. This means when a network partition does occur, the blockchain in the two subnetworks will continue to grow, adding blocks to the same root chain. When the subnetworks reconnect, there are two versions of the post-partition chain, which are not reconcilable. Equivalently, if a blockchain were designed to be tolerant to partitions, it could not also be both consistent and available.

The design of permissionless cryptocurrency blockchains, based on Nakomoto's original work [2], resolves this by selecting the longest chain, and then incorporating the transactions from in the discarded subchain into future blocks. This can be achieved because the transactions are broadcast through the network, until all nodes agree that they have been included in a block in the chain. However, this repeated broadcasting is an inefficient use of the available bandwidth, and should be avoided where possible. Further, when network partitions rejoin, there is an increase in required bandwidth to support core functions such as SA and C2, as well as network management.

The longest chain approach to dealing with network partition is widespread in cryptocurrency blockchains. This leaves a trade-off to be made between consistency and availability. Proof-of-work and proof-of-stake blockchain consensus mechanisms are designed to value availability over consistency [55], while PBFT-style consensus algorithms can be designed either way, but tend toward consistency as a preferred option.

5.3.5 Network size

The impact of network size, i.e., the number of nodes, on the blockchain's security depends on the consensus mechanism, but in general, with more nodes validating blocks, it becomes harder for attackers to introduce false blocks [183]. However, as the network size increases, the issues of latency, bandwidth and possibly connectivity become more significant. To enable trade-off between the benefit of network size and the costs of bandwidth requirements and latency, a clustering approach could be implemented in which a group of users submits their transactions to a cluster head node, which combines and hashes them, and sends the single Merkle root into the network. A clustering concept was proposed in [109] for reducing the overhead in an IoT blockchain. For example, multiple wearable devices could be grouped into a personal area network cluster, which is a node in the area tactical network (see Section 5.4).

Security in a clustered network hierarchy may introduce new vulnerabilities; for example, in the wearable device scenario above, compromising the cluster head node would allow the attacker to introduce false transactions into the local combined hash functon, which would not then be verifiable by other nodes in the network. The issue of data or transaction verification and validation is considered in Section 5.3.7.

5.3.6 Blockchain length

The length of the blockchain determines the immutability of the data stored in it: the more blocks there are, the more effort an attacker would need to expend to regenerate and replace one or more blocks in the chain. The chain should thus grow over time, to keep increasing the challenge for the attacker. In typical implementations of permissionless blockchains, such as those used for cryptocurrencies, there is a longest chain rule, such that soft forks are resolved by selecting the longest chain. In these, an attacker might race to add more blocks to the chain than the honest nodes, such that its corrupted chain is accepted by the network. The blockchain would then grow faster than predicted: this type of attack could overwhelm the memory capacity of a mobile device.

As each node should maintain its own copy of the entire blockchain to take advantage of the immutability properties, the memory requirements may be considerable. Further, when networks merge or new nodes join, ideally they should receive the entire blockchain so they can fully benefit from it. In limited bandwidth tactical networks, this may be an unachievable goal. Thus, as with network size, there is a trade-off between security due to blockchain length and the combination of bandwidth, latency, memory and power resources.

The problem of limited device capacity could be addressed by periodically transferring segments of the blockchain over a wideband backhaul link to secure storage, and to treat the retained blocks at the tactical edge as a new genesis block or short chain. There is an increased risk of compromise with this approach, as the backhaul becomes a target for attackers, and the shorter retained chain is less secure than the full length. A more secure alternative is to prune the blocks, removing the transactions themselves and keeping only the block headers. The originating information for the transactions must still be retained somewhere, but not at every blockchain node.

5.3.7 Data verification and validation

As described in Section 2.2, transaction verification is the process of checking its structure and signature. When the blockchain is used to transfer assets, validation involves confirming that the user transferring the assets actually owns them - this information is contained in the blockchain itself, in an earlier block.

In tactical networks, where device ownership may change hands, for example, soldiers exchanging radios when one malfunctions, verification should include additional checks to authenticate the device and its human user. This could be achieved by adding hash functions of system images (Sections 5.1.4) and user biometrics (Section 5.1.5). Validation of this type of transaction is critical, as failure would expose the whole network by allowing an attacker access by compromising a node. However, it is clear that if the transaction consists of, for example, SA information to support post-action analysis (Section 5.1.3), there is no mechanism to validate that the information itself is correct.

A validation process is required when data stored in the blockchain is updated, e.g., ownership of an asset such as a radio changes. When the transactions consist of information for future auditing, no validation is required; this is reminiscent of the timestamping origins of blockchain (Section 2.1). These two cases can coexist on the same blockchain, and their combination makes the blockchain longer, and therefore more secure, in general, but more resource intensive to maintain (Section 5.3.6).

5.4 Example tactical blockchain architecture

Based on the preceding, we propose an example architecture for a tactical blockchain system. The scenario we consider consists of a unit of dismounted soldiers, each carrying several devices connected on a personal network: a weapon, a radio, a camera, a radio frequency (RF) sensor and a computer (similar to a smart phone), sharing a battery and a memory drive such as a flash card. The soldier is also considered a network component, as they are a source and sink of data, and their identity is confirmed using a networked biometric sensor such as a fingerprint or iris scanner. The other devices may be authenticated using a radio frequency identification (RFID) chip or imaging as described in Section 5.1.4; authentication will only be required if the networked component has been disconnected from the personal network and attempts to rejoin.

We assume that the weapon tracks the ammunition it uses, and records the amount remaining. The camera may be continually recording, but to limit memory usage, only a few seconds before and after the weapon is fired are retained. C2 and other messages, either digital voice or data to and from the computer, all passed via the radio, are recorded for post-action analysis. SA in the form of RF sensor data is sampled periodically, and transferred via the radio to other soldiers in the unit and recorded locally. These different sources of data all use the computer's memory for storage; both the memory and battery usage are tracked.

We use blockchains to provide authentication and identification management for the soldiers and devices engaged in the operation, an auditing function to track cyber SA and C2, resource usage tracking, and a policy management function, which is used to support resource loading decisions across the unit. As noted in Section 5.3.6, the longer the blockchain, the stronger it is, so all these functions use the same blockchain within their cluster (Section 5.4.1).

This is a simplified scenario, intended to give insight into the potential application of blockchain technology in tactical networks. Note that, as discussed in Section 6, the fact that this technology might be used to address these problems does not mean it is the best choice. Note also that the exchange of transactions and blocks among the users is assumed to be secure.

5.4.1 Clustering

We group networked components by location into clusters, as illustrated in Figure 4.

Each soldier and their own devices are considered a single *personal cluster*: these clusters generally have static membership, however it must be possible to support devices being added, removed or replaced as equipment may fail mid-mission. The computer will be considered as the head of the personal cluster, and is the personal cluster node in the local cluster.

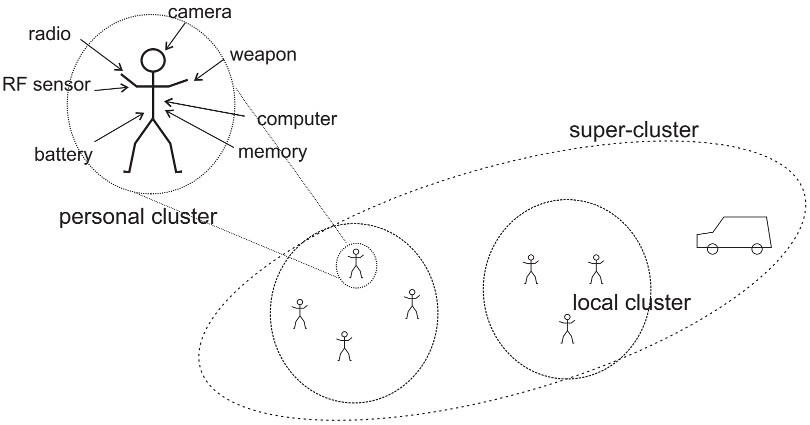


Figure 4: *Tactical clusters.*

Within the personal cluster, the users may be connected by wire, or by low power wireless. All devices are within range of one another, which has several advantages, including limiting the networking protocol overhead and costs of relaying. In addition, to address the platform and bandwidth limitations identified in Sections 5.3.1 and 5.3.2, clustering allows trade-offs among range, bandwidth and power, and supports re-use of spectrum across the whole unit. However, as noted in Section 5.3.5, fewer nodes in the blockchain reduces its strength; we address this in part by cross-registering information across cluster boundaries.

Soldiers are grouped by geographic proximity into *local clusters*, and the cluster size is such that all soldiers are within range of one another. This means the membership of the clusters is dynamic as the soldiers' relative positions change and they move from one cluster to another. At any given time, one soldier, or more specifically, their computer, will be designated as a clusterhead. The purpose of this cluster is to provide consensus to increase the integrity of the data registered in the local cluster blockchain.

The whole unit, and supporting platforms such as armoured carriers, also form a *super-cluster*, which might be connected via a backhaul link to a headquarters. The high level blockchain in this cluster further increases data integrity of the lower level blockchains, and also provides the backbone to support an authentication capability for all the networked devices. Due to the geographical size of the super-cluster, the nodes are not all connected directly to one another, but must use relays to reach from one cluster extreme to the other; this introduces additional overhead and latency into the transaction and block exchanges. It is assumed that there is at least one higher powered and secured node, a 'super-node', such as a vehicular platform, that can provide block mining capabilities. If not, the mining effort would be shared, as in the local cluster.

5.4.2 Layered model

There is an emerging view that blockchain should be considered as a stack of layers, as is accepted in standard networking. As with the network layered stack model, it is to be expected that formalising the architecture of blockchain applications would allow for increased flexibility, scalability and rapid design and implementation, potentially at the cost of efficiency and performance. There is no single accepted layered stack model for blockchain yet; several have been proposed with three, four or five layers, for example [201–205]; some of these are for very specific applications.

We propose a general layered model for tactical applications in Figure 5. The layering is designed to provide flexibility, even within a single deployment, as illustrated in subsequent sections.

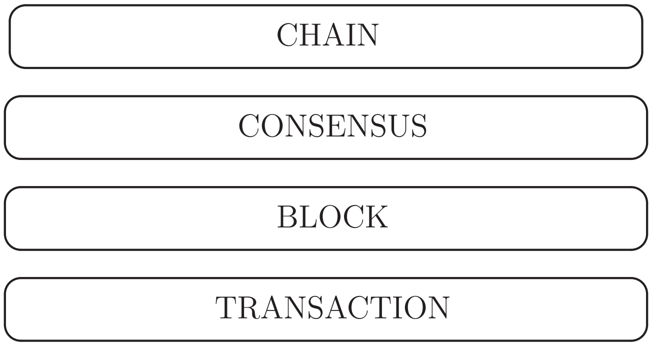


Figure 5: *Proposed blockchain layers.*

5.4.3 Personal cluster

Within a personal cluster, the main blockchain function is auditing, but tracking of resources is also required. In this architecture, authentication of devices will be achieved using the super-cluster blockchain, so this will be addressed in Section 5.4.5.

The blockchain layers in the personal cluster are implemented as follows.

Transaction layer

As a digital file, containing recorded messaging, camera recording or RF sensor measurements, is saved to the networked memory device, the computer calculates its hash function and generates a transaction, whose structure might be defined as in Figure 6(a).

The level of resources such as ammunition, battery or memory capacity can also be stored on the blockchain: this could be used in after-action analysis to assess the rate of usage, as well as being used to make local command decisions within the unit. A possible structure for a transaction to register this information on the blockchain is shown in Figure 6(b). Note that in this case, the data stored includes the transaction number for the previous recording of resource state: this allows for easier tracking.

Each transactions is signed using the originating device’s digital signature. There are several options of suitable public key cryptographic tools – Bitcoin and Ethereum both use the elliptical curve digital signature algorithm (ECDSA) [206].

FIELD	SIZE (bytes)
Trans. type = “AUDIT”	1
Transaction ID	4
Device ID	8
Data hash	32
Public key	33
Signature	72

(a) Audit transaction

FIELD	SIZE (bytes)
Trans. type = “RESOURCE”	1
Transaction ID	4
Device ID	8
Resource type = "AMMO"	2
Resource used	8
Previous transaction ID	4
Public key	33
Signature	72

(b) Resource transaction

Figure 6: *Personal cluster transaction structures.*

Block layer

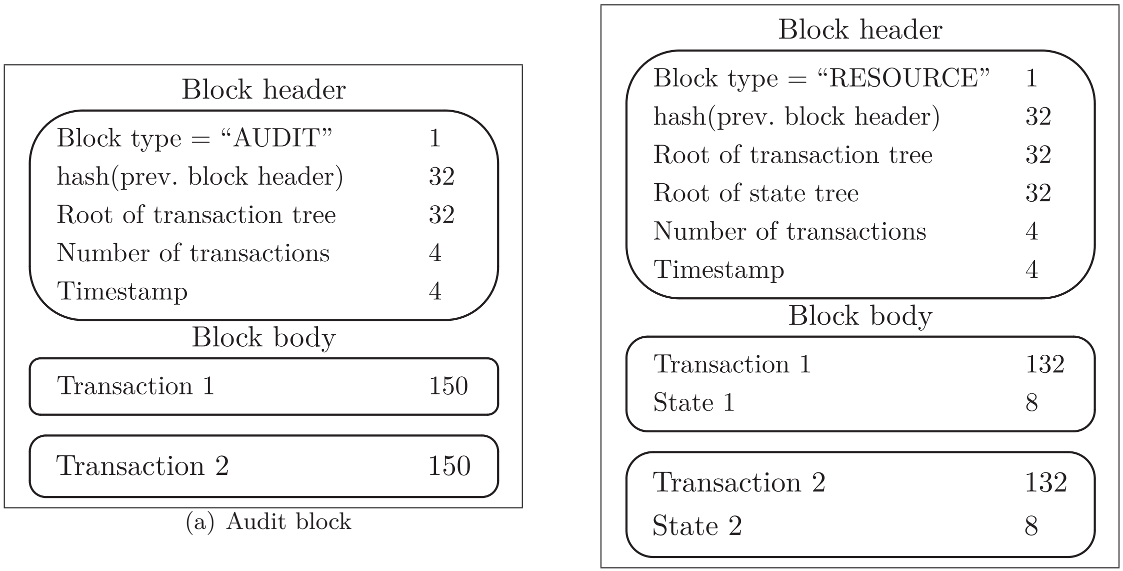
We allow different types of blocks in the same chain, corresponding to the different types of transactions. The blocks for audit and resource transactions are illustrated in Figure 7(a) and (b), respectively.

The transactions of the given type submitted by the networked devices are collected over a prescribed interval, for example, 15 mins, and are assembled into a single block. First, the structure and digital signature of each transaction is verified: these form the block body. The computer node may authenticate each device based on the super-cluster blockchain (Section 5.4.5).

The root of the Merkle tree of the hash functions of the transactions is computed, see Figure 1. The block header contains its type (audit or resource); the hash of the previous block header; the root of the Merkle tree to provide data integrity; the number of transactions included; and a timestamp, which not only supports tracking, but also introduces an extra source of randomness for the header hash function.

In this example, the resource block also tracks the state of resources, so an additional Merkle tree is computed based on the output of the transactions, e.g., the number of ammunition rounds or battery capacity remaining.

The personal cluster contains only a few devices, so each tree contains few if any leaves, in any interval. If no transmissions are submitted in an interval, an empty block would be generated to keep the blockchain growing and reducing its potential vulnerability to tampering. The root hash in an empty block should be randomly selected, as it serves to provide an additional variable for the header hash.



(a) Audit block

(b) Resource block

Figure 7: *Personal cluster block structures.*

Consensus layer

In the personal cluster, there is a single 'miner' generating blocks, *viz.* the computer, and no other nodes need to check each block's veracity. Therefore, there is no consensus protocol in this personal cluster blockchain.

Chain layer

The blockchain is constructed by the inclusion in each block header of the hash of the previous block's header, as shown in Figure 7.

To be able to locate old transactions within the blockchain quickly, they should be indexed. In this case, the computer should also maintain a database of transaction numbers and the blocks in which they are held.

5.4.4 Local cluster

In the local cluster, there are multiple computer nodes, which means that a consensus protocol can be implemented. This also requires the propagation of transactions and blocks around the cluster. As this is a permissioned, sovereign blockchain, the nodes do not need to compete to mine blocks; instead, we assume one soldier's computer is denoted the clusterhead at any time, and it generates the blocks. The other nodes validate the blocks to achieve consensus, which increases the security of the blockchain.

This cluster provides a registration forum for each soldier's personal cluster, to increase its resistance to tampering. The personal clusters can periodically record details of their own state and register the devices engaged in that local cluster, in an auditing function. The blockchain can also be used to support resource management among the soldiers in the cluster: in this example, when the battery resources used by the clusterhead node exceed some threshold, the blockchain can be used to move the clusterhead role to the node that has the most remaining resources. As with the personal cluster, authentication of nodes is achieved using the super-cluster blockchain (Section 5.4.5).

One of the challenges of the mobile environment is that the members of clusters may change, as soldiers move into and out of range[6]. The cluster blockchain must therefore accommodate the migration in of new nodes, and the departure of current member nodes – this departure may be unannounced if the node suddenly loses connectivity.

Unlike the large, permissionless blockchains like those described in Section 2.3, we do not aim to have every node in the cluster have identical versions of the blockchain as this would require too much bandwidth and processing power to exchange blocks, and to manage forks and sidechains. Instead, we allow that the clusterhead of one local cluster can query nodes in another cluster to update their own stored information, if necessary. Note that, although the blockchains stored at each node are not reconciled, all the transactions are recorded and linked, and can be resolved in after-action analysis, as long as they are not lost.

Transaction layer

As in the personal cluster, the local cluster has an auditing function; in this case, to record the status of the personal clusters and of their component devices. Computing the blocks for the cluster requires expendable resources, in particular battery power, thus the role of clusterhead must be shared among the cluster participants, and this is facilitated by tracking the resources available at each node. The transaction structures for these two functions would be quite similar to those in Section 5.4.3. These transactions must be propagated around the whole cluster, for the consensus process.

When a soldier node migrates from one cluster to another, it must create a transaction that contains details of its devices and current states. Such a transaction is illustrated in Figure 8. This transaction must also be propagated around the receiving cluster.

[6] We note that there are advantages to maintaining clusters of roughly equal size, and fewer large clusters rather than many small ones. The actual assignment of soldiers to one cluster or another is not considered here.

FIELD	SIZE (bytes)
Transaction type = “MERGE”	1
Transaction ID	4
Node ID	8
Number of devices	2
Number of resource states	2
Device ID 1	8
Device ID 2	8
⋮	⋮
Resource type 1	2
Resource 1 remaining	8
Resource type 2	2
Resource 2 remaining	8
⋮	⋮
Public key	33
Signature	72

Figure 8: *Local cluster merge transaction structure.*

Block layer

The clusterhead node is responsible for generating blocks from all the transactions within the cluster. As with the personal cluster, it is proposed this be done at regular intervals, and on demand for merges.

As in the personal cluster, we propose different types of blocks for different transaction types, and their structure would be similar to those in Section 5.4.3, with the addition of an identifier for the originating node. As before, the block generation process starts with verifying the structure and digital signature of each transaction. The nodes might also be authenticated by querying the super-cluster blockchain (Section 5.4.5).

We also require a block to incorporate the merge transaction from the migrating soldier node, which serves to link the blockchain held by the migrating soldier with the receiving cluster's to maintain data integrity. To achieve this, we propose a merge block, illustrated in Figure 9. Note that when more than one soldier node migrates to a cluster, the transactions would be incorporated into blocks separately. The block header includes the hash functions of the last block in the migrating node's blockchain and the corresponding one from the receiving cluster's blockchain, as well as the merge transaction information.

When blocks are generated, they must be propagated around the whole cluster for the consensus protocol to proceed.

Block header

Block type = "MERGE"	1
hash(prev. migrating block header)	32
hash(prev. receiving block header)	32
hash(merge transaction)	32
Timestamp	4

Block body

Merge transaction	$122 + \cdots$

Figure 9: *Local cluster merge block.*

Consensus layer

In the local cluster, the clusterhead node mines blocks, and the other nodes in the cluster check each block's integrity and communicate their agreement, or otherwise. As the number of nodes in the cluster may be unknown at any time, a fixed window is proposed within which all cluster nodes are expected to respond; among the responses, a majority decision is made. As all nodes in the cluster have the block for consensus purposes, it does not need to be propagated around the cluster again once accepted.

The use of a single node, the clusterhead, to mine the block, and the definition of clusters such that all nodes are within range of one another, means that the communication overhead to reach consensus is much lower than in permissionless blockchains.

Chain layer

When consensus is reached on the validity of each block, every node adds it to its local version of the local cluster blockchain, and performs any indexing required. Recall that each node is not expected to have the same historical blockchain, but each node in the cluster should add the same block to its version at a given time.

5.4.5 Super-cluster

We propose a super-cluster that includes all soldier nodes, and any other platforms within the unit. This blockchain supports auditing for the blockchains at the local cluster level: this is similar to the auditing function at that level and will not be detailed again. Rather, we focus on using this super-cluster blockchain to provide asset tracking and authentication functions across the whole unit. Note that authentication using a blockchain is an evolving concept; we propose an outline here of a possible approach but anticipate that much more work would need to be done in this area.

For authentication on a blockchain, not only do the authentication factors need to be stored within the chain, but so does the current state of authentication. For example, if a user can point to an old block that confirms their biometric is valid, that is not sufficient to authenticate them as their permissions may have been revoked more recently.

In a tactical scenario, it is reasonable to assume that every device in use has been provisioned securely, and as such can be registered on the blockchain prior to deployment. This means that system integrity checks, biometric features, passwords, etc., can be hashed and included as transactions in blocks similar to the auditing function illustrated in Figures 6(a) and 7(a). The ability to revoke this authentication must be carefully controlled - we conceive that this might be done through a smart contract that requires two or more inputs, for example, a failed integrity check and an order from the unit commander[7]. Similarly, a human override to deauthentication should be provided, but this is not considered here; nor are the logistics of providing new authentication factors mid-mission.

Transaction layer

Pre-mission transactions are to register the unit's devices in the super-cluster blockchain, and to assign those devices to each soldier. If there is expected to be a significant amount of device exchange, the asset management might be more effectively achieved using smart contracts. During the mission, the authentication state of every device will be tracked, and any changes to their assignments will be recorded[8].

Block layer

The super-node is responsible for mining blocks from all the transactions within the cluster. As with the lower level clusters, it is proposed this be done at regular intervals, and on demand for changes to the authentication status of devices. The structures of the blocks for the pre-mission and mission-tracking transactions follow from the lower level auditing and resource tracking blocks, respectively. Note that only the hash of the authentication factor need be stored, not the full information file.

Following the principle of different types of blocks for different purposes, we propose regular blocks storing the current authentication states. This will reduce search time when the blockchain is queried by a lower level cluster, as the information will always be held within a recent block. Further, the nature of the blockchain means that the query can be answered

[7] A smart contract could handle a more sophisticated formula to address the possibility that a commander's device might be compromised, such as inputs from two of three other unit members, but this is beyond the scope of the present work.

[8] This reassignment might be registered automatically using a proximity sensor and RFID chip on each device; the technology to achieve this is beyond our current scope.

by any node in the blockchain, as the blockchain is duplicated fully at every node in the super-cluster.

The format and implementation of smart contracts is highly dependent on the blockchain ecosystem, but they follow common programming practice. For example, smart contract pseudo-code to create authentication status storage for a device is loosely illustrated in Figure 10; similarly, and very over-simplified, an overview of how the authentication might be revoked based on inputs from an authentication request and human intervention is shown in Figure 11. In practice, a smart contract might be used to message the commander when a device fails authentication, soliciting a response to revoke or not.

```
contract deviceAuthentStorage{
   bool status;

   // default to false
   function deviceAuthentStorage(){
      status = FALSE;
   }

   function set(bool x){
      status = x;
   }

   function get() returns(bool){
      return status;
   }
}
```

Figure 10: *Device authentication status storage contract.*

```
contract deviceDeauthent{

   function deauthent(bool AuthResponse, bool CmdRevoke){

      if ((AuthResponse == FALSE) && (CmdRevoke == TRUE) {
         deviceAuthentStorage.set(FALSE);
      }
   }
}
```

Figure 11: *Device authentication revocation smart contract.*

Consensus layer

For the super-cluster blockchain, as in the local cluster, a single node generates all the blocks. These are then circulated to all the other nodes (soldiers' computers) for validation.

Achieving consensus is most complex in this case, as some nodes are likely to be multiple hops away, introducing latency and uncertainty into the communication process. A context-aware protocol is likely necessary in this case, to take into account the link quality to reach remote nodes, and to determine whether the consensus decision should wait for their input. This is a challenging problem that requires further investigation and analysis.

Chain layer

In the super-cluster, all nodes must have the same copy of the blockchain. As noted in Section 5.3.4, the blockchain cannot achieve consistency and availability in the face of network partition, or lack of connectivity to some nodes or clusters. While soft forks will not arise because a single node is responsible for mining, transactions from those partitioned nodes must be processed into blocks as soon as they re-connect, and the blocks they have missed must be propagated to them and attached to their local versions of the super-cluster blockchain in the correct order. This will require additional protocols to be built into the blockchain.

Authentication queries from the lower level clusters can be answered by any node in the super-cluster blockchain, including the soldier's computer node that is the clusterhead of the personal or local blockchain. These queries can therefore be answered rapidly with minimal overhead.

The blockchain keeps growing even in the absence of authentication state changes and device reassignments, because blocks are added periodically to register the state of the local cluster blockchain. This growth is important to maintain the integrity of the blockchain (Section 5.3.6). However, unlike the lower-level blockchains, which are not reconciled across multiple nodes, the nodes in the super-cluster can 'prune' their blockchains to reduce memory requirements. While each node must maintain the authentication factor blocks, smart contracts and recent status blocks, they do not need to keep the block bodies of older blocks that contain auditing and resource transactions. The block headers should all be retained, as their linking provides the blockchain's tamper resistance. The super-node should retain the full blockchain, for auditing purposes, unless it can reliably be transmitted to secure storage via, for example, a backhaul link.

6 Conclusions

This report has given an overview of blockchain technology, from its origins to emerging directions. The range of references cited has illustrated the wide variety of blockchain concepts that are in use, in development, or being proposed. While cryptocurrencies attract the most attention, the core technology provides a tool for increasing data integrity using a combination of cryptography and consensus.

An architecture for applying blockchain to a tactical networked environment has been illustrated, showing how blockchain can be used in a centralised or distributed way, to address local challenges of power, memory and bandwidth limitations. In the example presented, blockchain was used to provide an auditing function, which might be used to support post-action analysis of cyber and kinetic operations; a resource management function to track the state of networked devices; and an authentication function to validate the devices connected to the tactical network.

Blockchain is another tool in the network and cyber security toolbox, but it is far from clear that it is the correct solution for the problem of achieving data integrity in tactical networks. The strongest tamper-resistance is achieved when the blockchain is continually growing, is reconciled across a large network, and is supported by a distributed consensus mechanism. In networks of wirelessly connected devices, the platforms themselves have limited processing power, battery capacity and memory, and are connected by dynamic links of limited bandwidth. Network partitions necessarily result in a loss of consistency and availability across the blockchain, and managing this requires additional overhead.

Further work is required to investigate the tradeoffs among blockchain length and network size, platform constraints and bandwidth requirements, and to determine whether the security achieved warrants the cost.

In the broader context, blockchain should still be considered carefully. As was noted in [103], "Compared to a properly configured centralized database, a blockchain solution will generally underperform, resulting in lower transaction processing throughput and higher latencies".

References

[1] Bitcoin, bitcoin.org Accessed Feb. 10, 2018.

[2] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008, available at nakamotoinstitute.org. Accessed Feb. 10, 2018.

[3] S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” *J. Cryptography*, vol. 3, no. 2, pp. 99–111, 1991.

[4] J. Benaloh and M. de Mare, “Efficient broadcast time-stamping,” Clarkson Univ., Dept. Math. and Comp. Sci., Tech. Rep. 1, Aug. 1991.

[5] D. Bayer, S. Haber, and W. S. Stornetta, “Improving the efficiency and reliability of digital time-stamping,” in *Sequences II*, R. Capocelli, A. D. Santis, and U. Vaccaro, Eds. New York, NY, USA: Springer, 1993.

[6] H. Massias, X. S. Avila, and J.-J. Quisquater, “Design of a secure timestamping service with minimal trust requirement,” in *20th Symp. Info. Theory in the Benelux*, 1999.

[7] U. Friedman, “Trust in government is collapsing around the world,” *The Atlantic*, Jul. 2016, available at www.theatlantic.com/international/archive/2016/07/trust-institutions-trump-brexit/489554 Accessed Feb. 10, 2018.

[8] Edelman Trust Barometer, www.edelman.com/trust2017 Accessed Feb. 10, 2018.

[9] A. T. Bond, “An app for that: Local governments and the rise of the sharing economy,” *Notre Dame Law Rev. Online*, vol. 90, pp. 77–96, 2015.

[10] Airbnb, airbnb.ca Accessed Feb. 10, 2018.

[11] L. Richardson, “Performing the sharing economy,” *Geoforum*, vol. 67, pp. 121–129, 2015.

[12] e-Estonia, e-estonia.com Accessed Feb. 10, 2018.

[13] “The Government of Canada to test cutting-edge technologies to support secure and seamless global travel for air passengers,” Jan. 2018, www.canada.ca/en/transport-canada/news/2018/01/the_government_ofcanadatotestcutting-edgetechnologiestosupportse.html Accessed Feb. 10, 2018.

[14] “H.R.2810 - National Defense Authorization Act for fiscal year 2018,” www.congress.gov/bill/115th-congress/house-bill/2810/text Accessed Feb. 10, 2018.

[15] J. Richmond, “DARPA and advancing cybersecurity infrastructure with blockchain,” May 2017, www.nasdaq.com/article/darpa-and-advancing-cybersecurity-infrastructure-with-blockchain-cm783507 Accessed Feb. 10, 2018.

[16] DARPA, “Secure messaging platform,” 2016, sbir.defensebusiness.org/search/item?id=27859&c=topic Accessed Jan 3, 2018.

[17] “Applicability of blockchain technology to privacy respecting identity management,” www.sbir.gov/sbirsearch/detail/867797 Accessed Feb. 10, 2018.

[18] US Department of Energy, “Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs: Topics,” 2016, www.energy.gov/sites/prod/files/2016/11/f34/EERE_FY2017_Phase_1_Release_2_Topics_Combined_8.pdf Accessed Feb. 10, 2018.

[19] “BlockCypher and U.S. Department Of Energy’s National Renewable Energy Laboratory to provide blockchain agnostic distributed energy solution,” Jan. 2018, www.prweb.com/releases/2018/01/prweb15117801.htm Accessed Feb. 10, 2018.

[20] “DHS S&T awards $199k to Austin based Factom Inc. for internet of things systems security,” Jun. 2016, www.dhs.gov/science-and-technology/news/2016/06/17/st-awards-199k-austin-based-factom-inc-iot-systems-security Accessed Feb. 10, 2018.

[21] H. Starkie, “Usage of blockchain in the UN system,” Aug. 2017, unite.un.org/sites/unite.un.org/files/session_3_b_blockchain_un_initiatives_final.pdf Accessed Feb. 10, 2018.

[22] Blockchain for impact, blockchaincommission.org Accessed Feb. 10, 2018.

[23] “Governments may be big backers of the blockchain,” Jun. 2017, www.economist.com/news/business/21722869-anti-establishment-technology-faces-ironic-turn-fortune-governments-may-be-big-backers Accessed Feb. 10, 2018.

[24] M. Lesh, “Blockchain offers an innovative solution to the Brexit customs puzzle,” Aug. 2017, brexitcentral.com/blockchain-innovative-solution-brexit-customs Accessed Feb. 10, 2018.

[25] IBM Blockchain, www.ibm.com/blockchain Accessed Feb. 10, 2018.

[26] Deloitte Blockchain Lab, www2.deloitte.com/ie/en/pages/technology/topics/blockchain-lab.html Accessed Feb. 10, 2018.

[27] Peer Ledger, peerledger.com Accessed Feb. 10, 2018.

[28] EncryptoTel, encryptotel.com Accessed Feb. 10, 2018.

[29] Solidity, solidity.readthedocs.io Accessed Feb. 10, 2018.

[30] Ethereum, www.ethereum.org Accessed Feb. 10, 2018.

[31] Hyperledger, hyperledger.org Accessed Feb. 10, 2018.

[32] ING Wholesale Banking, www.ingwb.com Accessed Feb. 10, 2018.

[33] Société Générale Corporate & Investment Banking, cib.societegenerale.com/en Accessed Feb. 10, 2018.

[34] "U.S. soy cargo to China traded using blockchain," Jan. 2018, www.reuters.com/article/grains-blockchain/u-s-soy-cargo-to-china-traded-using-blockchain-idUSL8N1PG0VJ Accessed Feb. 10, 2018.

[35] York University blockchain.lab, blockchain.lab.yorku.ca Accessed Feb 10, 2018.

[36] MIT Blockchain, blockchain.mit.edu Accessed Feb. 10, 2018.

[37] University of Berkeley, blockchain.berkeley.edu Accessed Feb. 10, 2018.

[38] University of British Columbia – Blockchain UBC, blockchainubc.ca Accessed Feb. 10, 2018.

[39] Open University – OpenBlockchain, blockchain.open.ac.uk Accessed Feb 10, 2018.

[40] S. Wilson and D. Chou, "How healthy is blockchain technology?" in *Proc. HIMSS AsiaPac17*, Sep. 2017.

[41] I. Kaminska, "Growing scepticism challenges the blockchain hype," *Financial Times*, Jun. 2017, available at www.ft.com/content/b5b1a5f2-5030-11e7-bfb8-997009366969 Accessed Feb 10, 2018.

[42] V. L. Lemieux, "In blockchain we trust? Blockchain technology for identity management and privacy protection," in *Conf. for E-Democracy and Open Govt.*, 2017, pp. 57–62.

[43] K. Stinchcombe, "Ten years in, nobody has come up with a use for blockchain," Dec. 2017, hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100 Accessed Feb. 10, 2018.

[44] A. Back, "Hash cash postage implementation," Mar. 1997, available at www.hashcash.org/papers Accessed Feb. 10, 2018.

[45] A. Back, "Hashcash - a denial of service counter-measure," Aug. 2002, available at www.hashcash.org/papers Accessed Feb. 10, 2018.

[46] A. Back, "Hashcash - amortizable publicly auditable cost-functions," Aug. 2002, available at www.hashcash.org/papers Accessed Feb. 10, 2018.

[47] C. C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Proc. Int. Cryptology Conf. (CRYPTO '92)*, Aug. 1992.

[48] M. O. Rabin, *Digitalized signatures.* New York, NY, USA: Academic Press, 1978, pp. 155–166.

[49] G. Yuval, "How to swindle Rabin," *Cryptologia*, vol. 3, pp. 187-–189, 1979.

[50] R. Merkle, “Secrecy, authentication, and public key systems,” Ph.D. dissertation, Standford University, 1979.

[51] N. Boudriga, *Security of mobile communications.* Boca Raton, FL: Auerbach Publications, 2010.

[52] R. C. Merkle, “Protocols for public key cryptosystems,” in *Proc. 1980 Symp. on Security and Privacy*, Apr. 1980, pp. 122-–133.

[53] M. Hearn, “Corda: A distributed ledger,” Nov. 2016, available at www.corda.net/introduction Accessed Feb. 10, 2018.

[54] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, “Corda: An introduction,” Aug. 2016, available at www.corda.net/introduction Accessed Feb. 10, 2018.

[55] Proof-of-stake FAQ, github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ Accessed Dec 21, 2017.

[56] V. Zamfir, “Introducing Casper ‘the Friendly Ghost’,” Aug. 2015, available at blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost Accessed Feb. 10, 2018.

[57] Peercoin, peercoin.net Accessed Feb. 10, 2018.

[58] M. Castro and B. Liskov, “Practical Byzantine fault tolerance,” in *Proc. Symp. Oper. Syst. Design and Implementation*, 1999, pp. 173–186.

[59] Tendermint, tendermint.com Accessed Feb. 10, 2018.

[60] Backfeed, backfeed.cc Accessed Feb. 10, 2018.

[61] FairCoin, fair-coin.org Accessed Feb. 10, 2018.

[62] Intel software guard extensions, software.intel.com/en-us/sgx Accessed Feb. 10, 2018.

[63] J. Liu, W. Li, G. O. Karame, and N. Asokan, “Scalable Byzantine consensus via hardware-assisted secret sharing,” 2017, available at arxiv.org/abs/1612.04997 Accessed Feb. 10, 2018.

[64] Bitcoin statistics, blockchain.info Accessed Feb. 10, 2018.

[65] Bitcoin statistics, bitinfocharts.com Accessed Feb. 10, 2018.

[66] P. Fairley, “The ridiculous amount of energy it takes to run Bitcoin,” *IEEE Spectrum*, Sep. 2017, available at spectrum.ieee.org/energy/policy/the-ridiculous-amount-of-energy-it-takes-to-run-bitcoin Accessed Feb. 10, 2018.

[67] J. Redman, "The reason why Bitcoin miners dedicate time to mining empty blocks," Jul. 2017, news.bitcoin.com/reason-bitcoin-miners-empty-blocks Accessed Feb. 10, 2018.

[68] D. Bradbury, "Hyperledger 3 years later: But is anyone actually using it?" Jan. 2018, www.theregister.co.uk/2018/01/02/hyperledger_at_three Accessed Feb. 10, 2018.

[69] C. Group, cls-group.com Accessed Feb. 10, 2018.

[70] Corda, corda.net Accessed Feb. 10, 2018.

[71] R3, www.r3.com/blog/2017/11/13/r3s-corda-partner-network-grows-to-over-60-companies-including-hewlett-packard-enterprise-intel-and-microsoft Accessed Feb. 10, 2018.

[72] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. IFIP WG 11.4 Workshop Open Res. Problems Netw. Secur. (iNetSec)*, 2015, pp. 112–125.

[73] A. Back, M. Corallo, M. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," 2014, available at blockstream.com/technology Accessed Feb. 10, 2018.

[74] Lisk, lisk.io Accessed Feb. 10, 2018.

[75] Cosmos, cosmos.network Accessed Feb. 10, 2018.

[76] "On sharding blockchains," github.com/ethereum/wiki/wiki/Sharding-FAQ Accessed Dec 22, 2017.

[77] A. Rosic, "What are Ethereum nodes and sharding?" blockgeeks.com/guides/what-are-ethereum-nodes-and-sharding Accessed Feb 10, 2018.

[78] A. Reese, "Buterin lays out Ethereum's next 3-5 years, explains sharding," *ETH News*, Nov. 2017, available at www.ethnews.com/buterin-lays-out-ethereums-next-3-5-years-explains-sharding Accessed Feb. 10, 2018.

[79] P. Todd, "Tree-chains preliminary summary," Mar. 2014, available at www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg04388.html Accessed Feb. 10, 2018.

[80] P. Evans-Greenwood, "Blockchain performance might always suck, but that's not a problem," May 2016, available at blog.deloitte.com.au/blockchain-performance-sucks-not-problem Accessed Feb. 10, 2018.

[81] Viacoin, viacoin.org Accessesd Feb. 10, 2018.

[82] R. Aitken, “Smart contracts on the blockchain: can businesses reap the benefits?” Nov. 2017, available at https://www.forbes.com/sites/rogeraitken/2017/11/21/smart-contracts-on-the-blockchain-can-businesses-reap-the-benefits/#5ba799dc1074 Accessed Feb. 10, 2018.

[83] SmartContract, www.smartcontract.com Accessed Feb. 10, 2018.

[84] N. Szabo, “Formalizing and securing relationships on public networks,” *First Monday*, vol. 2, no. 9, 1997.

[85] G. Greenspan, “Why many smart contract use cases are simply impossible,” *Coindesk*, Apr. 2016, available at coindesk.com/three-smart-contract-misconceptions Accessed Dec Feb. 10, 2018.

[86] “KODAK and WENN digital partner to launch major blockchain initiative and cryptocurrency,” Jan. 2018, www.kodak.com/CA/en/corp/press_center/kodak_and_wenn_digital_partner_to_launch_major_blockchain_initiative_and_cryptocurrency/default.htm Accessed Feb. 10, 2018.

[87] Po.et, po.et Accessed Feb. 10, 2018.

[88] Photochain, photochain.io Accessed Feb. 10, 2018.

[89] COPYTRACK, copytrack.io Accessed Feb. 10, 2018.

[90] J. Rath, “Spotify acquired blockchain startup Mediachain,” Apr. 2017, www.businessinsider.com/spotify-acquired-blockchain-startup-mediachain-2017-4 Accessed Feb. 10, 2018.

[91] Long Island Iced Tea, www.longislandicedtea.com Accessed Feb 10, 2018.

[92] L. Gensler, “Long Island Iced Tea Company says it’s pivoting to blockchain, stock zooms 500% higher,” Dec. 2017, www.forbes.com/sites/laurengensler/2017/12/21/an-iced-tea-company-says-its-pivoting-to-blockchain-stock-rockets-higher Accessed Feb. 10, 2018.

[93] Blockcypher, blockcypher.com Accessed Feb. 10, 2018.

[94] L. Constantin, “Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON,” *CSO*, Sep. 2016, available at www.csoonline.com/article/3119765/security/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html Accessed Feb. 10, 2018.

[95] S. Hilton, “Dyn analysis summary of friday october 21 attack,” *Dyn Company News*, Oct. 2016, available at dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack Accessed Feb. 10, 2018.

[96] L. Franceschi-Bicchierai, “Hackers make the first-ever ransomware for smart thermostats,” *Vice Motherboard*, Aug. 2016, available at motherboard.vice.com/en_us/article/aekj9j/internet-of-things-ransomware-smart-thermostat Accessed Feb. 10, 2018.

[97] K. Noyen, D. Volland, D. Wörner, and E. Fleisch, “When money learns to fly: Towards sensing as a service applications using Bitcoin,” 2014, available at arxiv.org/abs/1409.5841 Accessed Feb. 10, 2018.

[98] M. Conoscenti, A. Vetrò, and J. C. D. Martin, “Blockchain for the Internet of Things: A systematic literature review,” in *Proc. Conf. Computer Systems and Appl. (AICCSA)*, Nov. 2016.

[99] A. Bahga and V. K. Madisetti, “Blockchain platform for industrial Internet of Things,” *J. Softw. Eng. Appl.*, vol. 9, no. 10, 2016.

[100] N. Kshetri, “Can blockchain strengthen the Internet of Things?” *IEEE IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.

[101] H. Kim and E. A. Lee, “Authentication and authorization for the Internet of Things,” *IEEE IT Professional*, vol. 19, no. 5, pp. 27–33, 2017.

[102] S. Huh, S. Cho, and S. Kim, “Managing IoT devices using blockchain platform,” in *Proc. Int. Conf. Advanced Communication Technology (ICACT)*, 2017, pp. 464–467.

[103] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[104] M. Mylrea and S. N. G. Gourisetti, “Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security,” in *Proc. Resilience Week (RWS)*, 2017, pp. 18–23.

[105] V. Pureswaran, S. Panikkar, S. Nair, and P. Brody, “Empowering the edge: Practical insights on a decentralized Internet of Things,” 2015, available at www-935.ibm.com/services/multimedia/GBE03662USEN.pdf Accessed Feb. 10, 2018.

[106] Gartner, “Gartner says 8.4 billion connected “things” will be in use in 2017, up 31 percent from 2016,” 2017, www.gartner.com/newsroom/id/3598917 Accessed Feb. 10, 2018.

[107] Statistica, “Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025,” 2017, www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide Accessed Feb. 10, 2018.

[108] L. MacVittie, “IoT tipping point: Connection capacity,” May 2017, www.networkcomputing.com/networking/iot-tipping-point-connection-capacity/503542613 Accessed Feb. 10, 2018.

[109] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in internet of things: challenges and solutions,” 2016, available at arxiv.org/abs/1608.05187 Accessed Feb. 10, 2018.

[110] L. Mearian, “Blockchain-as-a-service allows enterprises test distributed ledger technology,” Nov. 2017, www.computerworld.com/article/3237465/enterprise-applications/blockchain-as-a-service-allows-enterprises-test-distributed-ledger-technology.html Accessed Feb. 10, 2018.

[111] “Oracle launches enterprise-grade blockchain cloud service,” www.oracle.com/corporate/pressrelease/oow17-oracle-launches-blockchain-cloud-service-100217.html Accessed Feb. 10, 2018.

[112] “Blockchain on Azure,” azure.microsoft.com/en-us/solutions/blockchain Accessed Feb. 10, 2018.

[113] “Hewlett packard enterprise introduces blockchain as-a-service solution for enterprises,” news.hpe.com/hewlett-packard-enterprise-introduces-blockchain-as-a-service-solution-for-enterprises Accessed Feb. 10, 2018.

[114] H. P. Labs, www.labs.hpe.com/next-next/blockchain Accessed Feb. 10, 2018.

[115] Sia, sia.tech Accessed Feb. 10, 2018.

[116] Storj, storj.io Accessed Feb. 10, 2018.

[117] ITAMCO, www.itamco.com Accessed Feb. 10, 2018.

[118] SIMBA chain, www.simbachain.org Accessed Feb. 10, 2018.

[119] Crypto-chat, crypto-chat.com Accessed Feb. 10, 2018.

[120] R. A. International, “Mercury protocol whitepaper,” Oct. 2017, available at www.mercuryprotocol.com Accessed Feb. 10, 2018.

[121] Dust, usedust.com Accessed Feb. 10, 2018.

[122] Pikciome, pikcio.me Accessed Feb. 10, 2018.

[123] MatchUpBox, www.matchupbox.com Accessed Feb. 10, 2018.

[124] “Pikciochain whitepaper,” available at pikciochain.com Accessed Feb. 10, 2018.

[125] Blokcom, www.reply.com/en/content/blokcom Accessed Feb. 10, 2018.

[126] Obsidian, obsidianplatform.com Accessed Feb. 10, 2018.

[127] Crypviser, crypviser.net Accessed Feb. 10, 2018.

[128] V. Andryan, “Crypviser whitepaper,” 2017, available at ico.crypviser.net/static/docs/CrypViserWhitepaper_en.pdf Accessed Jan 23, 2018.

[129] SwiftMail, johnmcafeeswiftmail.com Accessed Feb. 10, 2018.

[130] CryptaMail, www.cryptamail.com Accessed Feb. 10, 2018.

[131] NXT, nxtplatform.org Accessed Feb. 10, 2018.

[132] Pomcor, pomcor.com Accessed Feb. 10, 2018.

[133] K. Lewison and F. Corella, “Backing rich credentials with a blockchain PKI,” Tech. Rep., Oct. 2016, available at pomcor.com/techreports/BlockchainPKI.pdf Accessed Feb. 10, 2018.

[134] J. S. Arun, “Reimagining the future of identity management with blockchain,” Mar. 2017, securityintelligence.com/reimagining-the-future-of-identity-management-with-blockchain Accessed Feb. 10, 2018.

[135] G. Wolfond, “A blockchain ecosystem for digital identity: Improving service delivery in Canada’s public and private sectors,” *Technol. Innov. Mgmt. Rev.*, vol. 7, no. 10, 2017.

[136] Guardtime, guardtime.com Accessed Jan 19, 2018.

[137] J. Leyden, “Estonia government locks down ID smartcards: Refresh or else,” Nov. 2017, www.theregister.co.uk/2017/11/03/estonian_e_id_lockdown Accessed Feb. 10, 2018.

[138] G. P. Forum, www.partnerships.org Accessed Feb. 10, 2018.

[139] J. J. Roberts, “Microsoft and Accenture unveil global ID system for refugees,” Jun. 2018, fortune.com/2017/06/19/id2020-blockchain-microsoft Accessed Feb. 10, 2018.

[140] J. Southurst, “BitID will verify your identity with the Bitcoin blockchain,” Jul. 2016, news.bitcoin.com/bitid-verify-id-bitcoin-blockchain Accessed Feb. 10, 2018.

[141] “How to use the BitID app?” support.ledgerwallet.com/hc/en-us/articles/115005198625 Accessed Feb 10, 2018.

[142] “BitAuth, for decentralized authentication,” blog.bitpay.com/bitauth-for-decentralized-authentication Accessed Feb 10, 2018.

[143] H. Weisbaum, “More than 4 billion data records were stolen globally in 2016,” Jan. 2017, www.nbcnews.com/storyline/hacking-in-america more-4-billion-data-records-were-stolen-globally-2016-n714066 Accessed Feb. 10, 2018.

[144] Shocard, shocard.com Accessed Feb. 10, 2018.

[145] Civic, www.civic.com Accessed Feb. 10, 2018.

[146] SecureKey, securekey.com Accessed Feb. 10, 2018.

[147] "Galois and Guardtime Federal awarded $1.8m DARPA contract to formally verify blockchain-based integrity monitoring system," Sep. 2016, galois.com/news/galois-guardtime-formal-verification Accessed Feb. 10, 2018.

[148] LCDR Jon McCarter, USN, "DON innovator embraces a new disruptive technology: Blockchain," www.secnav.navy.mil/innovation/Pages/2017/06/BlockChain.aspx Accessed Feb. 10, 2018.

[149] S. Higgins, "The US Navy wants to connect its 3-D printers with a blockchain," May 2017, www.coindesk.com/the-us-navy-wants-to-connect-its-3-d-printers-with-a-blockchain Accessed Jan 23, 2018.

[150] R. Greenfield, "Vulnerability: Proof of work vs. proof of stake," Aug. 2017, medium.com/@robertgreenfieldiv/vulnerability-proof-of-work-vs-proof-of-stake-f0c44807d18c Accessed Feb. 10, 2018.

[151] N. T. Courtois, "On the longest chain rule and programmed self-destruction of crypto currencies," 2014, available at arxiv.org/abs/1405.0534 Accessed Feb. 10, 2018.

[152] Blocktrail – pool distribution, www.blocktrail.com/BTC/pools Accessed Feb. 10, 2018.

[153] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," 2013, available at arxiv.org/abs/1311.0243 Accessed Feb. 10, 2018.

[154] N. Houy, "It will cost you nothing to 'kill' a proof-of-stake crypto-currency," 2014, available from halshs.archives-ouvertes.fr/halshs-00945053/document Accessed Feb. 10, 2018.

[155] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology.* Springer, 2017, pp. 297–315.

[156] J. Mattila, "The blockchain phenomenon," Berkeley Roundtable on the International Economy, Tech. Rep. 2016-1, 2016.

[157] N. Bozic, G. Pujolle, and S. Secci, "A tutorial on blockchain and applications to secure network control-planes," in *Proc. Smart Cloud Networks & Systems (SCNS)*, 2016.

[158] Z. Wan, D. Lo, X. Xia, and L. Cai, “Bug characteristics in blockchain systems: a large-scale empirical study,” in *Proc. Int. Conf. on Mining Software Repositories*, 2017, pp. 413–424.

[159] Dogecoin, dogecoin.com Accessed Feb. 10, 2018.

[160] F. Chaparro, “A cryptocurrency created as a joke about a dog meme now has a market cap above $2 billion,” Jan. 2018, www.businessinsider.com/dogecoin-cryptocurrency-has-market-cap-above-2-billion-2018-1 Accessed Feb 2, 2018.

[161] K. Werbach and N. Cornell, “Contracts ex machina,” *Duke Law Journal*, 2017, available at papers.ssrn.com/sol3/papers.cfm?abstract_id=2936294 Accessed Feb. 10, 2018.

[162] Quadrigacx on Reddit, reddit.com/r/ethereum/comments/6ettq5/statement_on_quadrigacx_ether_contract_error Accessed Feb. 10, 2018.

[163] Quadrigacx, quadrigacx.com Accessed Feb. 10, 2018.

[164] Parity, Nov. 2017, paritytech.io/security-alert-2 Accessed Feb. 10, 2018.

[165] L. Franceschi-Bicchierai, Jan. 2018, motherboard.vice.com/en_us/article/ev55na/electrum-bitcoin-wallets-were-vulnerable-to-hackers-for-two-years-json-rpc Accessed Feb. 10, 2018.

[166] A. Hern, “‘$300m in cryptocurrency’ accidentally lost forever due to bug,” Nov. 2017, www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether Accessed Feb. 10, 2018.

[167] M. Murphy, “£52m in bitcoin stolen after cryptocurrency exchange heist,” Dec. 2017, www.telegraph.co.uk/technology/2017/12/07/52m-bitcoin-stolen-cryptocurrency-exchange-heist Accessed Feb. 10, 2018.

[168] P. Bright, “‘Meltdown’ and ‘Spectre’: Every modern processor has unfixable security flaws,” Jan. 2018, arstechnica.com/gadgets/2018/01/meltdown-and-spectre-every-modern-processor-has-unfixable-security-flaws Accessed Feb. 10, 2018.

[169] S. Schroeder, “Spectre and Meltdown are a danger for your bitcoins, but there are ways to keep them safe,” Jan. 2018, mashable.com/2018/01/05/spectre-meltdown-bitcoin Accessed Feb. 10, 2018.

[170] Xapo, xapo.com Accessed Feb. 10, 2018.

[171] R. McMillan, “The inside story of Mt. Gox, Bitcoin’s $460 million disaster,” Mar. 2014, www.wired.com/2014/03/bitcoin-exchange Accessed Feb. 10, 2018.

[172] C. Baldwin, “Bitfinex says expects ‘socialized loss’ for $72 million bitcoin hack,” Aug. 2016, www.reuters.com/article/us-bitfinex-hacked-hongkong/bitfinex-says-

expects-socialized-loss-for-72-million-bitcoin-hack- idUSKCN10G0CZ?il=0 Accessed Feb. 10, 2018.

[173] J. Wieczner, “Hacking Coinbase: The great bitcoin bank robbery,” Aug. 2017, fortune.com/2017/08/22/bitcoin-coinbase-hack Accessed Feb. 10, 2018.

[174] F. Chaparro, “Cyberattack brings a cryptocurrency exchange to its knees,” Dec. 2017, www.businessinsider.com/cyberattack-brings-a-cryptocurrency-exchange-to-its-knees-2017-12 Accessed Feb. 10, 2018.

[175] “How to steal $500 million in cryptocurrency,” Jan. 2018, fortune.com/2018/01/31/coincheck-hack-how Accessed Feb. 10, 2018.

[176] J. A. Guerrero-Saade and P. Moriuchi, “North Korea targeted South Korean cryptocurrency users and exchange in late 2017 campaign,” Recorded Future, Tech. Rep. CTA-2018-0116, Jan. 2018, available at go.recordedfuture.com/hubfs/reports/cta-2018-0116.pdf Accessed Feb. 10, 2018.

[177] G. Jenkinson, “How DDOS attacks affect Bitcoin exchanges,” Dec. 2017, cointelegraph.com/news/how-ddos-attacks-affect-bitcoin-exchanges Accessed Feb. 10, 2018.

[178] Reuters, reuters.com Accessed Feb. 10, 2018.

[179] D. Verma, N. Desai, A. Preece, and I. Taylor, “A blockchain based architecture for asset management in coalition operations,” in *Proc. SPIE Defense & Security*, 2017.

[180] “H.R.4412 - National Aeronautics and Space Administration Authorization Act of 2014,” available at www.congress.gov/bill/113th-congress/house-bill/4412 Accessed Feb. 10, 2018.

[181] “Fake parts in Hercules aircraft called a genuine risk,” Jan. 2013, www.cbc.ca/news/politics/fake-parts-in-hercules-aircraft-called-a-genuine-risk-1.1345862 Accessed Feb. 10, 2018.

[182] “Alleged counterfeit parts in Canada’s CC-130J Hercules aircraft,” Feb. 2013, www.forces.gc.ca/en/news/article.page?doc=alleged-counterfeit-parts-in-canada-rsquo-s-cc-130j-hercules-aircraft/hie8w7n7 Accessed Feb. 10, 2018.

[183] N. Barnas, Maj, USAF, “Blockchains in National Defense: trustworthy systems in a trustless world,” Air University, US, Tech. Rep., Jun. 2016, available at www.jcs.mil/Portals/36/Documents/Doctrine/Education/jpme_papers/barnas_n.pdf Accessed Feb. 10, 2018.

[184] A. Greenberg, “The Petya plague exposes the threat of evil software updates,” Jul. 2017, www.wired.com/story/petya-plague-automatic-software-updates Accessed Feb. 10, 2018.

[185] "Cyber electromagnetic activities," US Department of the Army, Tech. Rep. FM3-38, Feb. 2014, available at fas.org/irp/doddir/army/fm3-38.pdf Accessed Feb. 10, 2018.

[186] NIST Engineering Laboratory - Cyber-Physical Systems, www.nist.gov/el/cyber-physical-systems Accessed Feb. 10, 2018.

[187] A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," 2017, available at arxiv.org/abs/1706.01730 Accessed Feb. 10, 2018.

[188] A. Gonsalves, "Cisco says blockchain ledger technology has networking role," Aug. 2017, searchsdn.techtarget.com/news/450423763/Cisco-says-blockchain-ledger-technology-has-networking-role Accessed Feb. 10, 2018.

[189] Z. Cole, "How blockchain technology could affect the future of network engineering," Nov. 2017, www.networkworld.com/article/3236479/asset-management/how-blockchain-technology-could-affect-the-future-of-network-engineering.html Accessed Feb. 10, 2018.

[190] J. Spencer and T. Willink, "SDN in tactical networks," in *Proc. IEEE Conf. Mil. Commun. (MILCOM)*, Nov. 2016.

[191] D. Kidston, Y. Ge, and K. Baddour, "Federated mission network scoping study," Communications Research Centre, Tech. Rep., Jul. 2014.

[192] Multinational Capability Development Campaign, "Federated mission networking and mission partner environment civilian military (FMCM) information sharing project," NATO, Tech. Rep., Jun. 2017, available at c2coe.org/wp-content/uploads/2017/06/150935JUN17_FMCM_C2COE_2017_REV_2.pdf Accessed Feb. 10, 2018.

[193] S. Dumoulin, "Policy-based spectrum management," Communications Research Centre, Tech. Rep., Jan. 2016.

[194] D. Fritz, "DISA perspective on dynamic spectrum access and policy-based spectrum management," Mitre Corp, Tech. Rep., Apr. 2012, available at energy.gov/sites/prod/files/Wednesday_Cedars_1330_Fritz.pdf Accessed Feb. 10, 2018.

[195] T. J. Willink, "Assured communications in challenging and contested environments," DRDC, Tech. Rep. DRDC-RDDC-2016-R107, Jun. 2016.

[196] M. Castro, "Practical Byzantine fault tolerance," Ph.D. dissertation, MIT, USA, Jan. 2001, available at www.pmg.csail.mit.edu/bft Accessed Feb. 10, 2018.

[197] R. Pass, L. Seeman, and A. Shelat, "Analysis of the blockchain protocol in asynchronous networks," in *Int. Conf. Theory and Applications of Cryptographic Techniques*, 2017, pp. 643–673.

[198] J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin backbone protocol: Analysis and applications," in *Int. Conf. Theory and Applications of Cryptographic Techniques*, 2015, pp. 281–310.

[199] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of distributed consensus with one faulty process," *Journal of the ACM*, vol. 32, no. 2, pp. 374–382, 1985.

[200] S. Gilbert and N. Lynch, "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services," *ACM SigAct News*, vol. 33, no. 2, pp. 51–59, 2002.

[201] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, and E. G. Sirer, "On scaling decentralized blockchains," in *Proc. Int. Conf. Financial Cryptography and Data Security*, 2016, pp. 106–125.

[202] M. Swan, *Blockchain: blueprint for a new economy.* Sebastopol, CA, USA: O'Reilly, 2015.

[203] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," 2017, available at arxiv.org/abs/1708.05665 Accessed Feb. 10, 2018.

[204] D. Xiao, "The four layers of the blockchain," Jun. 2016, available at medium.com/@coriacetic/the-four-layers-of-the-blockchain-dc1376efa10f Accessed Feb. 10, 2018.

[205] M. Singh and S. Kim, "Blockchain based intelligent vehicle data sharing framework," 2017, available at arxiv.org/abs/1708.09721 Accessed Feb. 10, 2018.

[206] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography.* Springer, 2006.

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or a tasking agency, is entered in Section 8.)

DRDC – Ottawa Research Centre
3701 Carling Avenue, Ottawa ON K1A 0Z4,
Canada

2a. SECURITY MARKING (Overall security marking of the document, including supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

On blockchain technology and its potential application in tactical networks

4. AUTHORS (Last name, followed by initials – ranks, titles, etc. not to be used. Use semi-colon as delimiter)

Willink, T. J.

5. DATE OF PUBLICATION (Month and year of publication of document.)

April 2018

6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)

62

6b. NO. OF REFS (Total cited in document.)

206

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter)

Scientific Report

8. SPONSORING CENTRE (The name and address of the department project or laboratory sponsoring the research and development.)

DRDC – Ottawa Research Centre
3701 Carling Avenue, Ottawa ON K1A 0Z4, Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

05ab

9b. CONTRACT NO. (If appropriate, the applicable contract number under which the document was written.)

10a. DRDC DOCUMENT NUMBER

DRDC-RDDC-2018-R033

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

blockchain; tactical networks

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

Awareness of blockchain has soared in recent years with the emergence of cryptocurrencies, but the technology has existed for much longer. The linking of blocks, containing cryptographic functions of transactions and data, means that tampering with their contents becomes increasingly difficult as the chain grows – this concept was exploited for document timestamping applications more than a decade before cryptocurrencies became reality. In many implementations, blocks are confirmed by, and stored at, many nodes in different locations, providing a high degree of data integrity. There are, however, many challenges for applying blockchain technologies in tactical networks, particularly due to the constraints of the platforms, the limited bandwidth available among them, and the impact of network partitioning. In this report, the development and principles of blockchains are presented, along with an overview of their weaknesses and vulnerabilities. There is a huge level of interest in this technology across many sectors, and this is reflected in the breadth of the referenced material. Weaknesses in design and implementation can make blockchains vulnerable to attack, and their interfaces are particularly at risk. A range of possible applications in tactical networks is explored, from supply chain management, to network management and application data immutability. Finally, a simple blockchain architecture for mobile tactical networks is developed, to illustrate the potential and challenges of this technology. Overall, it is clear that blockchain technology provides a potential avenue for solving some problems in the tactical network context, but it is not yet clear whether it is the best such solution.

L'intérêt à l'endroit des chaînes de blocs s'est accru de manière fulgurante durant les dernières années avec l'arrivée de la cryptomonnaie. Pourtant, cette technologie existe déjà depuis un bon moment. L'enchaînement de blocs qui contiennent des fonctions cryptographiques des transactions et des données a pour effet de rendre plus difficile la falsification du contenu des blocs à mesure que la chaîne s'allonge. Ce concept a été exploité dans les applications d'horodatage des documents plus d'une décennie avant l'apparition de la cryptomonnaie. Dans bon nombre d'applications, les blocs sont confirmés par de nombreux noeuds et entreposés à différents endroits, ce qui permet un niveau élevé d'intégrité des données. L'application de la technologie des chaînes de blocs aux réseaux tactiques pose beaucoup de problèmes particuliers cependant, surtout en raison des contraintes des plateformes, de la bande passante limitée disponible entre les plateformes et des répercussions du partitionnement du réseau. Dans le présent rapport, l'auteur présente l'élaboration et les principes des chaînes de blocs, de même qu'un aperçu de leurs désavantages et de leurs vulnérabilités. Cette technologie suscite un très grand intérêt dans un grand nombre de secteurs, comme en témoignent les différents documents de référence. Des faiblesses dans la conception et la mise en oeuvre peuvent rendre les chaînes de blocs vulnérables aux attaques; leurs interfaces sont d'ailleurs particulièrement à risques. L'auteur explore un éventail d'applications possibles dans les réseaux tactiques, de la gestion de la chaîne d'approvisionnement à celle des réseaux et à l'immuabilité des données d'application. Enfin, l'auteur élabore l'architecture simple des chaînes de blocs d'un réseau tactique mobile afin d'illustrer le potentiel et les difficultés de cette technologie. Dans l'ensemble, la technologie des chaînes de blocs offre manifestement une avenue possible pour régler certains problèmes dans le cadre des réseaux tactiques, sans qu'on ait établi clairement jusqu'à maintenant qu'elle constitue la meilleure solution.